SIEMENS

SIMATIC NET

Industrial Ethernet Security Security basics and application

Configuration Manual

Preface

Introduction and basics 1

Configuring with the Security Configuration Tool 2

Creating modules and setting network parameters 3

Configure the firewall 4

Configuring additional module properties 5

Secure communication in the VPN via an IPsec tunnel 6

Router and firewall redundancy 7

SOFTNET Security Client 8

Online functions - diagnostics and logging 9

Appendix A

References B

04/2017

C79000-G8976-C286-08

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
>
> indicates that minor personal injury can result if proper precautions are not taken.

> NOTICE
>
> indicates that property damage can result if proper precautions are not taken.

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
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: C79000-G8976-C286-08
℗ 04/2017 Subject to change

Preface

Preface

Validity of this manual

This manual is valid for the following SIMATIC NET modules:

Module	Article number
SCALANCE S602	6GK5 602-0BA10-2AA3
SCALANCE S612	6GK5 612-0BA10-2AA3
SCALANCE S623	6GK5 623-0BA10-2AA3
SCALANCE S627-2M	6GK5 627-2BA10-2AA3
CP 343-1 Advanced as of V3	6GK7 343-1GX31-0XE0
CP 443-1 Advanced as of V3	6GK7 443-1GX30-0XE0
CP 443-1 OPC UA	6GK7 443-1UX30-0XE0
CP 1628	6GK1 162-8AA00
Mobile wireless router SCALANCE M875	6GK5 875-0AA10-1CA2
Mobile wireless router SCALANCE M874 / SCALANCE M876	Link (https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10215930?tree=CatalogTree)
LAN router SCALANCE S615	6GK5 615-0AA00-2AA2
ADSL router SCALANCE M812	6GK5 812-1AA00-2AA2
	6GK5 812-1BA00-2AA2
ADSL router SCALANCE M816	6GK5 816-1AA00-2AA2
	6GK5 816-1BA00-2AA2
SHDSL router SCALANCE M826	6GK5 826-2AB00-2AB2

SCALANCE S V1/V2 modules are no longer supported as of SCT V5.0 and can no longer be inserted in SCT projects. SCALANCE S V1/V2 modules from projects of older SCT versions are simply displayed with their module properties. These properties cannot, however, be edited. Downloading, diagnostics and firmware updates of SCALANCE S V1/V2 devices are also not possible. All the functions described for SCALANCE S modules relate to the firmware versions as of V3.

To retain the configuration data, SCALANCE S V1/V2 modules can be replaced in SCT with SCALANCE S modules with a higher firmware version, see section Replacing a module (Page 24).

This manual is valid for the following SIMATIC NET configuration tools:

Configuration tool	Article number	Version
SOFTNET Security Client	6GK1704-1VW05-0AA0	V5.0
Security Configuration Tool (SCT)	-	V5.0

General terminology "security module"

In this documentation, the term "security module" includes the following products: SCALANCE S602 / SCALANCE S612 / SCALANCE S623 / SCALANCE S627-2M, CP 343-1 Advanced, CP 443-1 Advanced, CP 443-1 OPC UA, CP 1628.

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.

Use of the terms "interface" and "port"

In this documentation, the following terms are used for the ports of SCALANCE S modules:

- "External interface": The external port of the SCALANCE S602 / S612 / S623 or an external port of the SCALANCE S627-2M (marked red)
- "Internal interface": The internal port of the SCALANCE S602 / S612 / S623 or an internal port of the SCALANCE S627-2M (marked green)
- "DMZ interface": The DMZ port of the SCALANCE S623 / S627-2M (marked yellow)

The term "port" itself is used when the focus of interest is a special port of an interface.

General use of the term "STEP 7"

The configuration of the security functions of CPs is possible as of STEP 7 V5.5 SP2 HF1. For this reason, in this documentation, the term "STEP 7" stands for all versions of STEP 7 as of V5.5 SP2 HF1 and lower than STEP 7 V10. How to configure the security functions of all security modules in STEP 7 as of V12 can be found in the information system of STEP 7 as of V12, section "Industrial Ethernet Security".

General use of the term "CP x43-1 Adv."

In this documentation, the term "CP x43-1 Adv." includes the following products: CP 343-1 Advanced / CP 443-1 Advanced

Security Configuration Tool V5.0 - New and expanded functions

The Security Configuration Tool V5.0 includes the following new functions and expanded functions:

- **Supported operating systems**

  The following operating systems are also supported as of SCT V5.0:

  – Microsoft Windows 10 Professional / Enterprise Version 1607 x64

  – Microsoft Windows 10 Enterprise 2015 LTSB

  – Microsoft Windows Server 2012 R2 Standard x64

  – Microsoft Windows Server 2016 x64

  The following operating systems are no longer supported as of SCT V5.0:

  – Microsoft Windows XP x32

  – Microsoft Windows 7 Professional / Enterprise / Ultimate x32

  For the following operating systems Service Pack 1 is required as of SCT V5.0:

  – Microsoft Windows 7 Professional / Enterprise / Ultimate x64

  – Microsoft Windows Server 2008 R2 Standard x64

- **Supported security modules**

  SCALANCE S V1/V2 modules are no longer supported as of SCT V5.0.

- **Prioritization of firewall rules crated by SCT for NAT/NAPT rules**

  As of SCT V5.0, as default, firewall rules crated by SCT for NAT/NAPT rules have the highest priority.

Audience

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

SIMATIC NET Manual Collection (order no. A5E00069051)

The SIMATIC NET Manual Collection ships with SCALANCE S modules, the S7 CPs and the PC CP 1628. This Manual Collection is regularly updated and contains the device manuals and descriptions valid at the time it is created.

Security recommendations

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to make sure that this product meets these recommendations and/or other internal security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Keep the software you are using up to date. Check regularly for security updates of the product.
  You will find information on this at http://www.siemens.com/industrialsecurity.
- Only activate protocols you require to operate your devices.
- Whenever possible, always use the variants of protocols that provide greater security (e.g. SNMPv3, NTP (secure) etc.).
- Restrict access to the Security Configuration Tool to qualified personnel.

Passwords

- Define guidelines for the use of the software and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Change default passwords for users before you use the software.
- Only use passwords with a high password strength. Avoid weak passwords for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems or after it has expired.

Automation License Manager

If you do not require the network functions of the Automation License Manager, deny access to these functions in your firewall.

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

C-PLUG, CP 343-1, CP 443-1, SCALANCE, SIMATIC, SOFTNET

Symbols used in this manual

S≥V4.0

The chapter described / the section described / the line described is only relevant for SCALANCE S as of V4.0.

SCA. S

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

SCA. M

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

~~M875~~

The chapter described / the section described / the line described is relevant for all modules except SCALANCE M875.

~~SCA. M~~

The chapter described / the section described / the line described is relevant for all modules except SCALANCE M.

~~S602~~

The chapter described / the section described / the line described is relevant for all security modules except SCALANCE S602.

S602 ≥V3.1

The chapter described / the section described / the line described is relevant only for SCALANCE S602 as of V3.1.

S623

The chapter described / the section described / the line described is relevant for SCALANCE S623 only.

S627-2M

The chapter described / the section described / the line described is relevant for SCALANCE S627-2M only.

S62x

The chapter described / the section described / the line described is relevant for SCALANCE S623 and SCALANCE S627-2M only.

S62x ≥ V4.0

The chapter described / the section described / the line described is relevant only for SCALANCE S623 as of V4.0 and SCALANCE S627-2M as of V4.0.

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.

~~CP~~

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

CP x43-1 Adv.

The chapter described / the section described / the line described is only relevant for CP x43-1 Adv.

CP 443-1 OPC UA

The chapter described / the section described / the line described is only relevant for CP 443-1 OPC UA.

~~CP 443-1 OPC UA~~

The chapter described / the section described / the line described is relevant for all security modules except CP 443-1 OPC UA.

VPN device

The chapter described / the section described / the line described is only relevant for the VPN device.

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

Customer Support pages (https://support.industry.siemens.com/cs/us/en/ps/15326)

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary on the Internet at the following address:

50305045 (https://support.industry.siemens.com/cs/us/en/view/50305045)

Table of contents

Preface 3

1 Introduction and basics 17

1.1 Important information 17

1.2 Product characteristics 20
1.2.1 Introduction and basics 20
1.2.2 Overview of the functions 20
1.2.3 Configuration limits 22
1.2.4 Rules for user names, roles and passwords 23
1.2.5 Replacing a module 24

1.3 Using the SOFTNET Security Client 26

1.4 Use of SCALANCE S602 27

1.5 Use of SCALANCE S612, S623 and S627-2M 30

1.6 Use of the DMZ interface of SCALANCE S623 and SCALANCE S627-2M 33

1.7 Use of the media module ports of a SCALANCE S627-2M 37

1.8 Use of the CP 343-1 Advanced and CP 443-1 Advanced 38

1.9 Use of CP 1628 41

1.10 Use of CP 443-1 OPC UA 43

1.11 Configuration and administration 44

2 Configuring with the Security Configuration Tool 45

2.1 Overview - Range of performance and how it works 45

2.2 Installation of the Security Configuration Tool 47
2.2.1 Supported operating systems 47

2.3 User interface and menu commands 49

2.4 Creating and managing projects 55
2.4.1 Security Configuration Tool (standalone variant) 55
2.4.2 Security Configuration Tool in STEP 7 56
2.4.3 Migrating STEP 7 data 60
2.4.4 Overview 61
2.4.5 Specifying general object properties 66
2.4.6 Specifying default initialization values for a project 66
2.4.7 Consistency checks 66
2.4.8 You can assign symbolic names for IP / MAC addresses. 67

2.5 Managing users 70
2.5.1 Overview of user management 70
2.5.2 Create users 72
2.5.3 Creating roles 73
2.5.4 Managing rights 75

2.5.5 Configuring password policies 80
2.5.6 Authentication using a RADIUS server 81
2.5.6.1 Overview 81
2.5.6.2 Defining a RADIUS server 83
2.5.6.3 Assigning a RADIUS server to a security module 84

2.6 Managing certificates 85
2.6.1 Overview 85
2.6.2 Renewing certificates 88
2.6.3 Replacing certificates 89

3 Creating modules and setting network parameters 91

3.1 Parameters in the content area 94

3.2 Configuring interfaces 96
3.2.1 Overview of the connector options 96
3.2.2 Interfaces 99
3.2.3 Internet connection 103
3.2.4 Dynamic DNS (DDNS) 105
3.2.5 LLDP 107
3.2.6 Media redundancy in ring topologies 107
3.2.6.1 Media redundancy with MRP or HRP 107
3.2.6.2 Configuring MRP/HRP for the security module 108
3.2.7 Special features of the ghost mode 110

4 Configure the firewall 115

4.1 CPs in standard mode 117
4.1.1 CP x43-1 Adv. 117
4.1.1.1 Default firewall setting 117
4.1.1.2 Configure the firewall 120
4.1.1.3 Configuring the access list 121
4.1.1.4 Adding an entry in the access list 122
4.1.2 CP 1628 123
4.1.2.1 Default firewall setting 123
4.1.2.2 Configure the firewall 126

4.2 SCALANCE S in standard mode 128
4.2.1 Default firewall setting 128
4.2.2 Configuring a firewall for SCALANCE S 133

4.3 Firewall in advanced mode 136
4.3.1 Configuring the firewall in advanced mode 136
4.3.2 Global firewall rule sets 137
4.3.2.1 Global firewall rule sets - conventions 139
4.3.2.2 Creating and assigning global firewall rule sets 139
4.3.2.3 Exporting and importing global firewall rule sets 140
4.3.3 User-specific IP rule sets 149
4.3.3.1 Creating and assigning user-specific IP rule sets 150
4.3.4 Connection-related automatic firewall rules 152
4.3.5 Setting local IP packet filter rules 154
4.3.6 IP packet filter rules 155
4.3.7 Defining IP services 161
4.3.8 defining ICMP services 162
4.3.9 Setting MAC packet filter rules 163

4.3.10 MAC packet filter rules 164
4.3.11 defining MAC services 168
4.3.12 Setting up service groups 170
4.3.13 Adjusting standard rules for IP services 171

5 Configuring additional module properties 173

5.1 Security module as router 173
5.1.1 Overview 173
5.1.2 Specifying a standard router and routes 174
5.1.3 NAT/NAPT routing 175
5.1.4 Address translation with NAT/NAPT 177
5.1.5 Address translation with NAT/NAPT in VPN tunnels 183
5.1.6 Relationship between NAT/NAPT router and firewall 186
5.1.7 Relationship between NAT/NAPT router and user-specific firewall 191

5.2 Security module as DHCP server 193
5.2.1 Overview 193
5.2.2 Configuring a DHCP server 193

5.3 Time-of-day synchronization 198
5.3.1 Overview 198
5.3.2 Configuring time-of-day synchronization 199
5.3.3 Defining an NTP server 200

5.4 SNMP 201
5.4.1 Overview 201
5.4.2 Enabling SNMP 202

5.5 Proxy ARP 203

5.6 Security module as OPC UA server/client 204
5.6.1 OPC UA authentication and encryption 204
5.6.2 Certificate validation 205
5.6.3 S7 communication 206

6 Secure communication in the VPN via an IPsec tunnel 209

6.1 VPN with security and SCALANCE M modules 209

6.2 Authentication method 212

6.3 VPN groups 213
6.3.1 Rules for forming VPN groups 213
6.3.2 Supported tunnel communication relations 214
6.3.3 Creating VPN groups and assigning modules 216

6.4 Tunnel configuration in standard mode 218

6.5 Tunnel configuration in advanced mode 218
6.5.1 VPN group properties 219
6.5.1.1 VPN connection establishment by Known Peers and Unknown Peers 219
6.5.1.2 Configuring VPN group properties 219
6.5.1.3 Examples of the configuration of VPN group properties 226
6.5.2 Including module in configured VPN group 229
6.5.3 Configuring module-specific VPN properties 230
6.5.4 Configuring VPN properties for specific connections 234

6.6 Configuration data for SCALANCE M modules 235

6.7 Configuration data for VPN devices 237

6.8 Configuration data for NCP VPN clients (Android) 240

6.9 Configuring internal network nodes 242
6.9.1 Configuring other nodes and subnets for the VPN tunnel 243
6.9.2 How the learning mode works 244
6.9.3 Displaying the detected internal nodes 247

7 Router and firewall redundancy 249

7.1 Overview 249

7.2 Creating redundancy relationships and assigning security modules 250

7.3 Configuring redundancy relationships 251

8 SOFTNET Security Client 253

8.1 Using the SOFTNET Security Client 253

8.2 Installation of the SOFTNET Security Client 256
8.2.1 Installing SOFTNET Security Client 256
8.2.2 Uninstalling SOFTNET Security Client 256

8.3 Creating a configuration file with the Security Configuration Tool 256

8.4 Main dialog of the SOFTNET Security Client 259

8.5 Loading the configuration file and setting up tunnel connections 260

8.6 Diagnosing and configuring a tunnel - "Tunnel Overview" dialog 261

8.7 Setting a managed configuration - "Manage users and groups" dialog 265

8.8 Run extended diagnostics - "Extended diagnostics" dialog 266

8.9 Accessing log files - "Log files" dialog 267

8.10 Activate Windows firewall rule - "Windows firewall parameter assignment" dialog 268

8.11 SOFTNET Security Client settings - "Settings" dialog 270

9 Online functions - diagnostics and logging 273

9.1 Overview of the functions in the online dialog 274

9.2 Logging events 276
9.2.1 Local logging - settings in the configuration 277
9.2.2 Network syslog - settings in the configuration 280
9.2.3 Configuring packet logging 283

A Appendix 287

A.1 DNS compliance 287

A.2 Range of values for IP address, subnet mask and address of the gateway 287

A.3 MAC address 288

B References 291

B.1 Introduction - without CD/DVD 291

B.2 S7 CPs / On configuring, commissioning and using the CP 292

B.3 For configuration with STEP 7 / NCM S7 292

B.4 S7 CPs On installing and commissioning the CP ... 293

B.5 On setting up and operating an Industrial Ethernet network ... 294

B.6 SIMATIC and STEP 7 basics ... 294

B.7 Industrial Communication Volume 2 ... 295

B.8 On the configuration of PC stations / PGs ... 295

B.9 On configuration of PC CPs ... 295

B.10 SIMATIC NET Industrial Ethernet Security ... 296

Index ... 297

Introduction and basics 1

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit
Link: (http://www.siemens.com/industrialsecurity)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
Link: (http://www.siemens.com/industrialsecurity).

1.1 Important information

General

Note

Protection from unauthorized access

Make sure that the configuration computer (PC/PG) or the project are protected from unauthorized access.

Note

Disabling the guest account

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

Note

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 and active 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 for the current project, you cannot switch back.

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

Note

Additional security measures when using the SOFTNET Security Client

The SOFTNET Security Client provides a solution for secure communication with automation cells via VPN. For self-protection of the PC/PG and the corresponding automation cell, it is advisable to use additional measures such as a virus scanner and the Windows firewall.

In Windows 7, the firewall of the operating system must be enabled so that VPN tunnel establishment works.

CP x43-1 Adv.

Note

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 (e.g. blocking S7 communication or only allowing 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.

Note

STEP 7 multiprojects in connection with security

For each multiproject in STEP 7 only one security configuration is supported.

Note

Logging off from the security project.

Logging off from the security project is achieved by closing HW Config. Closing the Security Configuration Tool within HW Config is not adequate.

1.2 Product characteristics

1.2.1 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 protected communication in industrial automation engineering.

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

- SCALANCE S
- CP x43-1 Adv.
- CP 443-1 OPC UA
- 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.

1.2.2 Overview of the functions

Overview of the functions of the module 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 443-1 OPC UA	CP 1628	SCALANCE S
Configuration using				
Security Configuration Tool	-	-	-	x
Security Configuration Tool integrated in STEP 7	x	x	x	x
Compatibility with IP access control lists (ACL)	x	-	-	-
General				
NAT/NAPT router	x	-	-	x
NAT/NAPT routing in VPN connections	-	-	-	x ~~S602~~ S≥V4.0
DHCP server	-	-	-	x
Firewall				
Local firewall rules	x	-	x	x
Global firewall rule sets	x	-	x	x
User-specific IP rule sets	-	-	-	x
IPsec				
Establishment of IPsec tunnels	x	-	x	x ~~S602~~
User management				
User management	x	x	x	x
Migration of the current user management	x	-	-	x
User authentication using a RADIUS server	-	-	-	x
Supported protocols				
SNMPv3	x	x	x	x
HTTPS server	x	x	-	x
FTPS server	x	-	-	-
FTPS client	x	-	-	-
NTP client	x	x	x	x
NTP client (secure)	x	x	x	x
PPPoE client	-	-	-	x
DDNS client / DNS client	-	-	-	x
LLDP	x	x	-	x S≥V4.0
MRP/HRP client	-	-	-	x S627-2M
Logging				
Logging system events	x	x	x	x

Function	CP x43-1 Adv.	CP 443-1 OPC UA	CP 1628	SCALANCE S
Logging audit events	x	x	x	x
Logging packet filter events	x	-	x	x
Audit messages in the diagnostics buffers of the security module	x	x	x	-
Access to the log buffer of the security module using the Security Configuration Tool	x	x	x	x
Diagnostics with the Security Configuration Tool	x	x	x	x
Sending messages to Syslog server	x	x	x	x
Web diagnostics	x	x	-	-
Ghost mode				
Obtaining the IP address of the internal node during runtime and adopting the IP address for the external port of the security module	-	-	-	x S602 ≥V3.1
Demilitarized zone (DMZ)				
Setting up a DMZ for separating the secure network from the non-secure network	-	-	-	x S62x
Router and firewall redundancy				
Redundant security modules for maintaining the router and firewall functionality if a security module fails	-	-	-	x S62x ≥ V4.0

x Function supported

- Function not supported

1.2.3 Configuration limits

Note

You will find a complete overview of the permitted configuration limits on the Internet at the following address: (https://support.industry.siemens.com/cs/us/en/view/58217657).

1.2.4 Rules for user names, roles and passwords

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	The following characters from the ANSI X 3.4-1986 character set are permitted: 0123456789 A...Z a...z !#$%&()*+,-./:;<=>?@ [\]_{|}~^
Characters not allowed	" ' ` §
Length of the user name (authentication method "password")	1 ... 32 characters
Length of the user name (authentication method "RADIUS")	1 ... 255 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	128 (122 user-defined + 6 system-defined)
Maximum number of roles on one security module	37 (31 user-defined + 6 system-defined)

Note

User names and passwords

As an important measure for increasing security, always make sure that user names and passwords are as long as possible and include special characters, upper and lowercase letters and numerals.

Using password policies, you can further narrow down the restrictions listed above for passwords. How to define password policies is described in the section:
Configuring password policies (Page 80)

Password strength

When a new password is entered, its password strength is checked. The following levels are distinguished for the password strength:

- Very weak
- Weak
- Medium
- Good
- Strong
- Very strong

Note

Checking the password strength of existing users

Check the password strength

- of users already in the project,
- of the first user created in STEP 7,
- of migrated users,

by selecting the relevant user in the "User" tab of the user management and clicking the "Edit..." button.

1.2.5 Replacing a module

~~CP~~

How to access this function

1. Select the security module or the SOFTNET Security Client to be edited.
2. Select the "Edit" > "Replace module…" menu command.
3. Depending on the product type and the firmware release 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 CPs

You will find information about replacing CPs in the relevant device manual.

Initial module	Possible module replacement						
	S602 V3	S602 V4	S612 V3	S612 V4	S623 V3	S623 V4	S627-2M V4
S602 V2	x	x	x	x	x	x	x
S602 V3	-	x	!	!	!	!	!
S602 V4	!	-	!	!	!	!	!
S612 V1	!	!	x	x	x	x	x
S612 V2	!	!	x	x	x	x	x
S612 V3	!	!	-	x	x	x	x
S612 V4	!	!	!	-	x	x	x
S613 V1	!	!	x	x	x	x	x
S613 V2	!	!	x	x	x	x	x
S623 V3	!	!	!	!	-	x	x
S623 V4	!	!	!	!	!	-	x
S627-2M V4	!	!	!	!	!	!	-

x Without losses

! Possibly with losses

- The module type and the firmware version are not changed.

Initial configuration	Possible replacement			
	SOFTNET Security Client 2005	SOFTNET Security Client 2008	SOFTNET Security Client V3.0	SOFTNET Security Client V4.0
SOFTNET Security Client 2005	-	x	x	x
SOFTNET Security Client 2008	x*	-	x	x
SOFTNET Security Client V3.0	x* **	x**	-	x
SOFTNET Security Client V4.0	x* **	x**	x	-

***** If the SOFTNET Security Client is not in a routing group.

****** If the SOFTNET Security Client is not in a VPN group along with a SCALANCE M module.

See also

User interface and menu commands (Page 49)

/2/ (Page 292)

1.3 Using 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.

1.4 Use of 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 module protects individual devices or even entire automation cells from:

- Data espionage
- Unwanted access

SCALANCE S602 allows this protection flexibly and without complicated handling.

SCALANCE S602 is configured with the Security Configuration Tool.

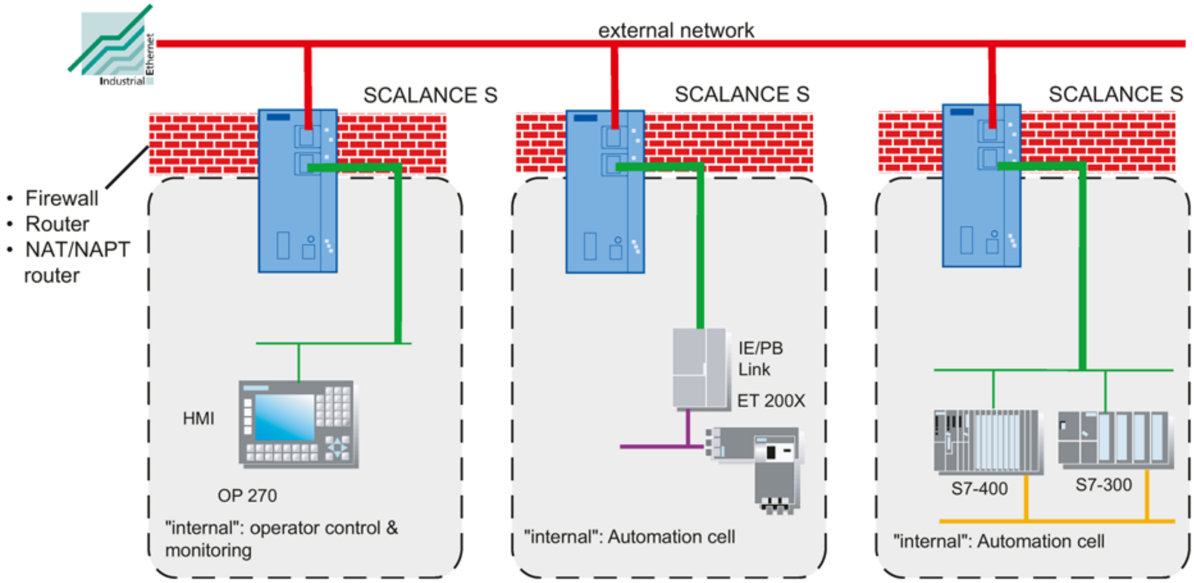


Figure 1-1 Network configuration with SCALANCE S602

Security functions

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

    (Layer 2 frames: does not apply if router mode is used);
  - Bandwidth limitation
  - Global firewall rule sets
  - User-specific IP rule sets

  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.
- Security module and internal node as one unit (ghost mode)

  When communicating with external stations, the security module uses the IP address of the internal node and the MAC address of the security module.
- NTP (secure) S≥V4.0

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

  Point-to-Point Protocol over Ethernet (RFC 2516) for obtaining IP addresses automatically from the provider so that the use of a separate DSL router is not necessary.
- User authentication using a RADIUS server S≥V4.0

  User names, passwords and roles of users can be stored centrally on a RADIUS server. These users are then authenticated by a RADIUS server.
- SNMPv3

  For secure transmission of network analysis information safe from eavesdropping.

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.

Note

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!

1.5 Use of SCALANCE S612, S623 and S627-2M

All-round protection - the job of SCALANCE S612, SCALANCE S623 and SCALANCE S627-2M

With a combination of different security measures such as firewall, NAT/NAPT routers and VPN (Virtual Private Network) via IPsec tunnels, the security modules SCALANCE S612, SCALANCE S623 and SCALANCE S627-2M protect individual devices or even entire automation cells from:

- Data espionage
- Data manipulation
- Unwanted 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.

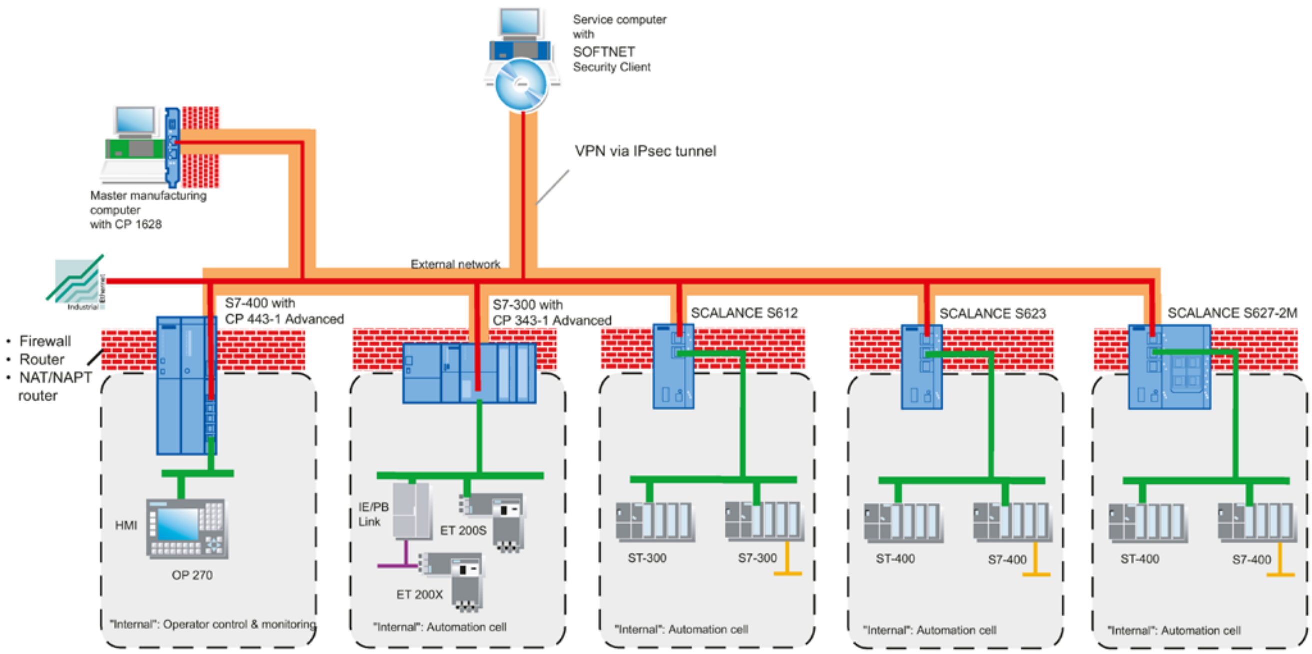

Service computer with SOFTNET Security Client
VPN via IPsec tunnel
Master manufacturing computer with CP 1628
External network
Industrial Ethernet
• Firewall
• Router
• NAT/NAPT router
S7-400 with CP 443-1 Advanced
S7-300 with CP 343-1 Advanced
SCALANCE S612
SCALANCE S623
SCALANCE S627-2M
HMI
OP 270
"Internal": Operator control & monitoring
IE/PB Link
ET 200S
ET 200X
"Internal": Automation cell
ST-300
S7-300
"Internal": Automation cell
ST-400
S7-400
"Internal": Automation cell
ST-400
S7-400
"Internal": Automation cell

Figure 1-2 Network configuration with SCALANCE S612, SCALANCE S623 and SCALANCE S627-2M

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; not available if router mode is used)
  - Bandwidth limitation
  - Global firewall rule sets
  - User-specific IP rule sets

  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 these security modules 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 packets 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.

- Client for dynamic DNS (DDNS client)

  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 in conjunction with the SOFTNET Security Client, SCALANCE M modules, SCALANCE S modules or other VPN clients.

- 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 interface S62x

  In a demilitarized zone (DMZ), servers can be placed for which access to other networks (non-secure external network, secure internal network) can be controlled and restricted.

This means that the two networks can have services and data made available securely without the two networks having direct communication between them.

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

- User authentication using a RADIUS server S≥V4.0

  User names, passwords and roles of users can be stored centrally on a RADIUS server. These users are then authenticated by a RADIUS server.

- NTP (secure) S≥V4.0

  For secure time-of-day synchronization and transmission.

Internal network nodes, external network nodes, DMZ network nodes

SCALANCE S divides networks into several areas:

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

  Internal nodes are all 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.

- DMZ network: Protected areas with the "DMZ nodes" S62x

  DMZ nodes are all nodes located in the DMZ and secured by a SCALANCE S.

Note

The networks connected to the internal interface are considered as being secure (trustworthy).

Connect an internal network segment with network segments with a different security level (external network, DMZ network) only via SCALANCE S.

There must be no other connection paths between the internal network and a network with a different security level.

1.6 Use of the DMZ interface of SCALANCE S623 and SCALANCE S627-2M

Scenarios for the use of the DMZ interface

In addition to the functions of the SCALANCE S612, the SCALANCE S623 and SCALANCE S627-2M are equipped with a third interface (DMZ) to which a additional network can be connected.
Depending on the various scenarios for its use, the interface can provide a variety of functions (not at the same time):

- Setting up a DMZ
- Endpoint for VPN tunnel connection
- Synchronization interface for router and firewall redundancy
- ...

Setting up a DMZ

With the SCALANCE S623 and the SCALANCE S627-2M, a DMZ (Demilitarized Zone) can be set up on the additional interface. The DMZ is often used when services for an insecure network need to be available and the secure network that supplies data for these services needs to remain separated from the insecure network.

The DMZ, for example, can include terminal servers with installed maintenance and diagnostic software which can be used by authorized users from the external network.

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).

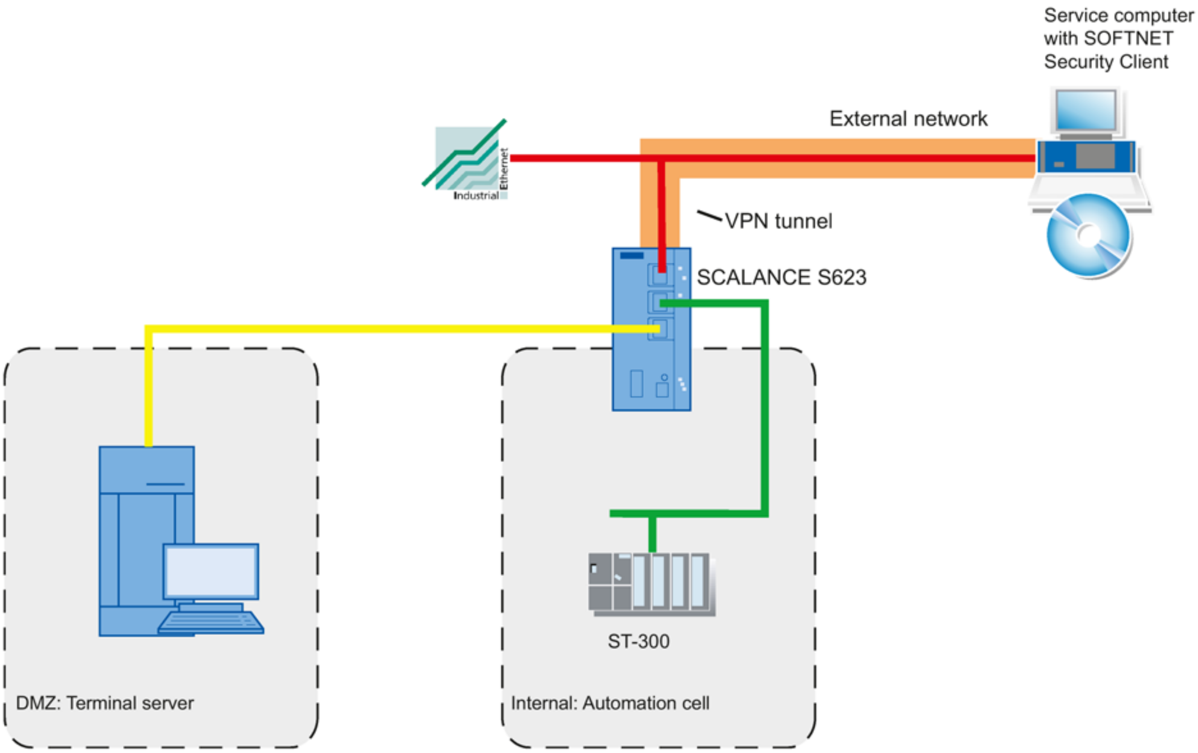


Figure 1-3 Setting up a DMZ

An example of a configuration in which the DMZ interface is used to set up a DMZ can be found in section "4.2 SCALANCE S as firewall between external network and DMZ" of the "SIMATIC NET Industrial Ethernet Security - Getting started" manual.

Endpoint for VPN tunnel connection

The DMZ interface can be used as the endpoint of a VPN tunnel. In this scenario, the DMZ interface is connected to the Internet via a connected DSL modem and is operated using PPPoE. The VPN tunnel allows secure communication with, for example, an automation unit connected to the internal port of another security module.

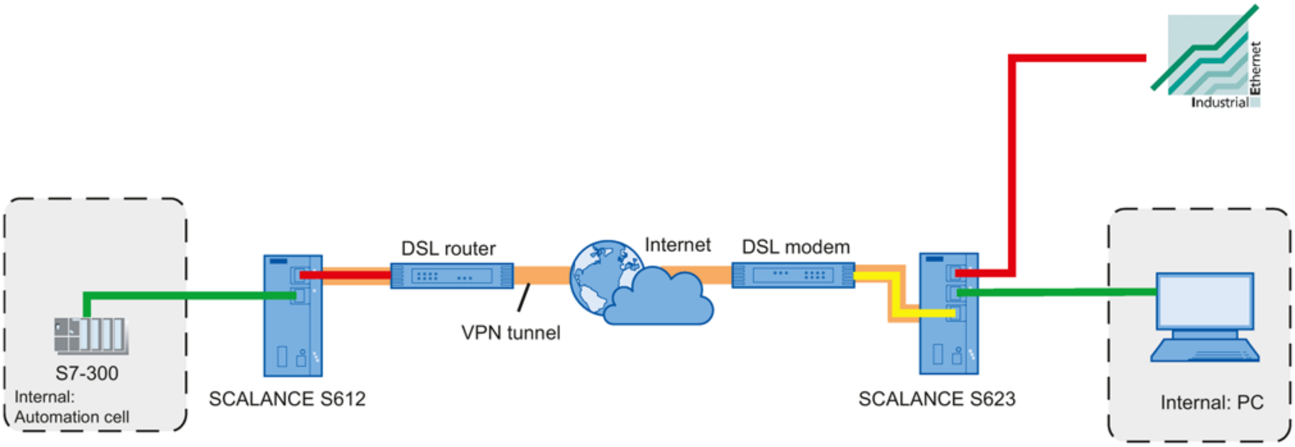


Figure 1-4 Endpoint for VPN tunnel connection

An example of a configuration in which the DMZ interface is used as the end point of a VPN tunnel can be found in section "5.2 VPN tunnel between SCALANCE S623 and SCALANCE S612" of the "SIMATIC NET Industrial Ethernet Security - Getting started" manual.

Synchronization interface for router and firewall redundancy S62x ≥ V4.0

When using two security modules of the type SCALANCE S623 or SCALANCE S627-2M, the failure of one security module can be compensated by router and firewall redundancy. Here, both security modules are operated in routing mode and connected to the external and internal network but only one security module is active at one time. If the active security module fails, the passive security module takes over its function as router or firewall. To ensure the identical behavior of both security modules, the two security modules are connected together via their DMZ interfaces and their configurations are synchronized during operation. In this case, the DMZ interfaces of the security modules involved cannot be used for other purposes.

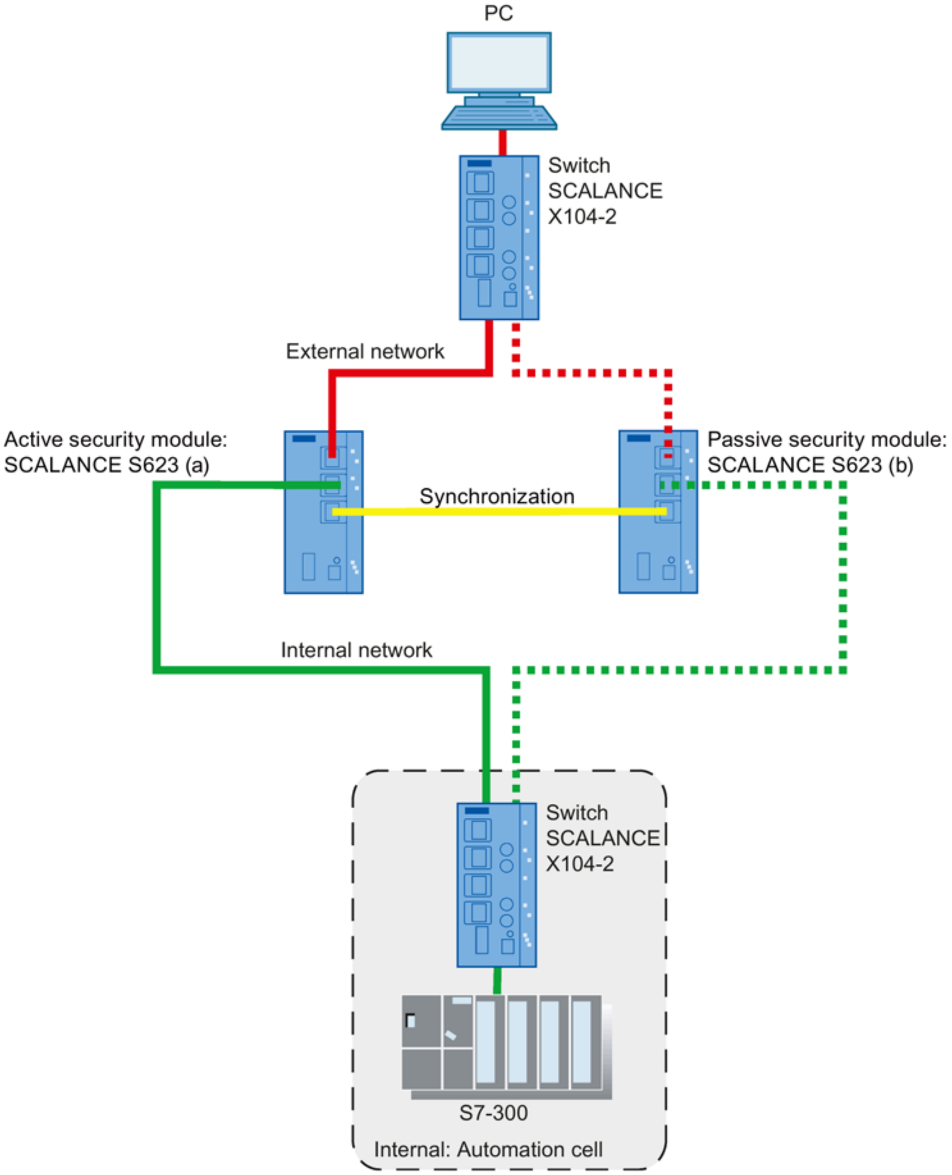


Figure 1-5 Router and firewall redundancy

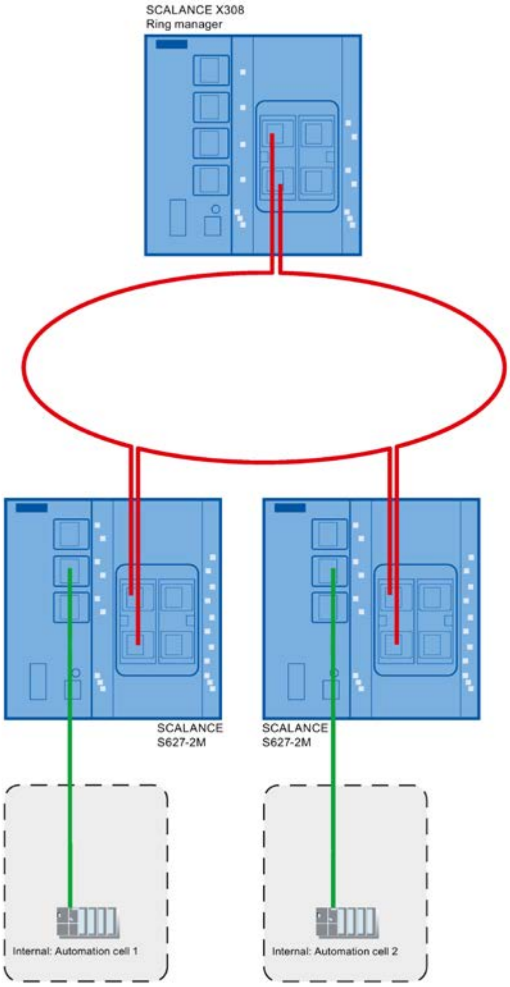
1.7 Use of the media module ports of a SCALANCE S627-2M

Integration in ring topologies

In addition to the functions of the SCALANCE S623, the SCALANCE S627-2M has two media module slots in which an electrical or optical media module with two ports can be inserted. This expands both the external and internal interface by up to two ports. In routing mode, the additional ports of the security module can be used to link the external and internal interface to ring topologies.

Ring redundancy with MRP or HRP

The SCALANCE S627-2M supports the MRP and HRP protocols on the media module ports of the external and internal interface as client. As a node of an MRP/HRP ring, a SCALANCE S627-2M can protect a lower-level automation cell or a lower-level ring. This protection can also be redundant. The loss of cables is detected by a separate ring manager, for example a SCALANCE X308, and compensated by redirecting the communication path.



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
- Unwanted access

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

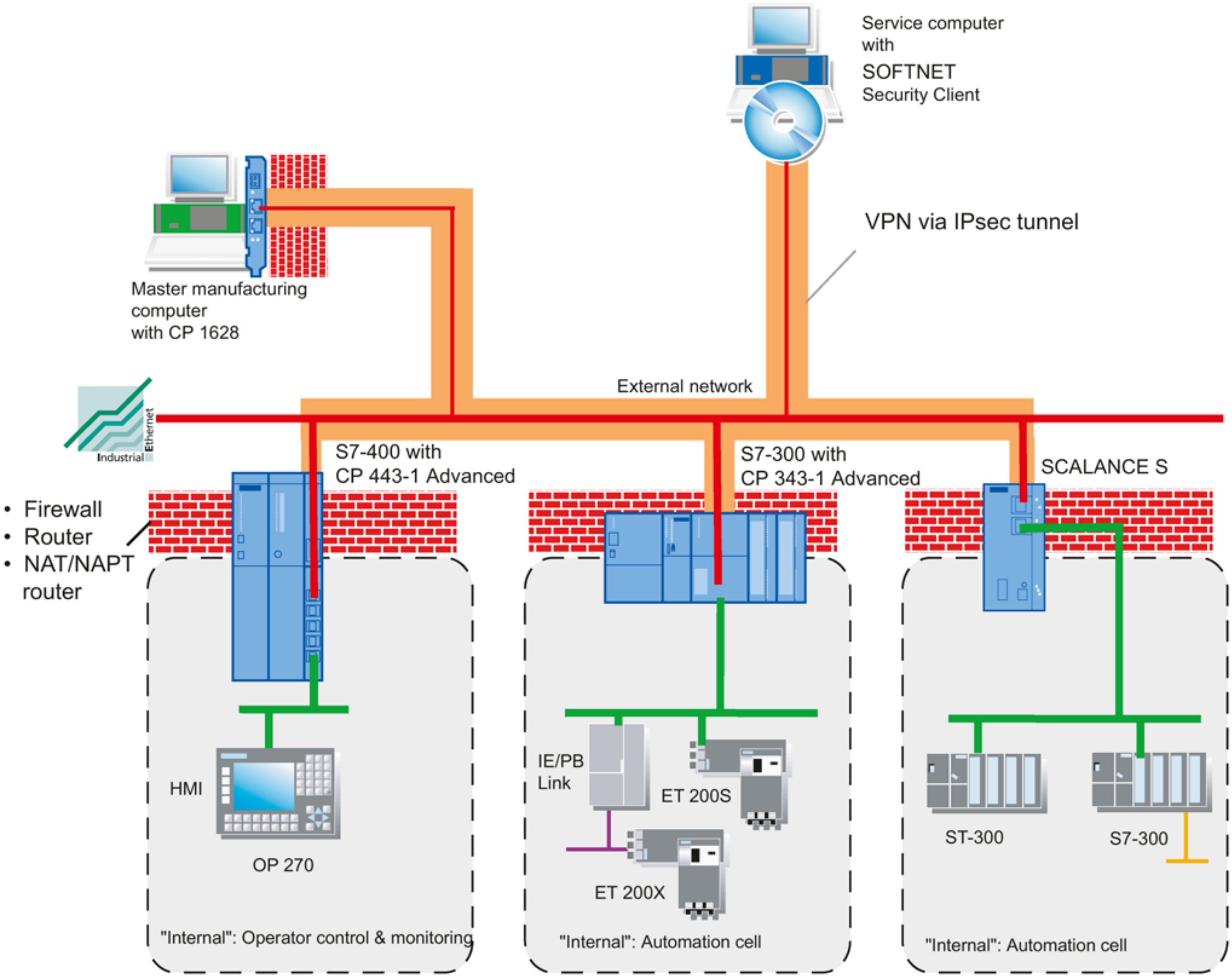


Figure 1-6 Network configuration with CP x43-1 Adv.

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 rule sets

  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 VPN group. 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.
- FTPS

  For encrypted transfer of files.
- NTP (secured)

  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.

Note

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 292)
- /2/ (Page 292)

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
- Unwanted access

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

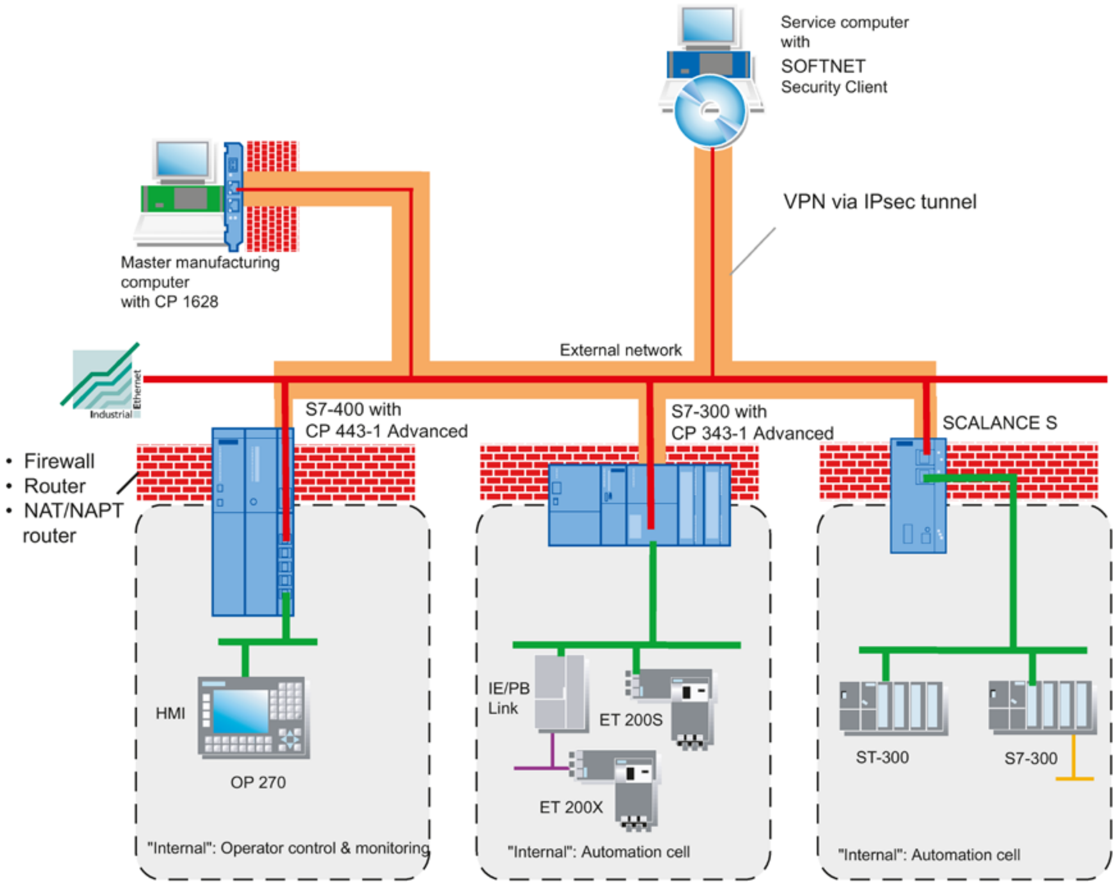


Figure 1-7 Network configuration with CP 1628

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).
- 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.
- NTP (secured)

  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 295)

1.10 Use of CP 443-1 OPC UA

Via its Ethernet interface (1 x RJ-45), the CP 443-1 OPC UA provides the function of an OPC UA client and an OPC UA server. The following security functions are available:

- NTP (secure)

  For secure transfer during time-of-day synchronization

- SNMPv3

  For secure transmission of network analysis information safe from eavesdropping

- Authentication using certificates

  Authentication of the OPC UA server with connected OPC UA client and of the client with the communications partner using certificates.

  The checking of the certificates of the communications partner exchanged during authentication can be set to different levels for the server and client function.

  The CP supports the security profiles of the Specification part 2, 4, 6, 7 and 12 of the OPC Foundation.

- Encryption

  The encryption of the OPC UA data can be configured for the following security profiles of the OPC UA Specification:

  - No security profile
  - Basic128Rsa15
  - Basic256
  - Basic256Sha256

- Write protection

  You can block write access to the data area of the CPU.

- Protection of access to diagnostics data and to the backplane bus

  You can block S7 routing via the backplane bus of the CP and access to diagnostics data of the CP via NCM diagnostics.

- 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.

- User management

  In the user management, you assign a role to individual users. The individual roles provide specific rights to various services.

1.11 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 advanced 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 ~~PC CP~~

  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 sections 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 Overview - Range of performance and how it works

Scope of performance

You use the Security Configuration Tool for the following tasks:

- Configuration of the security modules
- Configuration of SOFTNET Security Client
- Creating VPN configuration data for SCALANCE M / SCALANCE S615
- Creating VPN configuration files for VPN devices and software from third-party manufacturers
- Test and diagnostic functions, status displays

Two modes of the Security Configuration Tool

The Security Configuration Tool can be called up in the following 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:
  - Can only be called up from STEP 7
  - There must be at least one CP in the project with the security function activated.
  - The range of the Security Configuration Tool standalone is expanded by the option of configuring security functions for CPs

Offline configuration view and online diagnostics view

The Security Configuration Tool has an offline configuration view and an online diagnostics view:

- Offline configuration view

  In offline mode, the configuration data is created for the relevant module. Prior to downloading, there must already be a connection to this module.
- Online

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

Two operating modes

The Security Configuration Tool provides two operating modes in the offline configuration view:

- 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

  In Advanced mode, there are further optional settings, for example that allow individual setting of firewall rules, log settings, NAT/NAPT rules, VPN nodes and expanded security functionalities.

How it works - security and consistency

- Access only for authorized users

  Every project is protected from unauthorized access by assigning user names and passwords. With the help of password policies, project-specific rules for password assignment can be defined.
- 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, if it exists, on the C-PLUG (not for the CP 1628 and CP 443-1 OPC UA).

2.2 Installation of the Security Configuration Tool

2.2.1 Supported operating systems

Supported operating systems

The following operating systems are supported:

- Microsoft Windows 7 Professional / Enterprise / Ultimate SP1 x64
- Microsoft Windows 10 Professional / Enterprise Version 1607 x64
- Microsoft Windows 10 Enterprise 2015 LTSB
- Microsoft Windows Server 2008 R2 Standard SP1 x64
- Microsoft Windows Server 2012 R2 Standard x64
- Microsoft Windows Server 2016 x64

Note

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

SCALANCE S - follow the steps below

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

- Insert the product DVD in your DVD ROM drive. If the Autorun function is enabled, the user interface is started automatically from where you can perform the installation.

or

- Start the "start.exe" application on the supplied product S DVD.

CP x43-1 Adv. and CP 443-1 OPC UA - Follow the steps below

You install the Security Configuration Tool from the STEP 7 data medium. You will find the installation file on the STEP 7 data medium in the directory for optional software components.

CP 1628 - Follow the steps below

You install the Security Configuration Tool from the supplied data medium containing the driver data of the CP 1628.

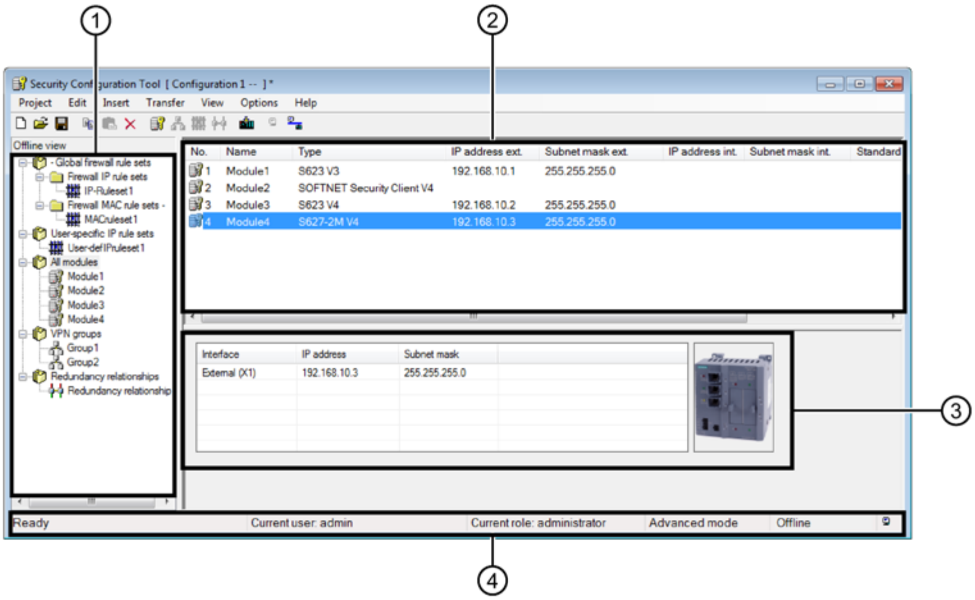
- Insert the data medium in your DVD drive. If the Autorun function is enabled, the user interface is started automatically from where you can perform the installation.

or

- Start the "start.exe" application on the supplied data medium.

2.3 User interface and menu commands

Structure of the user interface in advanced mode



No.	Name	Type	IP address ext.	Subnet mask ext.	IP address int.	Subnet mask int.	Standard
1	Module1	S623 V3	192.168.10.1	255.255.255.0			
2	Module2	SOFTNET Security Client V4					
3	Module3	S623 V4	192.168.10.2	255.255.255.0			
4	Module4	S627-2M V4	192.168.10.3	255.255.255.0			

Interface	IP address	Subnet mask
External (X1)	192.168.10.3	255.255.255.0

① Navigation panel:

- Global firewall rule sets ~~CP 443-1 OPC UA~~

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

  – Firewall IP rule sets

  – Firewall MAC rule sets

- User-specific IP rule sets SCA. S
- All modules

  The object contains all the configured modules and SOFTNET configurations of the project.

- VPN groups ~~CP 443-1 OPC UA~~

  The object contains all generated VPN groups.

- Redundancy relationships S≥V4.0

  The object contains all generated redundancy relationships of the project.

② Content area:

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

For some of the security modules, you can see and adapt excerpts of the interface configurations in this area.

Assuming that they provide corresponding configuration options, by double-clicking on the security modules, you open properties dialogs where you can enter further parameters.

③ Details window:

The Details window contains additional information about the selected object and allows the configuration of VPN properties for specific connections in the relevant context of a VPN group.

The Details window can be hidden and shown using the "View" menu.

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 panel in the "All modules" folder.
🖧	Create new VPN group. The symbol is only active if you are located in the navigation panel in the "VPN groups" folder.
▦	Create a new global IP rule set / MAC rule set or user-specific IP 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.
⇹	Create new redundancy relationship. The symbol is only active if you are located in the navigation panel in the "Redundancy relationships" folder.
⬇	SP Download the configuration to the selected security modules or create configuration data for SOFTNET Security Client / SCALANCE M / VPN device / NCP VPN client (Android).

Symbol	Meaning / remarks
🖥	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.	Ctrl + S
~~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.	
	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
	Import rule sets...	Import global firewall rule sets already exported as .XLSX files in to SCT	
	Export rule sets...	Export selected global firewall rule sets from SCT as XLSX files	
	Delete	Delete the selected object.	Del
	Rename	Rename the selected object.	F2
	New certificate...	Generate a new group certificate for a module selected in the content area after selecting the appropriate VPN group.	
	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.	
Insert ▸…		Menu commands only in offline mode	

Menu command		Meaning / remarks	Keyboard shortcut
	Module	Create new security module. The menu command is enabled only when a module object or a VPN group is selected in the navigation panel.	Ctrl + M
	Group	Create new VPN group. The menu command is enabled only when a group object is selected in the navigation panel.	Ctrl + G
	Firewall rule set	Create a new global firewall IP rule set, MAC rule set or user-specific IP rule set. The menu command is enabled only when a firewall object is selected in the navigation panel. The menu command is only visible in advanced mode.	Ctrl + F
	Redundancy relationship	Create new redundancy relationship. The menu command is only active if you are located in the navigation panel in the "Redundancy relationships" folder.	Ctrl + R
Transfer ▸...		**Note** When an object is selected, you can also activate some of the functions in the shortcut menu.	
SP	To module(s)...	Download the configuration to the selected security module(s) or create configuration data for SOFTNET Security Client / SCALANCE M / VPN devices / NCP VPN clients (Android). 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...	The configuration status of the configured security modules is shown in a list.	
SP	Transfer firmware ...	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.	

Menu command		Meaning / remarks	Keyboard shortcut
SCA. S ~~S602~~ VPN device	Exporting SINEMA RC files...	For the selected SCALANCE S module or the selected VPN device, a JSON file is exported. This JSON file contains the VPN properties of the selected module and can be used to configure SINEMA Remote Connect. The use of the JSON file simplifies the replacement of a SCALANCE S module or a VPN device by a SINEMA Remote Connect server in a VPN infrastructure. If the authentication method "Certificate" was configured for one of the VPN groups in which the selected SCALANCE S module is located, prior to exporting you need to specify a password for the PKCS12 archive. The following requirements must be met for the export: • Precisely one SCALANCE S module or precisely one VPN device was selected. • The SCALANCE S module or the VPN device is in at least one VPN group. • The SCALANCE S module or the VPN device is in routing mode.	
View ▸…			
	Advanced mode	Switch over from the standard (default) to the advanced mode. **Note** If you switch to the advanced mode for the current project, you cannot switch back.	Ctrl + E
	Show Details window	Show and hide additional details about the selected object.	Ctrl + Alt + D
	Offline	Default. Switch over to the offline configuration view.	Ctrl + Shift key + D
	Online	Switch over to the online diagnostics view.	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.	
~~CP~~	Network adapter...	The SCALANCE S is assigned an IP address via the selected network adapter.	

Menu command		**Meaning / remarks**	**Keyboard shortcut**
	Language...	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.	
	Configuration of the NTP servers...	Create and edit NTP servers.	
	Configuration of the RADIUS servers...	Create and edit RADIUS servers.	
	Consistency check...	Check the consistency of the entire project. The result is output in the results list.	
	User management...	Create and edit users and roles, assign rights and define password policies.	
	Certificate manager...	Display or import / export certificates.	
Help ▸...			
	Contents...	Help on the functions and parameters in the SCT.	F1
	About...	Information on the version and revision of the SCT.	

2.4 Creating and managing projects

2.4.1 Security Configuration Tool (standalone variant)

~~SP~~

Configuration with the Security Configuration Tool standalone

The Security Configuration Tool standalone variant 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, VPN devices and NCP VPN clients (Android). For each device or for each configuration, you create a module in the project.

2.4.2 Security Configuration Tool in STEP 7

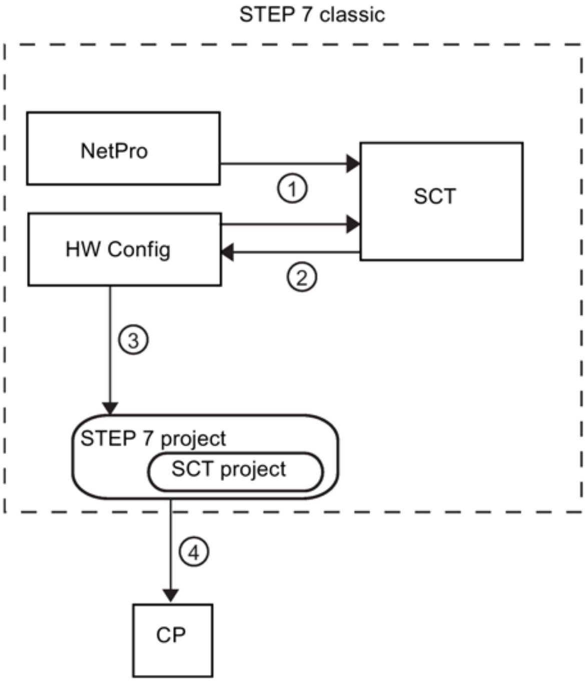
Project engineering

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 standalone 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. ~~CP 443-1 OPC UA~~

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
- IP address PROFINET IO
- IP address Bit
- IP address OPC UA
- Subnet mask PROFINET IO
- Subnet mask Gbit
- Subnet mask OPC UA
- MAC address PROFINET IO
- MAC address Gbit
- MAC address OPC UA
- Standard router

Which data can be migrated to SCT and modified there?

The following functions used in STEP 7 can be migrated to SCT and edited there:

- Access control lists (Page 121)
- Users (Page 70)
- NTP server (Page 198)

HLP F1

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 configured connections

~~CP 443-1 OPC UA~~

With specified connections configured in STEP 7, firewall rules are automatically created in SCT that allow connection establishment. For more detailed information, refer to the following section:

- Connection-related automatic firewall rules (Page 152).

With unspecified connections, you need to configure firewall rules that allow connection establishment in SCT. For more detailed information, refer to the following section:

- Firewall in advanced mode (Page 136).

Making security settings in STEP 7

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 STEP 7 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 online ~~CP 443-1 OPC UA~~	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.
~~CP 443-1 OPC UA~~	User	Start of user management	Starts the SCT user management in which users and roles can be created and rights assigned.
~~PC CP~~ ~~CP 443-1 OPC UA~~	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	
	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.
CP 443-1 OPC UA	OPC UA	Start of the OPC UA security setting	Opens the SCT dialog for configuration of the security functions of the server application.

- 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 294).

2.4.3 Migrating STEP 7 data

~~CP 443-1 OPC UA~~

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 the 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.

Note

The users and their roles can be adapted after migration in the user management of the Security Configuration Tool.

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	
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	

See also

Time-of-day synchronization (Page 198)

Configuring the access list (Page 121)

2.4.4 Overview

General contents

Both in the standalone version of the Security Configuration Tool, as well as in the version integrated in STEP 7, you will be prompted to assign a user name and a password when creating a new project. The user you create here is of the type "administrator". After making this entry, you can create the configurations in the project.

Generally, the configurations of a project contain the following:

- Valid settings throughout the project
- Module-specific settings
- Group assignments for IPsec tunnel ~~S602~~ ~~CP 443-1 OPC UA~~

User management also handles access rights to the project data and 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 ~~CP 443-1 OPC UA~~

  A global firewall rule set can be assigned to several modules at the same time. In many situations, this simplifies the configuration compared with configuring local firewall rules in the settings for specific modules.

- User-specific IP rule sets SCA. S

  A user-specific IP rule set is assigned to a user and a security module. A SCALANCE S V4 module can also be assigned a user-specific IP rule set to which a role is assigned.

  User-specific IP rule sets allow the definition of highly detailed user-specific access rights.

- Redundancy relationships S62x ≥ V4.0

  A redundancy relationship is created for two security modules. If one of the two security modules fails during operation, the other security module takes over its function as firewall and (NAT/NAPT) router.

- MRP domains S627-2M

  The members of an MRP ring are specified with the help of MRP domains. The same MRP domain must be selected for the interfaces of all modules to be connected to an MRP ring.

- Service definitions ~~CP 443-1 OPC UA~~

  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.

- RADIUS server S≥V4.0

  RADIUS servers are created throughout the project and can then be assigned to several security modules in SCT.

- Certificate manager

  All the certificates of the project and the security modules it contains are managed in the certificate management.

- User management

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

- Symbolic names

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

Module-specific settings

Most of the functions are configured in the tabs of the properties dialog that can be called up for a selected security module with the command "Edit" > "Properties...". In the properties dialog, the individual tabs can be arranged as required by dragging them with the mouse. The following table contains the functional descriptions of the individual tabs.

	Function / tab in the properties dialog	Specified in mode ...	
		Standard	Advanced
	Interfaces Overview of the individual interface and port settings. For CPs: The settings are taken from STEP 7 and cannot be modified.	X	X
~~CP 443-1 OPC UA~~	**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
SCA. S	**Internet connection** If you have set a connection using PPPoE, make the settings for the Internet Service Provider here.	X	X
SCA. S	**DNS** Settings related to dynamic DNS permitting access to continuously changing IP addresses via fixed defined names (FQDN). Dynamic DNS is permitted on the external interface and on the DMZ interface.	-	X
~~CP~~	**Routing** Here, enter the data for the standard router and/or specify a subnet-specific 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
~~PC CP~~ ~~CP 443-1 OPC UA~~	**NAT/NAPT** Enable NAT/NAPT functionality and specify the address translation in a list.	-	X
	Time-of-day synchronization Here, you specify the type of synchronization for the date and time. For CPs: Time-of-day synchronization can only be configured in SCT if the expanded NTP configuration was enabled in STEP 7.	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

	Function / tab in the properties dialog	Specified in mode ...	
		Standard	Advanced
~~S602~~ ~~CP 443-1 OPC UA~~	**VPN** If the security module is in a VPN group, here you can configure dead peer detection, the type of connection establishment and, if applicable, a WAN access point (IP address or FQDN) and the response of the VPN responder to road warriors. Depending on the security module, in the "VPN nodes" dialog area you make additional settings for subnets, IP/MAC nodes and NDIS nodes that should also be reachable via the VPN tunnels. For SCALANCE S: The learning of internal nodes can be enabled or disabled. The dialog areas "Settings for responders" and "VPN nodes" can only be edited if the project is in advanced mode.	X	X
~~SP~~	**DHCP server** For the internal network and the DMZ network (SCALANCE S623/S627-2M only), you can use the security module as a DHCP server.	-	X
	SNMP In this tab, set the SNMP protocol version and the authentication/encryption method.	X	X
SCA. S ~~S602~~	**Proxy ARP** In this tab, make static entries for proxy ARP on the external interface.	-	X
S627-2M	**MRP/HRP** In this tab, select the parameters for connecting the security module to MRP/HRP rings.	X	X
S≥V4.0	**RADIUS** In this tab, assign a RADIUS server to the security module that will authenticate users when activating user-specific IP rule sets instead of the security module.	X	X

Group assignments for an IPsec tunnel

~~S602~~

~~CP 443-1 OPC UA~~

VPN groups specify which security modules, SOFTNET Security Clients and SCALANCE M modules, VPN devices and NCP VPN clients (Android) communicate with each other via an IPsec tunnel.

By assigning these network nodes to a VPN group, you can establish a VPN (Virtual Private Network) communications tunnel.

Only modules of the same VPN group can communicate securely via tunnels, however the modules can belong to several VPN groups at the same time.

See also

Configuring additional module properties (Page 173)

2.4.5 Specifying general object properties

How to access this function

Menu command: "Project" > "Properties..." > "General" tab.

Settings for project and author

In this dialog, make informal entries about your security project and about the author of the configuration. Some of the entries are displayed in the online diagnostics and used during the transfer of management information using the Simple Network Management Protocol (SNMP).

2.4.6 Specifying default initialization values for a project

~~CP~~

Specifying default initialization values for a project

With the default initialization values, you specify the properties to be adopted when you create new modules. Using the "Save selection" check box, you can also specify whether a window for setting the properties is opened when you create a new module or whether the module will 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).

2.4.7 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. With the following actions, there is automatically a consistency check through the entire project:

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

Note

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 result of the check is displayed in a list that you can filter according to the message types "Errors" or "Warnings". 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.

2.4.8 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
- NTP

Forming symbolic names

Both when defining and using symbolic names, they must be preceded by a hash character (#). The symbolic names themselves must be DNS-compliant.

Validity and uniqueness

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

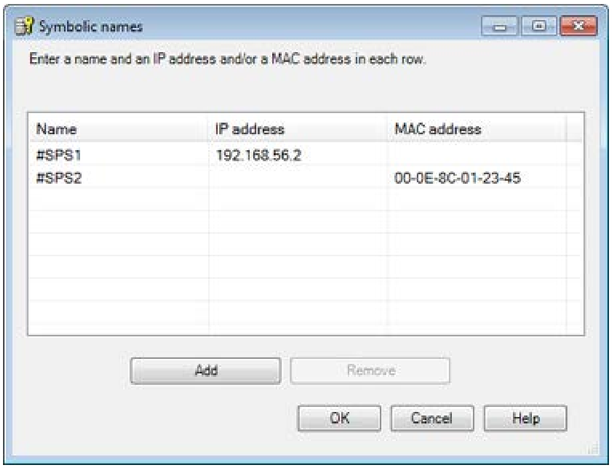
Each symbolic name must be assigned uniquely to a single IP address and/or MAC address within the project.

Dialog for defining 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.

Defining symbolic names

1. Click the "Add" button to add a new symbolic name in the next free table row.
2. Enter the hash character (#) followed by the required, DNS-compliant symbolic name.
3. Add the IP address and/or the MAC address to the entry.



Enter a name and an IP address and/or a MAC address in each row.

Name	IP address	MAC address
#SPS1	192.168.56.2	
#SPS2		00-0E-8C-01-23-45

Using undefined symbolic names

During the configuration of security modules, you can also use symbolic names that have not yet been defined. After entering a symbolic name that has not yet been defined and confirming the corresponding dialog, the selected symbolic name is added to the table of symbolic names. In this dialog, you can then specify the corresponding IP address and/or MAC address for the symbolic name.

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 regardless of whether or not you defined the symbolic name later.

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:

- Symbolic names must be preceded by a hash character (#).
- 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.
- The symbolic names must be DNS-compliant.
- A symbolic name must be assigned either an IP address or a MAC address or both.

- No symbolic names may be assigned to the IP addresses of the security modules.
- 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.

See also

Consistency checks (Page 66)

DNS compliance (Page 287)

2.5 Managing users

2.5.1 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 22).

Migrating existing users from STEP 7 to SCT

~~CP 443-1 OPC UA~~

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.

Note

Make sure that you keep your user passwords safe.

If you forget your user passwords, you can no longer access the relevant project or the security module involved.

In this case, you need to create a new project and reset to factory defaults. You will, however, lose the configuration.

Note

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 security modules.

User authentication when activating user-specific IP rule sets SCA. S

Users that log on to the Web page of the security module to activate a user-specific IP rule set, can be authorized either by the security module or for SCALANCE S as of V4 by a RADIUS server.

How you specify a user for the "RADIUS" authentication method is described in the next section:

- Create users (Page 72)

You will find more detailed information on user authentication by the RADIUS server in the following section:

- Authentication using a RADIUS server (Page 81)

2.5.2 Create users

How to access this function

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

STEP 7 menu command: ~~CP 443-1 OPC UA~~
"Users" > "Start of user administration", "Run" button. The user administration can also be called up from individual tabs.

Parameter	Meaning
User name	Freely selectable user name.
Authentication method	• **Password**: Use this authentication method for users that edit and download the SCT project and that are intended to run diagnostics on the security module. The authentication of the user is performed by the security module when user-specific IP rule sets are activated. • **RADIUS** S≥V4.0 : The authentication of the user is performed by a RADIUS server when user-specific IP rule sets are activated. The password of the user is not configured in SCT when using this authentication method but must be stored on the RADIUS server. Only use this authentication method for users that only need to log on to the Web page of a security module. A user with the "RADIUS" authentication method cannot log on to SCT projects.
Password (only with the "Password" authentication method)	Entry of the password for the user. When it is entered, the password strength is checked. For more detailed information on password strength, refer to the following section: Rules for user names, roles and passwords (Page 23)
Repeat password (only with the "Password" authentication method)	Repeat the entered password.
Comment	Entry of additional comments.
Maximum time of the session SCA. S	Entry of the time after which a user logged on to the Web page for user-specific IP rule sets of SCALANCE S modules is automatically logged off. The time entered here starts after the logon and after renewing the session on the Web page of the security module. • Default setting: 30 minutes • Minimum value: 5 minutes • Maximum value: 480 minutes
Assigned role	Depending on the assignment made.

Table 2- 1 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 settings listed above.
Add...	With this button, you can add a new user.
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.

2.5.3 Creating roles

Which roles are available?

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

Managing rights (Page 75)

- administrator

  Default role when creating new SCT project.

  Unrestricted access rights to all configuration data.
- standard

  Role with restricted access rights.
- diagnostics

  Default role when creating new user.

  Read-only access.
- remote access

  No rights except for logging on to the Web page for user-specific firewall rule sets.

- radius

  Role that can be used to activate user-specific IP rule sets with authentication using a RADIUS server.

  Read-only access.

- administrator (radius)

  Role that can be used to activate user-specific IP rule sets with authentication using a RADIUS server.

  Access rights to all configuration data except SNMP MIBs.

Note

For more detailed information on user-specific IP rule sets, refer to the following section:

User-specific IP rule sets (Page 149)

Note

For more detailed information on authentication using a RADIUS server, refer to the following section:

Authentication using a RADIUS server (Page 81)

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: ~~CP 443-1 OPC UA~~
"Users" > "Start of user administration", "Run" button. The user administration can also be called up from individual tabs.

Table 2- 2 Information in the "Roles" tab

Parameter	Meaning
Role name	Freely selectable role name.
Comment	Entry of additional comments.
Maximum time of the session SCA. S	Entry of the time after which a user with the assignment role is automatically logged off from the Web page for user-specific IP rule sets of SCALANCE S modules. The time entered here starts after the logon and after renewing the session on the Web page of the security module. • Default setting: 30 minutes • Minimum value: 5 minutes • Maximum value: 480 minutes

Table 2- 3 Buttons in the "Roles" tab

Name	Meaning / effect
Properties... / Edit...	Select a user-defined role in the list and click the button. In the dialog that opens, change the properties of the role such as the role name, the assignment of rights to the role and the maximum session time. 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 (default: "diagnostics").
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 not assigned to any user. If necessary, assign the user a different role. • System-defined roles cannot be deleted.

2.5.4 Managing rights

How to access this function

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

STEP 7 menu command: ~~CP 443-1 OPC UA~~

"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 (default: "diagnostics"). 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. If required, enter a comment and a maximum session time for the role to be created.
5. Click the "Apply" button to save the selection or "OK" to save and close window.
6. Assign the role to a user.

Copying the role rights of a security 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 role type, the following configuration rights are available for selection for each security project:

Table 2- 4 Configuration rights for access to the security project

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

x Right is enabled

- Right is disabled

Module rights

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

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

Table 2- 5 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	-	

x Right is enabled

- Right is disabled

Table 2- 6 Module rights CP 443-1 OPC UA

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 LLDP MIB	x	x	x	
SNMP: Read SNMPv2 MIB	x	x	x	
SCT: Run diagnostics of the security module ****	x	x	x	Security
Web: Access Web diagnostics	x	x	x	Web

Right within the service	administrator	standard	diagnostics	Service
Web: Update firmware *	x	x	-	Maintenance
Web: Load diagnostics texts later *	x	x	-	
OPC UA: Read variables	x	x	x	OPC UA
OPC UA: Write variables	x	-	-	

x Right is enabled

- Right is disabled

* To be able to use the function, the module right "Web: Access Web diagnostics and CP file system" must be enabled as well.

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

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

**** 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

x Right is enabled

- Right is disabled

Table 2- 8 Module rights SCALANCE S

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 S627-2M	x	x	x	
SNMP: Write MRP MIB S627-2M	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

x Right is enabled

- Right is disabled

Setting module rights before and after creating the security modules

Within a user-defined role, the module rights for each security module are defined separately. If a security module was created for which module rights will be defined within a role before the role was added, the module rights for this security module will be set automatically according to the selected rights template and can, if necessary, be adapted. If a security module was added after creating a role, SCT does not set any rights. In this case, you will need to set all module rights for the security module yourself.

You can also transfer existing module rights to another security module by copying and, if necessary, adapting them there. To do this, select a security module in the shortcut menu in the module rights and select the "Copy rights" or "Paste rights" menu command.

2.5.5 Configuring password policies

Meaning

Using the password policies, specifications can be defined that need to be taken into account when assigning passwords to new users.

How to access this function

Select the "Options" > "User management..." menu command, "Password policies" tab. After selecting a check box, the corresponding policy is active and can, if necessary, be adapted using the relevant input box.

Parameter	Meaning
Minimum password length	Minimum number of characters that passwords are required to contain. The corresponding check box is enabled as default and cannot be disabled. • Minimum value: 8 characters • Maximum value: 32 characters
Minimum number of digits	Minimum number of digits that passwords are required to contain. • Minimum value: 1 digit • Maximum value: 32 digits
Minimum number of special characters	Minimum number of special characters that passwords are required to contain. A special character is any character that is neither a letter nor digit. • Minimum value: 1 special character • Maximum value: 32 special characters
Number of passwords blocked for further use	Number of the most recently used passwords that are not available for use as a new password if the password is changed. • Minimum value: 1 password • Maximum value: 10 passwords
At least one uppercase and lowercase character	If you select this check box, passwords must contain at least one uppercase and one lowercase letter.

2.5.6 Authentication using a RADIUS server

2.5.6.1 Overview

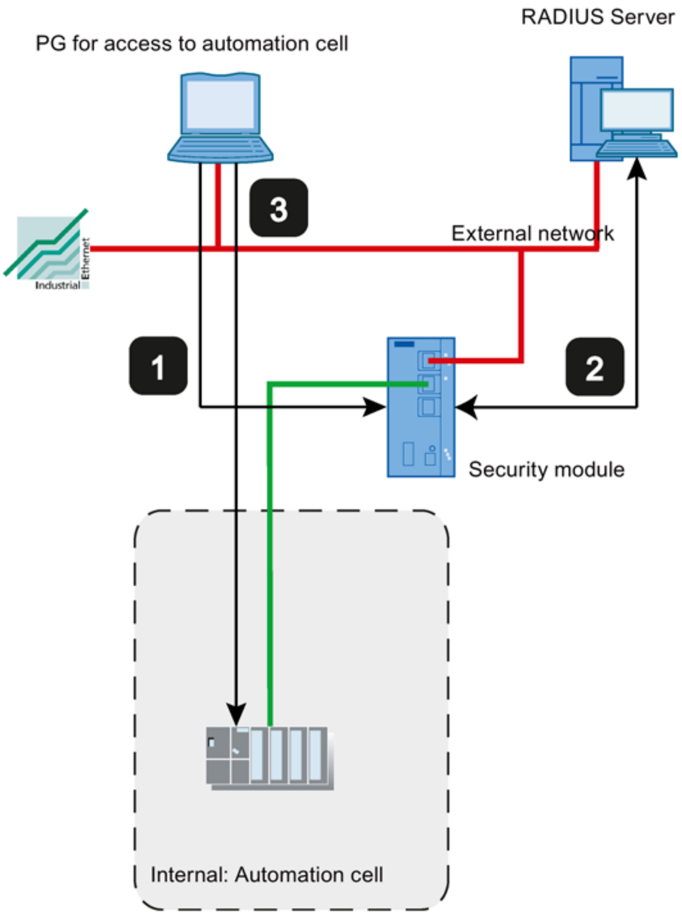
S≥V4.0

Meaning

RADIUS (Remote Authentication Dial-In User Service) is a protocol for authenticating users by servers on which user data can be stored centrally. The use of RADIUS servers can increase the protection of user names, assigned roles and passwords.

Scenario for the use of RADIUS servers

Authentication by RADIUS servers can be performed when activating user-specific IP rule sets.



1 Entry of the user data on the Web page of the security module

2 Authentication by RADIUS server and activation of the user-specific IP rule set

3 Access to an automation cell

The network setup shown above is simply an example. The RADIUS server can also be located in the internal network or in the DMZ network of the security module.

For the configuration options described below, it is assumed that a RADIUS server is configured in SCT and was assigned to the relevant security module. In addition to this, one user or role must be configured with the "RADIUS" authentication method. For more detailed information, refer to the following sections:

- Defining a RADIUS server (Page 83)
- Assigning a RADIUS server to a security module (Page 84)
- Create users (Page 72)
- Creating roles (Page 73)

For general information on user-specific IP rule sets, refer to the following section:

- User-specific IP rule sets (Page 149)

Configuration options

To authenticate the user using a RADIUS server, there are two configuration options available:

- The user and the user's role are known on the security module, only the password management for the user is performed on the RADIUS server. The user and the password are configured on the RADIUS server.
  - A user with the "RADIUS" authentication method is configured.
  - The user is assigned to the user-specific IP rule set.

  Result:
  - When a user logs on to the Web page of the security module, the authentication query is forwarded to the RADIUS server.
  - The RADIUS server runs a password check and signals the result back to the security module.
  - If the password check is passed successfully, the user-specific IP rule set is activated.
- The role is known on the security module, user management is via the RADIUS server. The user and the password are configured on the RADIUS server.
  - A user-defined role or a system-defined role is assigned to the user-specific IP rule set.
  - In the "RADIUS" tab of the security module, the "Allow RADIUS authentication of non-configured users" and the "Filter ID is required for authentication" check boxes are enabled.

  Result:
  - When a user logs on to the Web page of the security module, the authentication and authorization query is forwarded to the RADIUS server.
  - The RADIUS server runs a password check and signals the result back to the security module.
  - Case a: If, in addition to this, the role name is configured on the RADIUS server:

The RADIUS server returns the role name assigned to the user to the security module.

– Case b: If the role name is not configured on the RADIUS server:

The security module assigns the user the system-defined role "radius".

– If the password check is passed successfully, the user-specific IP rule set is activated.

Conventions for RADIUS servers

- The RADIUS servers can be in any network connected to the security module.
- A maximum of two RADIUS servers can be configured per security module. During operation only one of the RADIUS servers is active.
- When defining a RADIUS server, an FQDN can also be used instead of IP an address.

2.5.6.2 Defining a RADIUS server

S≥V4.0

Meaning

Before authentication by a RADIUS server is possible, this first needs to be stored in the SCT project. Following this, you assign the defined RADIUS server to the security module for which the RADIUS server will handle user authentication.

Procedure

1. Select the "Options" > "Configuration of the RADIUS server..." menu command.
2. Click the "Add..." button.
3. Enter the required parameters according to the following table.

Parameter	**Meaning**
Name	Freely selectable name for the RADIUS server.
IP address / FQDN	IP address or FQDN of the RADIUS server.
Port	UDP port via which the RADIUS server can be reached. As default, authentication data is received at port 1812.
Shared secret	Entry of the password that will be used when transferring the logon data between the RADIUS server and security modules for encryption. The following characters from the ANSI X 3.4-1986 character set are permitted: 0123456789 A...Z a...z !#$%&()"*'+`,-./:;<=>?@ [\]_{|}~^ Length of the shared secret: 1 ... 31 characters

Parameter	Meaning
Repeat shared secret	Confirmation of the password
Authentication method	Display of the method used to check the user data. Only the "PAP" method (Password Authentication Protocol) is supported.
Comment	Entry of freely selectable, optional comments.

Result

You have defined a RADIUS server and can now assign this to the required security modules.

2.5.6.3 Assigning a RADIUS server to a security module

S≥V4.0

Requirement

You have defined a RADIUS server.

Procedure

1. Select the security module to which you want to assign a RADIUS server.
2. Select the "Edit" > "Properties..." menu command.
3. Select the "RADIUS" tab.
4. Select the "Enable RADIUS authentication" check box.

Note

Changing the method of authentication with the Web server on the security module

If RADIUS authentication is enabled on the security module, the method for authentication with the Web server is changed from "Digest Access Authentication" to "Basic Access Authentication".

5. In the "RADIUS timeout" input box, enter the maximum time in seconds that the security module will wait for a response from the RADIUS server.
6. In the "RADIUS retries" input box, enter the number of connection establishment attempts with the RADIUS server.
7. Select the "Allow RADIUS authentication of non-configured users" check box if the user-specific IP rule to be activated was assigned a role instead of a user.
8. Select the "Filter ID is required for authentication" check box if the assigned role is a user-defined role.

9. Click the "Add" button.

   Result: The RADIUS server that was configured first is assigned to the security module.

10. From the "Name" drop-down list, select the RADIUS server you want to assign to the security module.

You will find general information on authentication by the RADIUS server in the following section:
Authentication using a RADIUS server (Page 81)

See also

Create users (Page 72)

2.6 Managing certificates

2.6.1 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.

A CA certificate is a certificate issued by a certificate authority from which the device certificates are derived. The device certificates include SSL certificates. SSL certificates are required for authentication in secure communication between a security module and another network node. Further device certificates include the VPN group certificates of security modules located in VPN groups and OPC UA client/server certificates of CP 443-1 OPC UA modules. Certification 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) certification 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 certification 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:

- Import of new certificates and certification authorities.
- Import of FTPS certificates if the CP is being used as an FTP client. CP x43-1 Adv.
- Export of the certificates and certification authorities used in the project.
- Renewal of expired certificates and certification authorities.
- Replacing existing certificate authorities.

Note

Downloading the project

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.

Note

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 *.crt *.p12 *.der *.cer **Note** • Users with the system-defined "diagnostics" role must not use the export function.
Display...	Opens the certificate dialog of Windows where you will see an overview of all certificate data.

"Certification authority" tab

The following certification authorities are displayed

- Certification authority of a project: When you create a new SCT project, a CA certificate is generated for the project. The SSL certificates and OPC UA client/server certificates for the individual security modules are derived from this certificate.
- Certification authority of a VPN group: When you create a new VPN group, a CA certificate is generated for the VPN group. The VPN group certificates of security modules located in the VPN group are derived from this certificate.

"Device certificates" tab

Display of the device-specific certificates generated by the certification authority for modules. These include:

- SSL certificate of a security module: An SSL certificate that is derived from the 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.
- OPC UA client/server certificate of the module: Depending on the configured OPC UA client/server function of the CP 443-1 OPC UA, an OPC UA client/server certificate is generated that is used for authentication with the relevant communications partner. The properties of this certificate are strictly adopted from the module properties configured in STEP 7. If the alternative applicant name of the certificate is changed manually in SCT using the function "Renew certificate", the the values changed by the user will be adopted. If the alternative applicant name is deleted by the user in SCT, the alternative applicant name will be regenerated from the module properties of STEP 7.
- VPN group certificate of a security module: A VPN 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. S

Display of the certification authorities required for verification of external services such as providers of dyn. DNS by the security modules.

2.6.2 Renewing certificates

Meaning

In this dialog, you renew CA certificates and device certificates.

How to access this function

1. Right-click on a list entry in the certificate manager.
2. Select the "Renew certificate ..." entry.

Parameter	Options
Signing	• Self-signed • Signed by a certification authority: Only certification authorities located in the certificate memory of the SCT project can be selected.
Applicant	Depending on the certificate to be renewed, enter the following values for the applicant: • CA certificate of the project: [name of the CA certificate] • CA certificate of VPN group [name of the CA certificate] • SSL certificate for S7 CP [name of the security module] • SSL certificate for PC CP [name of the security module] • SSL certificate for SCALANCE S, SCALANCE M and SOFTNET Security Client [name of the security module] • OPC UA client/server certificate of the module: [name of the security module] • VPN group certificate of a security module: [name of the VPN group cerrtificate]
Valid from / to	Validity period of the certificate. Validity data after 2037 is not supported.
Alternative applicant name	Depending on the certificate to be renewed, enter the following values for the alternative applicant name: • SSL certificate for S7 CP: For CP x43-1 Adv.: IP:[IP address of the gigabit interface],IP:[IP address of the PROFINET interface] For CP 443-1 OPC UA: IP [IP address of the security module] • SSL certificate for PC CP: IP [IP address of the security module] • OPC UA client/server certificate of the module: DNS:[name of the security module],URI:urn:[application name]:[GUID],IP:[IP address of the security module] • VPN group certificate of a security module: Derived from the CA.
Signature algorithm (only for SSL certificates)	Select the algorithm with which the signature for the certificate will be created: • SHA1 • SHA256

2.6.3 Replacing certificates

Meaning

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

How to access this function

1. Right-click on a list entry in the "Certification 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 certificate of an already configured VPN group can be replaced in the SCT project by the CA certificate of a VPN group from a different SCT project. The VPN group certificates for the VPN group members are therefore derived from the same CA 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 certificate 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.

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 SCT dialog.

Note

Performance features and device types

Note which functions the device type you are using supports.

See also

Online functions - diagnostics and logging (Page 273)

How to access this function

1. Select the "All modules" object in the navigation panel.
2. Select the "Insert" > "Module" menu command.
3. Make the following settings.

Parameter	Meaning
Product type	Product type used when a new module is created. SCALANCE S SCALANCE M SOFTNET Configuration (SOFTNET Security Client, VPN device, NCP VPN client)

Parameter	Meaning
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 the option "NCP VPN client for Android" to insert a VPN client device as proxy for a device with NCP Secure VPN Client for Android software installed. Select the "VPN device" option to insert a VPN client device as proxy for a device from another manufacturer. Select the option "SCALANCE M-800" to insert a SCALANCE M-800 configuration that can also be used for SCALANCE S615. Note The checked out configuration file simply provides help on the configuration of the VPN connection, but is no guarantee for compatibility with products of other manufacturers.
Firmware release	You can specify the firmware/software versions here for the SCALANCE S modules and the SOFTNET Security Client.
Name of the module	Freely selectable name for the module.
MAC address	Entry of the MAC address of the module.
IP address (ext.)	IP address for the external interface. The IP address consists of four decimal numbers with the range from 0 to 255, each number separated by a period, example: 141.80.0.16
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
Interface routing external/internal	Selecting the mode for the security module. The following modes are available for SCALANCE S: • Bridge mode • Routing mode When selecting routing mode, you need to configure an IP address and a subnet mask for the internal interface of the security module.
IP address (int.) Only needs to be specified when routing mode is enabled	IP 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: 141.90.10.10

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

You make further interface settings in the "Interfaces" tab of the module properties. For information on this, refer to section:

- Configuring interfaces (Page 96)

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 STEP 7 module 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

Parameters in the content area (Page 94)

Range of values for IP address, subnet mask and address of the gateway (Page 287)

MAC address (Page 288)

3.1 Parameters in the content area

How to access this view

Select the "All modules" object in the navigation panel.

For CPs only the content of the "Comment" column can be edited.

The following properties of the modules are displayed in columns:

Property/column	Meaning	Comment/selection
No.	Consecutive module number	Assigned automatically
Name	Unique module name	Freely selectable
Type	Device type	**Note** For devices of the type "SOFTNET Security Client" there is no properties dialog. In the module properties of the NCP VPN client, you can specify the storage path of the files on the NCP VPN client. For VPN devices, you can only adapt the file types of the configuration files to be exported in the module properties.
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 for the external IP address	Assigned as suitable in the network.
IP address int.	IP address with 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 for the internal IP address	Assigned as suitable in the network. The input box can only be edited when routing mode is enabled.
Standard router	IP address of the standard router	Assigned as suitable in the network.
MAC address	Hardware address of the module	The MAC address is printed on the module housing.
Comment	Information on the module and the subnet protected by the module	Freely selectable

Changing address parameters for SCALANCE S / M

For SCALANCE S / M modules, some 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 Adv.	CP 443-1 OPC UA	CP 1628
IP address ext.	IP address gigabit	IP address OPC UA	IP address IE (Industrial Ethernet)
Subnet mask ext	Subnet mask gigabit	Subnet mask OPC UA	Subnet mask IE
IP address int.	IP address PROFINET	Is not displayed	Is not displayed
Subnet mask int.	Subnet mask PROFINET	Is not displayed	Is not displayed
Standard router	Standard router configured in STEP 7	Standard router configured in STEP 7	Standard router configured in STEP 7
MAC address	MAC address gigabit (if configured)	MAC address OPC UA	MAC address IE (if configured)

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 / OPC UA interface

Mode in STEP 7	IP address ext. / Subnet mask ext. (boxes in SCT)
Obtain IP address from a DHCP server	dynamic

Table 3- 2 PROFINET interface

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

3.2 Configuring interfaces

3.2.1 Overview of the connector options

SCA. S

Supported connector options

Each security module has a certain number of ports to which the network nodes can be connected. Depending on the interface, the network nodes are handled differently.

Security module	Interface	MAC address of the interface*	Port of the interface	Port type	MAC address of the port*
SCALANCE S602 / S612 / S613	External	MAC address (see labeling)	P1	Built-in RJ-45 jack (copper)	MAC address + 2
	Internal	MAC address + 1	P2	Built-in RJ-45 jack (copper)	MAC address + 3
SCALANCE S623	External	MAC address (see labeling)	P1	Built-in RJ-45 jack (copper)	MAC address + 3
	Internal	MAC address + 1	P2	Built-in RJ-45 jack (copper)	MAC address + 4
	DMZ	MAC address + 2	P3	Built-in RJ-45 jack (copper)	MAC address + 5
SCALANCE S627-2M	External	MAC address (see labeling)	P1	Built-in RJ-45 jack (copper)	MAC address + 3
			P4	Media module port (copper/FOC)	MAC address + 4
			P5	Media module port (copper/FOC)	MAC address + 5
	Internal	MAC address + 1	P2	Built-in RJ-45 jack (copper)	MAC address + 6
			P6	Media module port (copper/FOC)	MAC address + 7
			P7	Media module port (copper/FOC)	MAC address + 8
	DMZ	MAC address + 2	P3	Built-in RJ-45 jack (copper)	MAC address + 9

* When operating in bridge mode, the printed MAC address is valid both on the external and on the internal interface.

The MAC addresses of the interfaces are used for all services except LLDP.

The MAC addresses of the ports are used for topology discovery with LLDP (only for modules in routing mode).

Note

The Ethernet interfaces must not be confused when connecting to the communications network:

- X1 interface - external

  Red marking = unprotected network area;
- Interface X2 - internal

  Green marking = network protected by SCALANCE S;
- Interface X3 - DMZ (universal network interface)

  Yellow marking = unprotected network area or network area protected by SCALANCE S.

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

Functions of the DMZ interface S62x

A demilitarized zone (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 cannot be accessed. To improve protection, it is also possible to allow access only to VPN data traffic. An example of a configuration in which the DMZ interface is used to set up a DMZ can be found in section "4.2 SCALANCE S as firewall between external network and DMZ" of the "SIMATIC NET Industrial Ethernet Security - Getting started" manual.
To be able to assign a dynamic IP address to devices in the DMZ as well, A DHCP server can enabled on the DMZ interface. 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.

The DMZ interface can be used as a VPN endpoint. In conjunction with the DSL modem, the DMZ interface is then operated in PPPoE mode or in conjunction with an upstream DSL router with a static IP address. An example of a configuration in which the DMZ interface is used for remote access via a VPN tunnel can be found in the section "5.2 VPN tunnel between SCALANCE S623 and SCALANCE S612" in the "SIMATIC NET Industrial Ethernet Security - Getting started" manual.

Media module ports of the external and internal interface S627-2M

In addition to the functions of the SCALANCE S623, the SCALANCE S627-2M has two media module slots in which an electrical or optical 2-port media module can be inserted. This expands both the external and internal interface by up to two ports. If the media module "MM992-2SFP" is used for an interface, you can insert up to two electrical or optical SFP transceivers (Small Form-factor Pluggable transceiver) into the media module. The additional ports can be used to connect the external and internal interface of the SCALANCE S627-2M to MRP/HRP rings.

The media module ports are connected to the built-in port of the particular interface via a switch chip. Between the ports connected via a switch chip, there is no firewall functionality (layer 2 / layer 3). All the ports connected via a switch chip can be reached using the same IP address.

Functions of the individual interfaces

The following functions can be used on the individual interfaces:

Function	Green (internal)	Red (external)	Yellow (DMZ)
Static IP address	x	x	x
WAN access with DSL router	-	x	x
WAN access with DSL modem (PPPoE, dynamic IP address from ISP)	-	x (when not on yellow interface)	x (when not on red interface)
Bridge mode	x		-
Routing mode	x	x	x
Ghost mode S602 ≥V3.1	-	x	-
DHCP server	x	-	x
Endpoint of a VPN tunnel connection (with DSL modem and DSL router)	-	x	x
MRP/HRP client (in routing mode, ring ports on the media modules) S627-2M	x	x	-
LLDP (in routing mode) S≥V4.0	x	x	x
Passive listening (in routing mode when media modules are plugged in) S627-2M	x	x	-

x is supported

- is not supported

Duplex mode

One of the following two duplex modes can be selected for a port:

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

Note

Duplex method and transmission speed with optical ports S627-2M

For ports with the port type "optical", the port mode is fixed by the media module used or by the SFP transceiver used and cannot be adapted.

3.2.2 Interfaces

SCA. S

SCA. M

How to access this function:

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

Interface routing - options available SCA. S

If the SCALANCE S module is not in a VPN group and is not in a redundancy relationship, the interface routing can be modified in this box. The selection applies to interface routing between the external and internal interface. The DMZ interface (SCALANCE S623 and SCALANCE S627-2M only) is always connected in routing mode.

Bridge mode	For operation in flat networks. External and internal interface are in the same IP subnet. For S623 / S627-2M: External and internal interface are in the same IP subnet, the DMZ interface is in a different IP subnet or is deactivated.
Routing mode	All interfaces 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.

Ghost mode S602 ≥V3.1	In operation, the SCALANCE S module adopts the IP address of the node connected to the internal interface of the SCALANCE S module for the external interface. The IP address data specified for the external interface is only used for downloading the configuration prior to operation in ghost mode. **Note** The ghost mode can only be selected in the "Interfaces" tab if the project is in advanced mode.

Configuring the interfaces

If the interface of a module is to be configured, this must be activated using the "Activate interface" check box. Set the IP address information for each interface and settings for the individual ports (only for SCALANCE S). There are two ways in which you can assign an IP address for the external interface and for the DMZ interface (SCALANCE S623/S627-2M only):

- Static IP address with subnet mask
- Address assignment using PPPoE SCA. S

  The internal interface and the tunnel interface (only for SCALANCE S612/S623/S627-2M as of V4) can only be configured using a static IP address.

If alias IP addresses were registered on an interface due to configuring a NAT/NAPT rule for a SCALANCE S module, these are displayed in the "Alias IP addresses" box.

Note

External interface and DMZ interface (only SCALANCE S623/S627-2M) as Internet access

The simultaneous operation of PPPoE on the external interface and on the DMZ interface (dual ISP) is not possible.

Meaning of the tunnel IP address S≥V4.0 ~~S602~~

If you use the function "NAT/NAPT in the VPN tunnel", you need to assign a tunnel IP address for the security module. This ensures the reachability of the security module via the VPN tunnel and provides a configuration and diagnostics option. The configured tunnel IP address can be expanded with alias tunnel IP addresses using suitable NAT / NAPT rules. The subnet mask is fixed at 32 bits for the tunnel IP address and cannot be changed. The tunnel IP address can only be configured if the following requirements are met:

- The security module is in a VPN group.
- The project is in advanced mode.

You will find further information on address translation with NAT/NAPT in VPN tunnels in the following section:
Address translation with NAT/NAPT in VPN tunnels (Page 183)

Point to Point Protocol over Ethernet (PPPoE) SCA. S

To allow Internet/WAN access directly via a DSL modem, the IP address on the external interface or on the DMZ interface is assigned using 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.

To use this IP address assignment mode, specify the ISP in the "Internet connection" tab. The IP address, the subnet mask, the standard router and the DNS server of the interface are specified by the ISP.

Note

A configured standard router is not taken into account when using PPPoE. This is assigned dynamically to the module by the ISP.

Note

No network components between SCALANCE S and DSL modem

If the interface of a SCALANCE S module is operated using PPPoE, there must be no other network components between this interface and the connected DSL modem otherwise the dial-in data of the Internet Service Provider may be transferred unencrypted over this link. When using the "CHAP" authentication protocol, the data is transferred encrypted.

Port settings SCA. S

Column	Meaning		
Port ID	Automatically assigned ID for the port of the interface.		
Port type	Physical characteristic of the port (copper/fiber)		
Port mode	Autonegotiation	The transmission speed and the duplex method are negotiated automatically between IEEE 802.3-compliant ports. **Note** A transmission speed of 1000 Mbps and the autocrossing function are 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	
	Long Distance Signaling (LDS)	The transmission speed and the duplex method are negotiated automatically between BroadR-Reach-compliant ports.	
	Off (only external port or DMZ port with SCALANCE S623 and SCALANCE S627-2M)	The port is disabled.	
	Note S627-2M Ports of media modules using fiber-optic cables as the transmission medium always use full duplex and operate at the maximum transmission speed. This means that the port mode of the ports of optical media modules cannot be configured.		
S≥V4.0 LLDP mode (in routing mode)	RxTx	LLDP frames can be sent and received.	For more detailed information on LLDP, refer to the following section: LLDP (Page 107)
	Off	Receive LLDP frames	
S627-2M MRP port (in routing mode for the media module ports of the external and internal interface)	Display indicating whether the media module ports of the interface are connected to an MRP ring. If this is the case, the character strings "RingportOne" and "RingportTwo" are displayed in the table rows of the media module ports. For the ports with the port ID "X1 P1" and "X2 P1", the character string "None" is displayed as default since these cannot be involved in an MRP ring. You will find general information on media redundancy with MRP in the following section: Media redundancy with MRP or HRP (Page 107) You will find information on configuring MRP for the security module in the following section: Configuring MRP/HRP for the security module (Page 108)		
S627-2M HRP port (in routing mode for the media module ports of the external and internal interface)	Display indicating whether the media module ports of the interface are connected to an HRP ring. If this is the case, the character strings "RingportOne" and "RingportTwo" are displayed in the table rows of the media module ports. For the ports with the port ID "X1 P1" and "X2 P1", the character string "None" is displayed as default since these cannot be involved in an HRP ring. You will find general information on media redundancy with HRP in the following section: Media redundancy with MRP or HRP (Page 107) You will find information on configuring HRP for the security module in the following section: Configuring MRP/HRP for the security module (Page 108)		
Comment	Freely selectable comment		

Configuration of media modules S627-2M

Click the "Configure media module..." button to call up the dialog for configuring the media module for the corresponding interface.

The following configuration modes are available:

- "Automatic" (default setting): The media module you are using is detected automatically during operation. The port mode is set to "Autonegotiation" for both ports.
- "Manual": Select the media module type being used from the "Module type" drop-down list. If you select the media module type "MM992-2SFP", you can select the required transceivers (SFPs) from the two "SFP type" drop-down lists.
  For ports with the port type "Copper", you can specify the transmission speed and the duplex method manually using the port mode. For ports with the port type "Optical", the port mode is fixed by the media module used or by the SFP transceiver used and cannot be adapted.

See also

Special features of the ghost mode (Page 110)

Overview of the connector options (Page 96)

Configuration data for SCALANCE M modules (Page 235)

3.2.3 Internet connection

SCA. S

How to access this function:

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

Meaning

In this tab, you make settings related to the Internet Service Provider (ISP) if a connection using PPPoE is set for one of the interfaces of the security module.

Table 3- 3 Settings for the ISP account

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.
Repeat password	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 have to use the same authentication method otherwise no connection can be established.

Table 3- 4 Rules for user names and passwords

Permitted characters	The following characters from the ANSI X 3.4-1986 character set are permitted: 0123456789 A...Z a...z !#$%&()"*'+`,-./:;<=>?@ [\]_{|}~^
Length of the user name	1 to 255 characters
Length of the password	1 to 31 characters

Table 3- 5 Settings for the connection

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 currently no packets to be sent.
On-demand connection	The Internet connection is established automatically if packets need to be sent to the Internet. In this setting, delays in the sending of packets are possible.
Forced disconnection (only with the "Permanent connection" setting)	The provider terminates the Internet connection automatically after a certain period. If you enter a time of day in the "Forced disconnection" box, the security module terminates the Internet connection itself at this time. This allows disconnection of the Internet connection by the provider to be delayed under certain circumstances. A self-initiated forced disconnection is only possible with an existing permanent connection. Permitted entries: 00:00 ... 23:59
Maximum idle time (only with the setting "on-demand connection")	If no packets are sent during a certain time, the Internet connection is automatically terminated. In the "Maximum idle time" box, enter the time in seconds after which the connection will be terminated. Permitted values: 10 ... 3600.

Configuring address translation into the PPPoE network

The check box "Allow NAT from internal to PPPoE network" is only available if the project is not in advanced mode. If you enable the check box, SCT creates a NAT rule with which the source IP addresses of all nodes in the internal network are translated to the module IP address in the PPPoE network. This NAT rule and the corresponding firewall rule are visible after enabling the check box in advanced mode.

3.2.4 Dynamic DNS (DDNS)

SCA. S

Meaning

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, IP address that changes.

How it works

The security module signals the current WAN IP address via which the security 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 security module are replied to with the current WAN IP address of the security module.

Dynamic DNS is permitted at the following interfaces:

- External interface
- DMZ interface

Setting up dynamic DNS - Requirements

Requirement:

- An account has been created with a providers of dynamic DNS and an FQDN has been registered.

Setting up dynamic DNS - Follow the steps below:

1. Select the "DNS" tab in the module properties of the security module.
2. If the security module is downstream from a DSL router or DSL modem, you specify a valid DNS server address. To do this, two options are available:

Option	Meaning
Obtain DNS server address automatically	The address of the DNS server can be obtained automatically using PPPoE if the security module is connected to the Internet via a DSL modem. Can only be set for the external interface and the DMZ interface.
Use the following DNS server address:	Enter the address of the preferred and of the alternative DNS server manually.

3. Activate the "Activate service" check box in the "Primary dynamic DNS service" area and make the following settings:

Setting	Meaning
Provider	Choose the provider with which you have set up an account for dynamic DNS.
User account with the provider	Enter the user name that you specified when you created the account.
Password with the provider	Enter the password that you specified when you created the account.
FQDN	Enter the host name (e.g. mysecuritydevice) and the domain name (e.g. dyndns.org) that is registered with the provider separated by a period. If an FQDN is also entered in the "VPN" tab, both must match.
Monitor IP address change on DSL router	If the security module is connected to the Internet via a DSL router, enabling this function 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. The IP address specified in this way is sent to the provider with each change ID.
Period	Specify the interval at which the Check IP service is called. Permitted values: 10 … 1440 minutes

4. In case the primary provider fails, create a second provider in the "Secondary dynamic DNS service" tab (optional setting).

Setting up a user-defined provider - follow the steps below:

Select the "User-defined" entry in the "Provider" drop-down list and make the following entries:

Setting	Meaning
Provider update URL	Enter the URL you received from your provider. The placeholder texts <FQDN> and <CurrentWanIP> need to be placed at the correct positions in the URL.
Check IP service URL	Enter the URL you received from your provider.
Ignore errors when checking the server certificate	To ensure that the authentication data is protected, the certificate of the update server is normally checked. If the certificate check fails, the HTTP 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 dynamic DNS service is invalid (for example expired). It is advisable not to ignore the check and not to select the check box.

3.2.5 LLDP

S≥V4.0

Meaning

LLDP (Link Layer Discovery Protocol) is a protocol used to discover network topologies. A device capable of LLDP can send information about itself to neighboring devices at regular intervals and at the same time receive information from neighboring devices. The received information is stored on every device with LLDP capability in an LLDP MIB file. Network management systems can access these LLDP MIB files using SNMP and therefore recreate the existing network topology.

Configurable parameters

The degree of activity of the security module in terms of LLDP can be configured in the "Interfaces" tab of the module properties as follows:

- Send and receive LLDP frames (default setting "RxTx")
- Receive LLDP frames ("Off")

3.2.6 Media redundancy in ring topologies

3.2.6.1 Media redundancy with MRP or HRP

S627-2M

Meaning

The term "media redundancy" groups together various methods for increasing availability in Industrial Ethernet networks in which devices can be reached over different paths. This might be achieved by meshing networks, arranging parallel transmission paths or by closing a linear bus topology to form a ring.

Media redundancy methods MRP and HRP

Media redundancy within a ring topology is available with SIMATIC NET products with the methods MRP (Media Redundancy Protocol) and HRP (High Speed Redundancy Protocol).

With both these methods, one of the nodes is configured as the redundancy manager. The other nodes are redundancy clients. SCALANCE S627-2M modules can only adopt the role of an MRP or HRP client. Using test frames, the redundancy manager checks the ring to make sure it is not interrupted. The redundancy clients forward the test frames. If the test frames of the redundancy manager no longer arrive at the other ring port of the redundancy manager due to an interruption, the redundancy manager switches through its two ring ports and informs the redundancy clients of the change immediately.

The two media redundancy methods MRP and HRP operate according to the same functional principle. They differ in the time the SCALANCE X switches need to switch through their ring ports as redundancy manager.

- MRP: 200 ms
- HRP: 300 ms

Note on the use of MRP and HRP

- MRP and HRP are supported in ring topologies with up to 50 devices. Exceeding this number of devices can lead to a loss of data traffic.
- It is recommended that you set the ring ports involved to full duplex and 100 Mbps. Otherwise there may be a loss of data traffic.

Possible uses of MRP/HRP on media module ports

MRP/HRP are supported only on the media module ports of the SCALANCE S627-2M. The following table shows the possible uses of MRP/HRP on the media module ports of a SCALANCE S627-2M:

Ring ports	Media module 1		Media module 2	
	P4	P5	P6	P7
MRP client or HRP client*	-	-	-	-
	Ring 1	Ring 1	-	-
	-	-	Ring 2	Ring 2
	Ring 1	Ring 1	Ring 2	Ring 2

* The simultaneous connection of the security module to an internal and an external ring is possible only if at least one of the interfaces is connected as an MRP client.

With two lower-layer rings per SCALANCE S module, layer 3 communication is possible between the rings.

3.2.6.2 Configuring MRP/HRP for the security module

S627-2M

Requirements

- The security module is in routing mode.
- Media modules are configured for the interfaces to be connected to rings.

How to access this function

1. Select the security module to be edited.
2. Select the "Edit" > "Properties..." menu command, "MRP/HRP" tab.

Configurable parameters

Parameter	Meaning	Possible selections
MRP/HRP interfaces	Selection of the interface to be connected to the MRP/HRP ring.	• External • Internal
Media redundancy role	Selection of the media redundancy protocol or disabling of media redundancy for the selected interface.	• Not a node in the ring • MRP client (default setting) • HRP Client
Activate 'passive listening'	Enable this check box if the selected interface will be connected to third-party networks in which STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol) is used.	• Activate 'passive listening' (default) • Deactivate 'passive listening'
MRP domain (only if the "MRP client" media redundancy role is selected)	The members of an MRP ring are specified with the help of MRP domains. The same MRP domain must be selected for the interfaces of all modules to be connected to the same MRP ring.	As default, the predefined MRP domain "mrpdomain-1" is selected for the external interface. Using the buttons "Add...", "Edit..."and "Remove", you can add new MRP domains, edit the names of existing MRP domains and delete existing MRP domains.
Ring port 1 (only when the media redundancy role "MRP client" or "HRP client" is selected)	Name of the first ring port of the interface selected in "Interface" if "MRP client" or "HRP client" was selected.	-
Ring port 2 (only when the media redundancy role "MRP client" or "HRP client" is selected)	Name of the second ring port of the interface selected in "Interface" if "MRP client" or "HRP client" was selected.	-
MRP node (only if the "MRP client" media redundancy role is selected)	Display of information on all security modules that belong to the same MRP domain as the selected interface.	-

Result

You have connected the security module to the MRP/HRP ring via the selected interface. The media module ports of which interface(s) are connected to the MRP/HRP ring is also shown in the "Interfaces" tab of the module properties.

Consistency check - this rule must be kept to

Remember the following rule when making the entries:

- The names of MRP domains may only be made up of lowercase letters, digits and the "-" character. The names must begin with a lowercase letter or a digit.

See also

Consistency checks (Page 66)

3.2.7 Special features of the ghost mode

S602 ≥V3.1

Meaning

In ghost mode, the security module has no IP address of its own, neither on the internal nor on the external interface. Instead, the security module obtains the IP address for its external interface during runtime from a node connected to the internal interface of the security module whose IP address parameters can be unknown at the time of configuration. It is possible to change an IP address of the internal node and a corresponding IP address at the external interface. Since the internal node is identified based on its MAC address, IP address changes are made only for the learnt MAC address. No IP address is configured or obtained on the internal interface of the security module.

As regards the MAC addresses, the security module replaces the MAC address of the internal node with the MAC address of the security module in all outgoing packets on the external interface (responses from the internal node).

Enabling ghost mode - follow the steps below:

Requirement: The ghost mode can only be selected if the project is in advanced mode.

1. Select the security module to be edited.
2. Select the "Edit" > "Properties..." menu command.
3. From the drop-down list "Interface routing external/internal" in the "Interfaces" tab, select the "Ghost mode" entry.

Configurable module properties

In ghost mode, the module properties can be configured in the following tabs:

- Interfaces
- Firewall
- Time-of-day synchronization
- Log settings
- SNMP

Since no DNS servers can be configured in ghost mode, no FQDN resolution is possible.

Requirement for identifying an internal node

The security module can only obtain the IP address of the internal node if the internal node initiates data communication with a communications partner of the external network.
In addition to this, the security module does not provide any server services while obtaining the IP address. The security module can only reply to queries from external after data packets have been sent to the security module by the internal node.

Port assignment for incoming and outgoing data connections

As the external interface of the security module and the internal node have the same IP address, the network components must be addressed explicitly via the TCP/UDP ports. For this reason, the ports are either assigned to the security module or the internal node. The assignments of the ports to the corresponding devices are shown in the following tables for incoming and outgoing data connections:

Table 3- 6 Port assignments for incoming connections (from external to security module)

Service	Port	Protocol	Comment
Web services, configuration and diagnostics access	443	TCP	The HTTPS port is permanently activated for configuration and diagnostics access using the Security Configuration Tool and cannot be changed.
SNMP	161	TCP	Once SNMP is activated in the Security Configuration Tool, incoming SNMP queries are transmitted via UDP port 161. Transfer via TCP port 161 is also possible, for example, to be able to reach the internal node. **Note** After activating SNMP, the SNMP port is permanently assigned to the security module. If SNMP is not activated, the internal node can be accessed using SNMP with the aid of a firewall rule.
		UDP	

Table 3- 7 Port assignments for outgoing connections (from security module to external)

Service	Port	Protocol	Comment
Syslog	514	UDP	If the syslog service is activated in the Security Configuration Tool, syslog messages are transmitted via UDP port 514 by the security module. This port assignment cannot be changed.
NTP	123	UDP	If NTP servers are used for time-of-day synchronization, NTP queries are transferred via UDP port 123. This port assignment cannot be changed.

Recognizable IP addresses and subnet masks

The security module only recognizes internal nodes with IP addresses in the range of the network classes A, B or C. The subnet mask is identified by the security module based on the network class (see table "Network classes and corresponding subnet masks"). To allow the subnet mask to be determined correctly, a standard router must be entered for the internal node.

Nodes with IP addresses in the network classes D and E are rejected by the security module.

Table 3- 8 Network classes and corresponding subnet masks

Network class	IP addresses		Subnet mask
	Low limit	High limit	
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	Is rejected by the security module
I	240.0.0.0	255.255.255.255	Is rejected by the security module

Configuration limits

A maximum of one internal node is recognized by the security module. If several internal nodes exist, the security module reacts as follows:

- The first device the security module recognizes in the internal network obtains access to the external network segment if the firewall is suitably configured.
- The data traffic of any additional nodes in the internal network is blocked in the outgoing direction at level 2 (MAC layer) based on the sender address.

Loading configurations and diagnostics after commissioning

After obtaining an IP address from the internal node, the security module has an IP address on the external interface that can differ from the IP address with which the security module was initially configured. To make a change to the configuration or for diagnostic purposes, you need to replace the initially configured IP address for the external interface with the IP address that the security module has obtained from the internal node during runtime in the Security Configuration Tool.

Routing information for hierarchical networks at the external port

If there are hierarchical networks with subnet transitions on the external interface of the security module, the security module needs to obtain the corresponding routing information from the internal node. To achieve this, the internal node must respond to ICMP queries sent to it. Responding to ICMP broadcasts is not necessary.

4 Configure the firewall

~~CP 443-1 OPC UA~~

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 a reply being sent.

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. IP rules affect all IP packets of layer 3 or higher. MAC rules only affect frames lower than layer 3.

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 rules or rule sets must be distinguished in advanced mode:

  - Local firewall rules are assigned to one security module. They are configured in the properties dialog of the security modules.
  - Global firewall rule sets can be assigned to individual or several security modules at the same time. They are displayed in the navigation panel in advanced mode of the Security Configuration Tool and configured globally.
  - User-specific IP rule sets can be assigned to individual or several security modules at the same time. They are displayed in the navigation panel in advanced mode of the Security Configuration Tool and configured globally.
    SCALANCE S V4 (RADIUS): User-specific IP rule sets can be assigned individual or multiple users as well as individual or multiple roles.

With the aid of service definitions, you can also define firewall rules clearly in a compact form. Service definitions can be used in all the rule types listed above.

Enabling the firewall

In standard mode, the firewall is controlled by selecting the "Activate firewall" check box. If you deselect the check box, the firewall settings 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

In standard mode, you can enable logging globally in the "Firewall" tab. With this, however, not all the packets that pass the firewall are displayed.

In advanced mode, you can enable logging for each individual firewall rule. This means that the restriction relating to displayed packets from the standard mode does not apply.

Note

Firewall of SCALANCE S627-2M

The media module ports of the SCALANCE S627-2M are connected to the built-in port of the particular interface via a switch chip. For this reason, there is no firewall functionality (layer 2 / layer 3) between the ports of the external interface themselves nor between the ports of the internal interface themselves.

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 nodes have access using the services you have enabled.

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.

Note

No return to standard mode possible

If you switch to the advanced mode for the current project, you cannot switch back.

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 Adv.

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 x43-1 Adv.

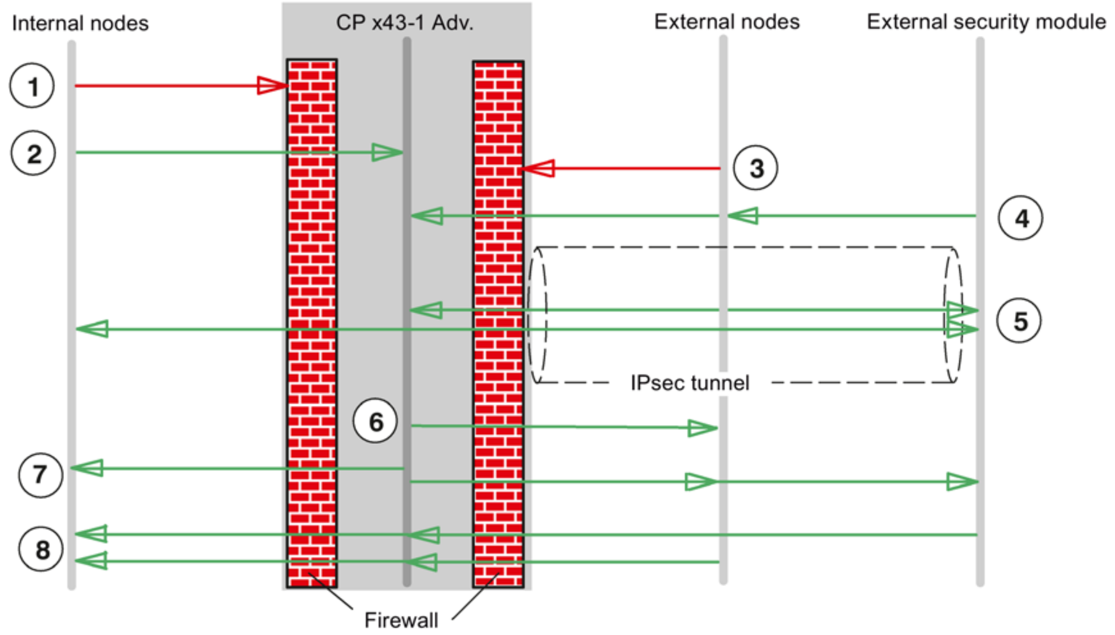


Figure 4-1 Default setting for the IP packet filter CP x43-1 Adv.

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 or from the security module are allowed.

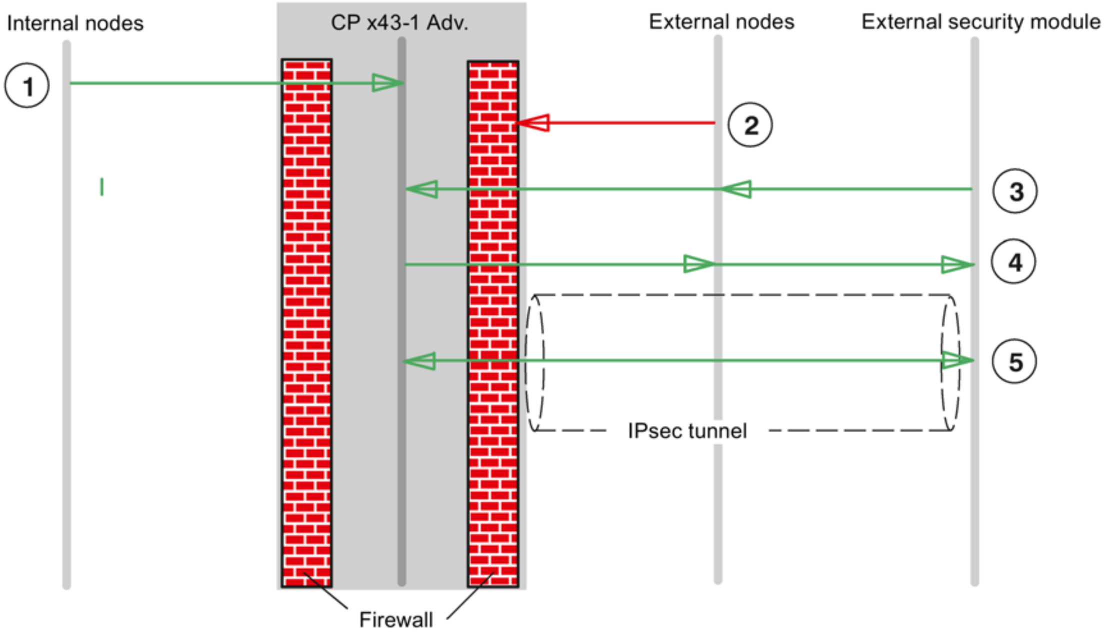


Figure 4-2 Default setting for the MAC packet filter CP x43-1 Adv.

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

② All frames from external to the security module 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 Configure the firewall

How to access this function

1. Select the security 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	Allow	Station	Tunnel

Rule set	**Action when activated**	**Created rule**		
	a member of a VPN group. All IP packets forwarded via the tunnel are logged.	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.

Note

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 the CP available, configure suitable firewall rules in SCT.

How to access this function

Menu command SCT: Select the security 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.
Modify...	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 address range.
End of the IP range (optional)	Enter the end value of an IP address range.

Box	Description
Comment	Entry of an additional comment, for example to describe the communication partner or the address range.
This IP address is authorized for the following accesses.	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

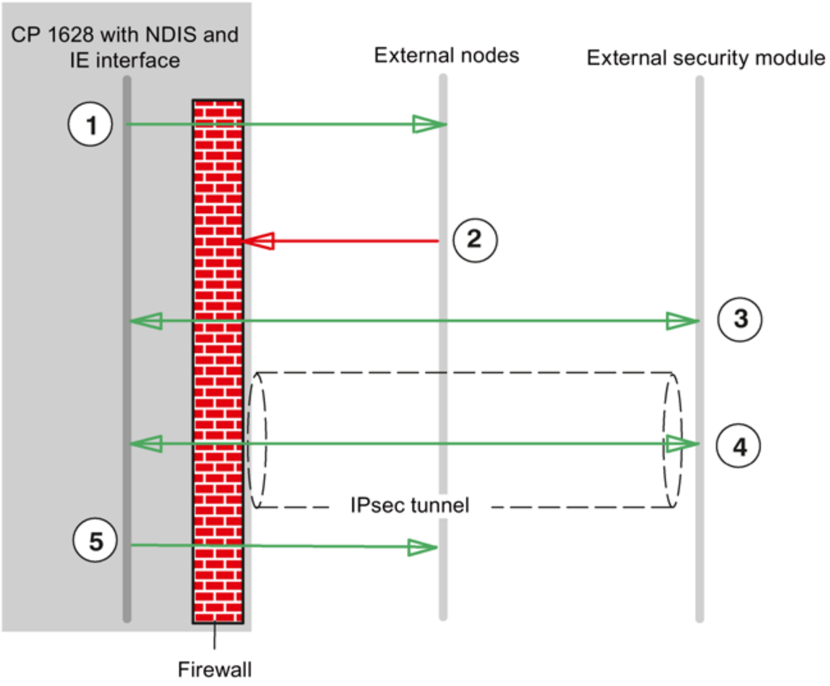


Figure 4-3 Default setting for the IP packet filter CP 1628

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)
- NAT Traversal (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.

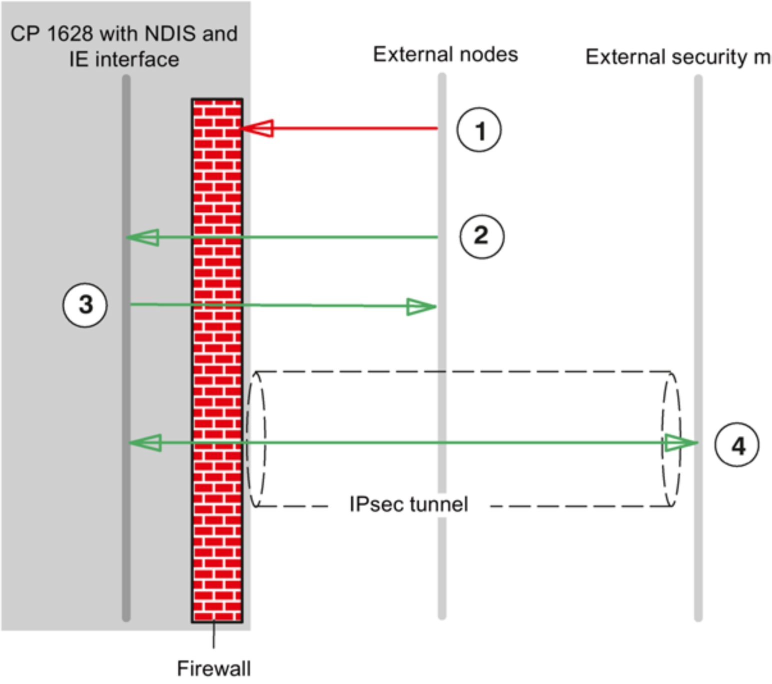


Figure 4-4 Default setting for the MAC packet filter CP 1628

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 Configure the firewall

How to access this function

1. Select the security 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 Default firewall setting

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 S602/S612

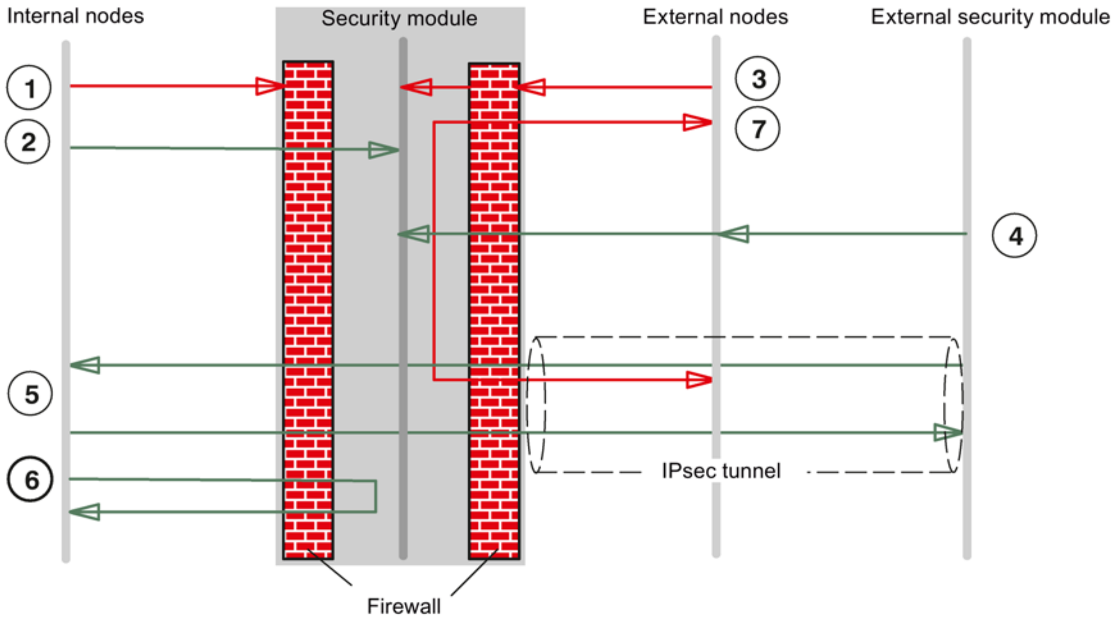


Figure 4-5 Default setting for the IP packet filter SCALANCE S602/S612

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.

④ Frames of the following types from external sources (external nodes and external security modules) to the security module 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. ~~S602~~

⑥ Frames from internal to external are allowed.

⑦ Frames from external to tunnel on the external interface and vice versa are blocked. ~~S602~~

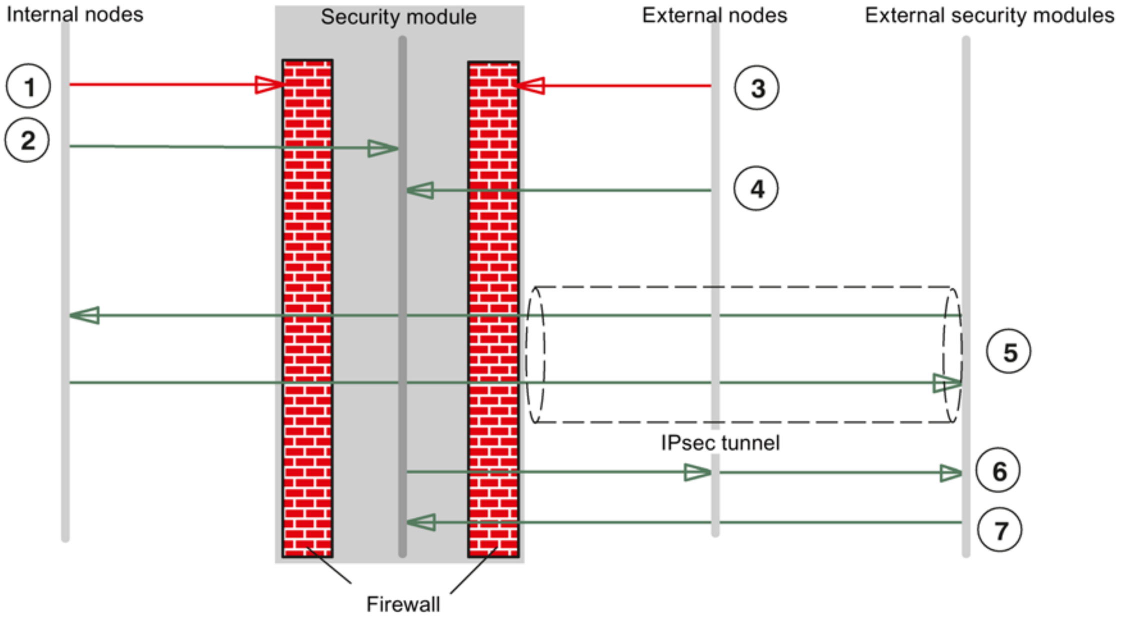


Figure 4-6 Default setting for the MAC packet filter SCALANCE S602/612

① All frame types from internal to external are blocked except for the following frame types.

- ARP frames

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

③ All frames from external to internal are blocked except for the following frame types.

- ARP frames with bandwidth limitation

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

- ARP with bandwidth limitation
- PROFINET DCP with bandwidth limitation
- In routing mode: LLDP frames (Ethertype 0x88CC) S≥V4.0

⑤ In bridge mode: MAC protocols sent through an IPsec tunnel are permitted.

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

- PROFINET
- In routing mode: LLDP frames (Ethertype 0x88CC) S≥V4.0

⑦ Multicast and broadcast frames of the following type from external to the security module are allowed:

- PROFINET with bandwidth limitation

Note

Automatic enabling of Ethertypes

If PPPoE is active, the Ethertypes 0x8863 and 0x8864 are automatically allowed (PPPoE Discovery and Session Stage).

Default setting for SCALANCE S623/S627-2M

The default firewall rules for the external and internal interfaces correspond to the rules applying to SCALANCE S modules of the type S602 and S612. Only IP packet filter rules relating to the DMZ interface are shown in the following two figures. MAC packet filter rules cannot be defined for the DMZ interface because the frames are routed between the external or internal network and DMZ interface.

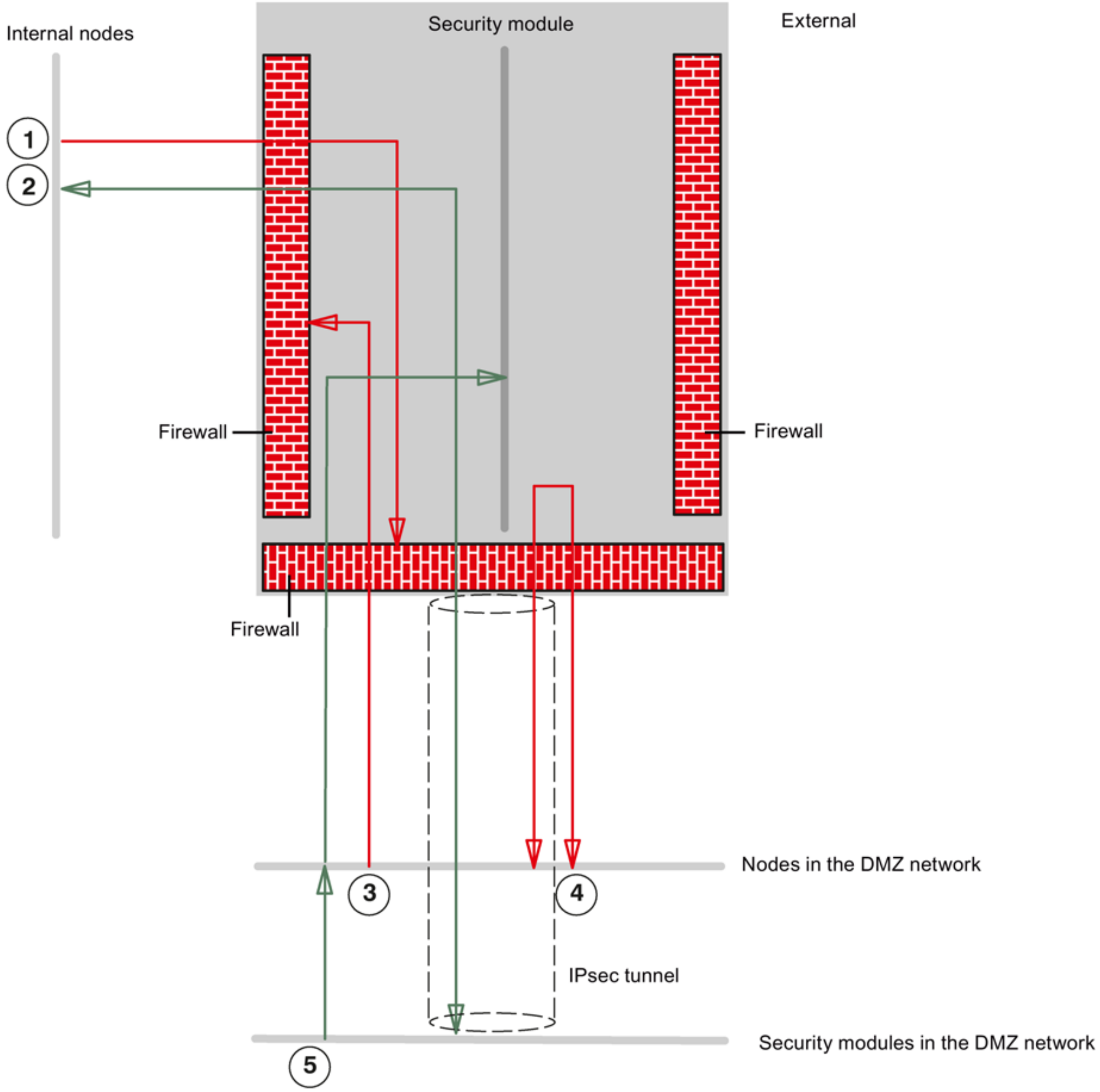


Figure 4-7 Default setting for IP packet filter SCALANCE S623/S627-2M (traffic between DMZ network and internal network or DMZ network and security module)

①All frames from internal to DMZ network are blocked.

②All frames from internal to tunnel on the DMZ interface and vice versa are allowed.

③All frames from DMZ network to internal are blocked.

④All frames from the DMZ network to tunnel on the DMZ interface and vice versa are blocked.

⑤Frames of the following type from DMZ network (nodes in the DMZ network and security modules in the DMZ network) to the security module are permitted:

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

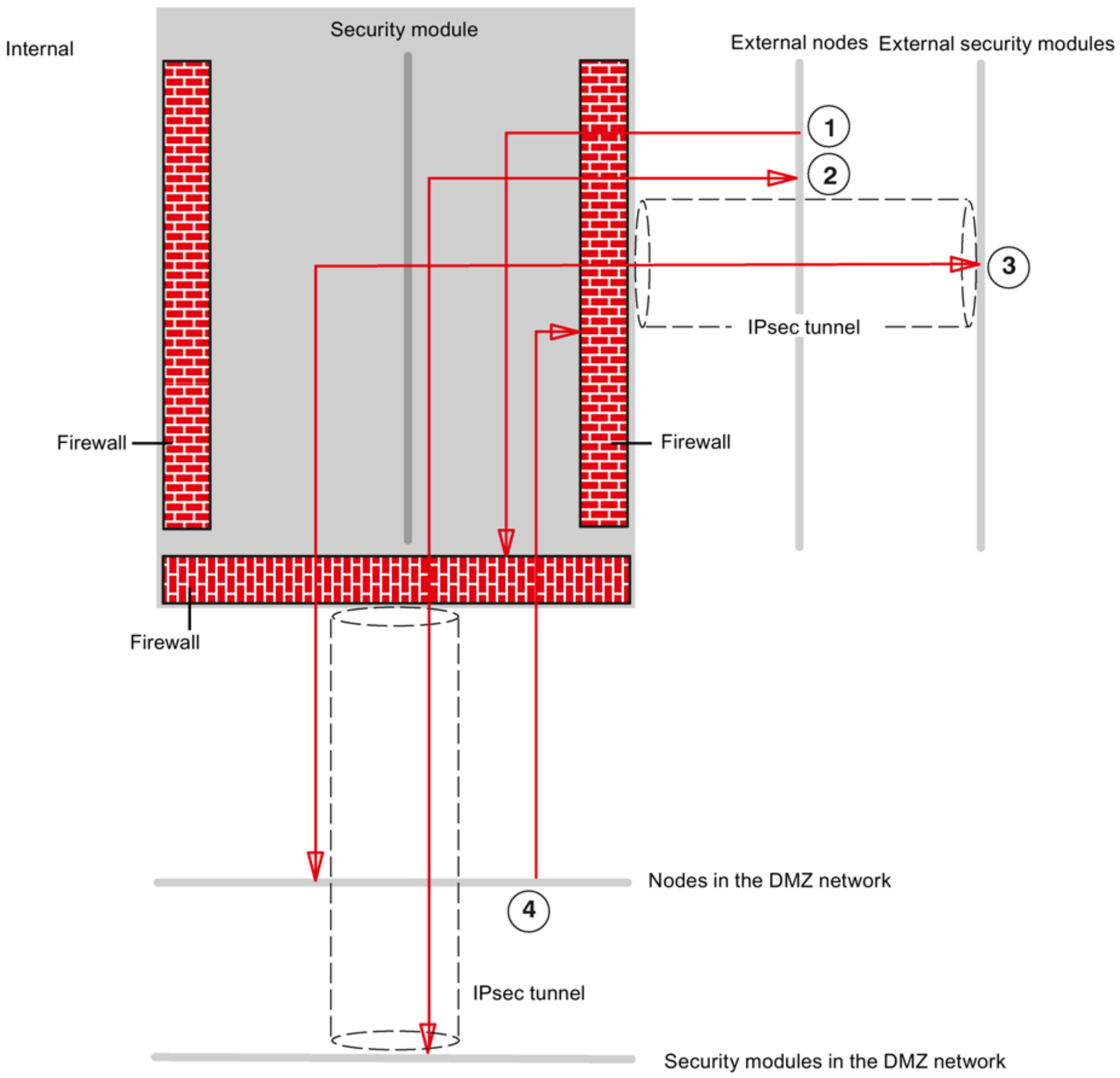


Figure 4-8 Default setting for IP packet filter SCALANCE S623/S627-2M (traffic between DMZ network and external network)

① All frames from external to DMZ network are blocked.

② All frames from external to tunnel on the DMZ interface and vice versa are blocked.

③ All frames from the DMZ network to tunnel on the external interface and vice versa are blocked.

④ All frames from the DMZ network to external are blocked

Note

Automatic enabling of Ethertypes

If PPPoE is active, the Ethertypes 0x8863 and 0x8864 are automatically allowed (PPPoE Discovery and Session Stage).

4.2.2 Configuring a firewall for SCALANCE S

How to access this function

1. Select the security 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 automatically active and all access from external to the security module is blocked. By clicking the relevant check box in standard mode, enable the firewall for the specific directions.

Detailed firewall settings in advanced mode

In advanced mode, you can restrict firewall rules to individual nodes, refer to the following section:

- Firewall in advanced mode (Page 136)

Firewall configuration with VPN

If the security module is in a VPN group and if the "Tunnel communication only" check box is selected in standard mode, only encrypted IPsec data transfer is allowed via the external interface or the DMZ interface. Only HTTPS access to the module (TCP port 443) remains allowed untunneled.

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 (IP traffic)

Service	Internal ⇒ External	External ⇒ Internal	internal => DMZ S62x	DMZ => Internal S62x	From internal	From external	Enabled ports	Meaning
Allow IP communication	x	x	x	x	-	-	-	IP communication for the selected communication directions is allowed.
Allow S7 protocol	x	x	x	x	-	-	TCP port 102	Communication of the nodes using the S7 protocol is allowed.
Allow FTP/FTPS (explicit mode)	x	x	x	x	-	-	TCP port 20 TCP port 21	For file management and file access between server and client.
Allow HTTP	x	x	x	x	-	-	TCP port 80	For communication with a Web server.
Allow HTTPS	x	x	x	x	-	-	TCP port 443	For secure communication with a Web server, for example, for Web diagnostics.
Allow DNS	x	x	x	x	-	-	TCP port 53 UDP port 53	Communications connection to a DNS server is allowed.
Allow SNMP	x	x	x	x	-	-	TCP port 161/162 UDP port 161/162	For monitoring nodes capable of SNMP.
Allow SMTP	x	x	x	x	-	-	TCP port 25	For the exchange of e-mails between authenticated users via an SMTP server.
Allow NTP	x	x	x	x	-	-	UDP port 123	For synchronization of the time of day.
Allow DHCP	x	x	x	x	-	-	UDP Port 67 UDP Port 68	Communication with a DHCP server is allowed.

Service	Internal ⇒ External	External ⇒ Internal	internal => DMZ S62x	DMZ => Internal S62x	From internal	From external	Enabled ports	Meaning
Allow MAC level communication	-	-	-	-	x	x	-	The MAC traffic from internal to external and vice versa is allowed.
Allow ISO communication	-	-	-	-	x	x	-	The ISO traffic from internal to external and vice versa is allowed.
Allow SiCLOCK	-	-	-	-	x	x	-	SiClock time frames from internal to external nodes and vice versa are allowed.
Allow DCP	-	-	-	-	x	x	-	Internal to external or external to internal DCP traffic for IP address assignment is allowed.

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.

4.3 Firewall 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: 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. For further information on symbolic names, refer to the section:

- You can assign symbolic names for IP / MAC addresses. (Page 67)

4.3.1 Configuring the firewall in advanced mode

Meaning

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:

- Layer 3, 4: IP protocol, IP services
- Layer 2: MAC protocol, MAC services

Note

No MAC rules if routing mode is enabled

SCA. S

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 of the firewall apply. For more detailed information, refer to the following section:

- Default settings for CP x43-1 Adv.: Default firewall setting (Page 117)
- Default settings for CP 1628: Default firewall setting (Page 123)
- Default settings for SCALANCE S: Default firewall setting (Page 128)

Global, user-specific and local definition possible

- Global firewall rule sets can be assigned to several security modules at the same time. They are displayed in the navigation panel in advanced mode of the Security Configuration Tool and configured globally.
- User-specific IP rule sets can be assigned to individual or several security modules at the same time. They are displayed in the navigation panel in advanced mode of the Security Configuration Tool and configured globally.
  SCALANCE S V4 (RADIUS): User-specific IP rule sets can be assigned individual or multiple users as well as individual or multiple roles.
- Local firewall rules are assigned to one security module. They are configured in the properties dialog of the security modules.

Several local firewall rules, several global firewall rule sets and several user-specific IP rule sets can be assigned to a security module.

4.3.2 Global firewall rule sets

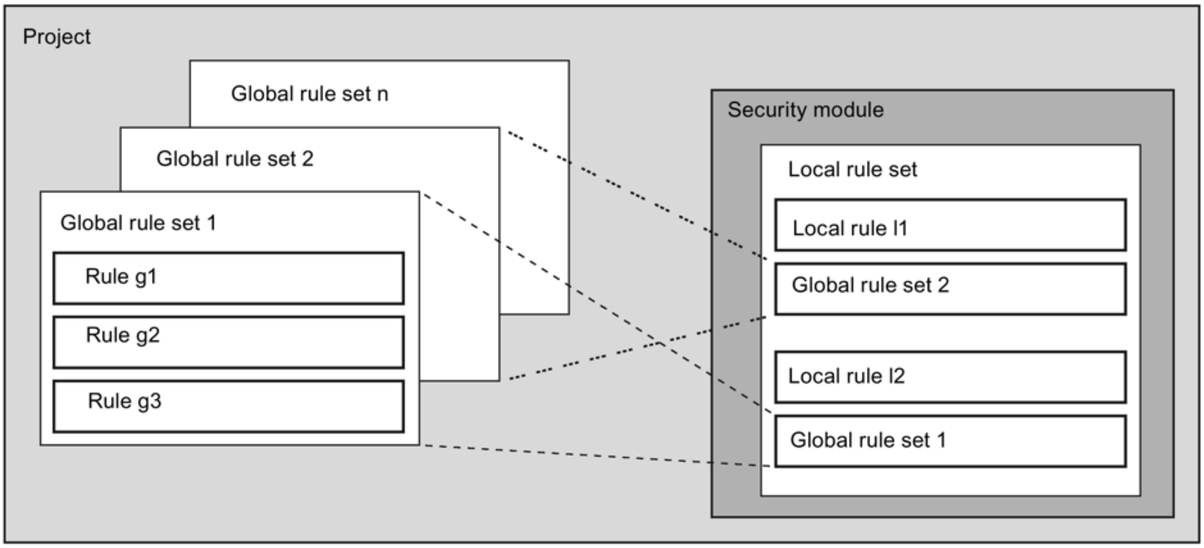
Application

Global firewall rule sets are configured depending on the module at project level and are visible in the navigation panel of the Security Configuration Tool. A global firewall rule set consists of one or more firewall rules and is assigned to the several security modules.

In the global firewall rule sets, a distinction is made between 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 firewall rule sets useful?

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

Note

Only assign firewall rule sets that are supported by the security module

A bad assignment of firewall rule sets 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 IP rule sets (Page 149)

4.3.2.1 Global firewall rule sets - conventions

Global firewall rule sets are used locally

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

- Configuration view

  Global firewall rule sets can only be created, edited, exported and imported in advanced mode.

- Priority

  As default, locally defined firewall rules have a higher priority than the global firewall rule sets that were assigned locally. Global firewall rule sets are therefore initially entered at the bottom of the local rule list.

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

- Entering, changing or deleting rule sets

  Global firewall rule sets 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.

  In the local rule list, an individual firewall rule of an assigned global firewall rule set cannot be deleted. Only the entire firewall rule set can be removed from the local list of rules. Adaptation of the global rule set is possible at any time using the properties dialog of the global rule set.
  All devices affected by this change must then be downloaded again.

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 155).

   For MAC rule sets: MAC packet filter rules (Page 164).

6. Assign the global firewall rule set to the security modules in which you want it to be used. To do this, select the global firewall rule set in the navigation panel and drag this to the security modules in the navigation panel (drag and drop). As an alternative, you can make the assignment in the local rule list of a security module using the "Add rule sets..." button.

Result

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

See also

Global firewall rule sets - conventions (Page 139)

4.3.2.3 Exporting and importing global firewall rule sets

Meaning and function

Global IP rule sets and global MAC rule sets can be exported from SCT in the XLSX format and imported into SCT. Per firewall rule set an XLSX file is created when you export.

The export and import provides the option of exchanging firewall rule sets between different SCT projects. Exported firewall rule sets can also be edited in Microsoft Excel® and then imported into SCT again. This simplifies the making of mass changes.

Firewall rule sets exported from SCT are fully compatible with STEP 7 Professional. Firewall rule sets exported from STEP 7 Professional are largely compatible with SCT.

Note

Restrictions when importing firewall rule sets from STEP 7 Professional into the Security Configuration Tool

In SCT IPv6 firewall rules and ICMPv6 services are not supported. During import firewall rules identified as IPv6 firewall rules and ICMPv6 services are ignored.

As the bandwidth limit a maximum of 100 Mbps are permitted in SCT. During import firewall rules with more than 100 Mbps are ignored.

Note

Released configuration limits

The export and import has been released for a maximum of 1000 firewall rule sets each with a maximum 1000 firewall rules.

Exporting firewall rule sets from SCT

1. In the navigation area, select the firewall rule sets you want to export. If you want to export all IP rule sets or all MAC rule sets, select the corresponding folder in the navigation area.
2. Select the "Export rule sets..." menu command.
3. Select a path on which the firewall rule sets will be saved.

Result: Per firewall rule set an XLSX file was created. The XLSX files were named with the name of the corresponding firewall rule set and according to the date and time of the export.

Importing firewall rule sets into SCT

Exported firewall rule sets can be edited prior to importing them. Refer to the information in the section “Requirements for firewall rule sets to be imported".

Follow the steps outlined below to import firewall rule sets into SCT:

1. In the navigation area, select the folder "Firewall IP rule sets" or the folder "Firewall MAC rule sets". With this selection you do not restrict the importable firewall rule sets.
2. Select the "Import rule sets..." menu command.
3. Select the XLSX files to be imported. Multiple selection is possible.
4. Specify whether existing entries should be overwritten by the import.

   Note: For the comparison between the firewall rule sets existing in SCT and the XLSX files, only the name of the firewall rule sets is used. The information about the date and time of the XLSX files is ignored.

Result: The firewall rule sets of the selected XLSX files have been imported into SCT.

Structure of exported IP rule sets

For every IP rule set exported from SCT, an XLSX file is created with the following table sheets:

- IP Ruleset: Contains the IP packet filter rules of the IP rule set
- IP Services: Contains the IP services used in packet filter rules of the IP rule set. IP services in the IP service groups used are also displayed.
- ICMP Services: Contains the ICMP services used in packet filter rules of the IP rule set. ICMP services in the IP service groups used are also displayed.
- IP Service Groups: Contains the IP service groups used in IP packet filter rules of the IP rule set. The corresponding IP and ICMP services are displayed for every IP service group.

Structure of exported MAC rule sets

For every MAC rule set exported from SCT, an XLSX file is created with the following table sheets:

- MAC Ruleset: Contains the MAC packet filter rules of the MAC rule set
- MAC Services: Contains the MAC services used in MAC packet filter rules of the MAC rule set. MAC services in the MAC service groups used are also displayed.
- MAC Service Groups: Contains the MAC service groups used in MAC packet filter rules of the MAC rule set. The corresponding MAC services are displayed for every MAC service group.

Conventions for rule sets to be imported

The following conventions apply to firewall rule sets to be imported into SCT:

- The files have the file extension*.XLSX and the corresponding Office Open XML format.
- If the name of the XLSX file is longer than 128 characters, the rule set will be created in SCT with a standard name.
- The names of the columns within the table sheets must not be changed, the order of the columns may, however, be changed.
- The names of the table sheets must not be changed, the order of the table sheets may, however, be changed.

Permitted parameter values for IP rule sets to be imported

The following values may be entered in the table columns of XLSX files for IP rule sets. Upper and lower case characters are not taken into account when the notation is checked.

Table 4- 9 Permitted parameter values for table sheet “IP Ruleset“

Action	From	To	IPv6*	Source IP address	Destination IP Address	Service	Bandwidth	Logging	Stateful	Comment
• Allow • Drop	External	• Internal • DMZ • Tunnel • Any • Station	False	[free text with max. 255 characters]	[free text with max. 255 characters]	[free text with max. 128 characters]	[Possible values: 0.001…100]	• True • False	• True • False	[free text with max. 255 characters]
	Internal	• External • Internal • DMZ • Tunnel • Any • Station								
	DMZ	• External • Internal • Tunnel • Any								
	Tunnel	• External • Internal • DMZ • Tunnel • Any • Station								
	Any	• External • Internal • DMZ								
	Station	• External • Internal • Tunnel								

* This column is optional. If the column does not exist when importing into SCT, the value “False” is used in SCT.

Table 4- 10 Permitted parameter values for table sheet “IP Services“

Name	Protocol	Source Port	Destination Port
[free text with max. 128 characters]	• UDP • TCP • All	[free text with max. 32 characters] If the character "*" is specified, no ports are checked.	[free text with max. 32 characters] If the character "*" is specified, no ports are checked.

Table 4- 11 Permitted parameter values for table sheet “ICMP Services“

Name	ICMPv6*	Type	Code
[free text with max. 128 characters]	False	• Star (No types are checked) • EchoReply • SourceQuench • AlternateHostAddress • EchoRequest • RouterSolicitation • TimestampReply • TimestampRequest • InformationRequest • InformationReply • AddressMaskReply • AddressMaskRequest • MobileHostRedirect • IpV6WhereAreYou • IpV6IAmHere • MobileRegistrationReply • MobileRegistrationRequest • Skip	NoCode

Name	ICMPv6*	Type	Code
		DestinationUnreachable	• Star (No codes are checked) • NetUnreachable • HostUnreachable • ProtocolUnreachable • PortUnreachable • FragmentationNeededAndDontFragmentWasSet • SourceRouteFailed • DestinationNetworkUnknown • DestinationHostUnknown • SourceHostIsolated • CommunicationWithDestinationNetworkIsAdministrativelyProhibited • CommunicationWithDestinationHostIsAdministrativelyProhibited • DestinationNetworkUnreachableForTypeOfService • DestinationHostUnreachableForTypeOfService • CommunicationAdministrativelyProhibited • HostPrecedenceViolation • PrecedenceCutOffInEffect
		Redirect	• Star (No codes are checked) • DatagramForNetwork • DatagramForTheHost • DatagramForTheTypeOfServiceAndNetwork • DatagramForTheTypeOfServiceandHost

Name	ICMPv6*	Type	Code
		RouterAdvertisement	• Star (No codes are checked) • NormalRouterAdvertisement • DoesNotRouteCommonTraffic
		TimeExceeded	• Star (No codes are checked) • TimeToLiveExceededInTransit • FragmentReassemblyTimeExceeded
		ParameterProblem	• Star (No codes are checked) • TheIpHeaderIsInvalid • ArequiredOptionIsMissing
		Traceroute	• Star (No codes are checked) • OutboundPacketSuccessfullyForwarded • NoRouteForOutboundPacketThePacketWasDiscarded

Name	ICMPv6*	Type	Code
		ConversionError	• Star (No codes are checked) • UnknownOrUnspecifiedError • DontConvertOptionPresent • UnknownMandatoryOptionPresent • KnownUnsupportedOptionPresent • Unsupported-TransportProtocol • OverallLengthExceeded • IpHeaderLengthExceeded • TransportProtocol-GreaterThen255 • PortConversionOutOfRange • TransportHeader-LengthExceeded • BitRollover-MissingAndAckSet • UnknownMandatoryTransportOption-Present
		Photuris	• Star (No codes are checked) • BadSpi • AuthenticationFailed • DecompressionFailed • DecryptionFailed • NeedAuthentication • NeedAuthorization

* This column is optional. If the column does not exist when importing into SCT, the value “False” is used in SCT.

Table 4- 12 Permitted parameter values for table sheet “IP Service Groups“

Name	Description	IP Services
[free text with max. 128 characters]	[free text with max. 255 characters]	[free text, services are separated from each other with commas]

If a service group is imported with an undefined service, the corresponding firewall rule set is discarded.

Permitted parameter values for MAC rule sets to be imported

The following values may be entered in the table columns of XLSX files for MAC rule sets. Upper and lower case characters are not taken into account when the notation is checked.

Table 4- 13 Permitted parameter values for table sheet “MAC Ruleset“

Action	From	To	Source MAC Address	Destination MAC Address	Service	Bandwidth	Logging	Comment
• Allow • Drop	External	• Internal • Tunnel • Any • Station	[MAC address in the correct format: xx-xx-xx-xx-xx-xx]	[MAC address in the correct format: xx-xx-xx-xx-xx-xx]	[free text with max. 128 characters]	[Possible values: 0.001…100]	• True • False	[free text with max. 255 characters]
	Internal	• External • Tunnel • Any						
	Tunnel	• External • Internal • Station						
	Any	• External • Internal						
	Station	• External • Tunnel						

Table 4- 14 Permitted parameter values for table sheet “MAC Services“

Name	Protocol	DSAP	SSAP	CTRL	OUI	OUI Type
[free text with max. 128 characters]	• SNAP • PROFINET IO • ISO • [hexadecimal values beginning with 0x]	[hexadecimal values with max. 2 characters]	[hexadecimal values with max. 2 characters]	[hexadecimal values with max. 2 characters]	[hexadecimal values with max. 6 characters]	[hexadecimal values with max. 4 characters]

You will find rules for permitted parameter values in the section defining MAC services (Page 168).

Table 4- 15 Permitted parameter values for table sheet “MAC Service Groups“

Name	Description	MAC Services
[free text with max. 128 characters]	[free text with max. 255 characters]	[free text, services are separated from each other with commas]

4.3.3 User-specific IP rule sets

SCA. S

Meaning

Initially, individual or multiple users are assigned to user-specific IP rule sets. The user-specific IP rule sets are then assigned to individual or multiple 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 nodes can be allowed temporarily for a user based on their IP addresses. This means that access is allowed for this user but access remains blocked for other users. The responses to user-specific access are always automatically allowed. This means that only IP rules for the initiative direction need to be configured.

User logon via the Internet

The user can log in to the external interface or the DMZ interface via the Web page of the security module. If authentication is successful, the IP rule set defined for the user for the IP address of the device from which the login is made is enabled.

The connection to the Web page 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 interface: 192.168.10.1

Call up of the login page with: https://192.168.10.1/

Users can log on with every role as long as the user or the role is assigned to a user-specific firewall rule set.

Options for authenticating the user

Depending on the authentication method selected when the user who will log in to the security module was created, the authentication is handled by different instances:

- Authentication method "Password": Authentication is handled by the security module.
- Authentication method "RADIUS": Authentication is handled by a RADIUS server.
  S≥V4.0

Assignment of roles to user-specific IP rule sets S≥V4.0

On SCALANCE S modules as of V4, it is also possible to assign user-specific IP rule sets that are assigned to roles. This makes it possible to enable a group of users for access to certain IP addresses.

If a RADIUS server is used for user authentication and a role is assigned to the user-specific IP rule set, users can also be authenticated by the RADIUS server although they are not configured on the security module. These users must be stored on the RADIUS server or on a separate database where they need to be assigned to the role assigned to the user-specific IP rule set in SCT. This procedure has the advantage that all user data is stored exclusively on the RADIUS server.

You will find more information on authentication by the RADIUS server in the following section:
Authentication using a RADIUS server (Page 81)

User-specific IP rule sets are used locally - conventions

The same conventions as described in the following section apply:

- Global firewall rule sets - conventions (Page 139)

4.3.3.1 Creating and assigning user-specific IP rule sets

How to access this function

1. In the navigation panel, 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 user-specific IP 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-specific IP 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 following section:
   - IP packet filter rules (Page 155)

   Note the special features of firewall rules generated automatically by SCT for NAT/NAPT rules:
   - Relationship between NAT/NAPT router and user-specific firewall (Page 191)

6. Assign one or more users and/or one or more roles to the user-specific IP rule set. The assignment of roles to user-specific IP rule sets is possible only for SCALANCE S V4 modules.

Note

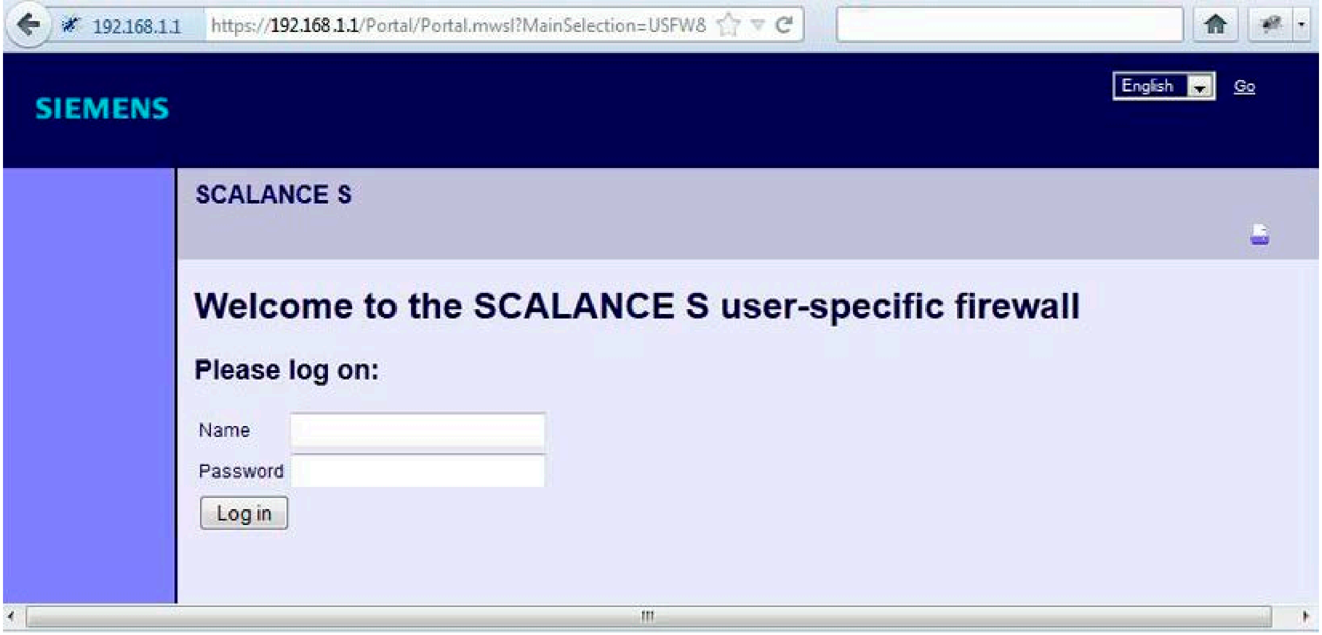
Assignment of user-specific IP rule sets

- A security module can only be assigned one user-specific rule set per user.
- Due to the assignment, the right "User/role may log in to module" is activated implicitly for all users or roles assigned to the IP rule set.

7. Assign the user-specific IP rule set to the security modules in which you want it to be used. To do this, select the user-specific IP rule set in the navigation panel and drag this to the security modules in the navigation panel (drag and drop). As an alternative, you can make the assignment in the local rule list of a security module using the "Add rule sets..." button.

Result

- The user-specific rule set is used by the assigned security modules as a local rule set and automatically appears in the module-specific list of firewall rules.
- The user can log on to the security module. Authentication of the user is performed depending on the selected authentication method either by the security module or a RADIUS server.



Welcome to the SCALANCE S user-specific firewall

Please log on:

Name

Password

Log in

Range of values for the maximum session time

The time after which the user is automatically logged out can be specified when creating or editing a user, the default is 30 minutes. On the Web page of the security module, the session time can be extended to the value assigned to the user.

You will find more information creating users in the following section:
Managing users (Page 70)

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/MAC address, the action and the interface are synchronized automatically. Regardless of the number of connections, 2 rules result per communications partner.

Note

Releasing UDP multicast connections manually

S7-CP

No automatic firewall rules are created for UDP multicast 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. If the security module is in a VPN group, the direction "External" changes to "Tunnel".

The IP address of the connection partner is entered in the "Source IP address" or "Destination IP address" column of these firewall rules.

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

~~PC CP~~

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, "Allow" rules are created for both directions. If the security module is in a VPN group, the direction "External" changes to "Tunnel".

The MAC address of the connection partner is entered in the "Source MAC address" or "Destination MAC address" column of these firewall rules.

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

Conventions for automatically created firewall rules

- Priority

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

- Deleting rules

  The rule sets cannot be deleted. Logging can be enabled and services can be assigned. You can also insert a bandwidth and a comment.

- 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 to retain your changes, select "Allow*" or "Drop*". In this case, only the IP address/MAC address is synchronized with STEP 7 and the action and direction remain as set. Settings for logging, service, bandwidth and comment are also retained after a renewed system synchronization even without changing the action to "Allow*" or "Drop*". If the corresponding connection does not exist in STEP 7, the rule is removed from the list.

Security module in VPN group

As default, the "Tunnel communication only" check box is enabled. If you deselect the check box, in addition to tunnel communication between tunnel partners, communication is also possible with network nodes to which there is no tunnel.

- 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". To avoid this adaptation being overwritten by the next system synchronization, the "Allow*" or "Drop*" action must be selected.

Note

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

To allow only tunneled communication for a CP, add a rule with the following settings:

- "Action": "Drop"
- "From": "Any"
- "To": "External"

For the CP 1628, add a rule with the following settings:

- "Action": "Drop"
- "From": "Station"
- "To": "External"

In addition to this, you need to remove existing firewall rules that allow untunneled communication.

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 security 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 firewall rule sets and user-specific rule sets you have assigned to the module are automatically entered in the local rule list. If the assigned 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 rules.

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: CP • 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.

Name	Meaning/comment	Available options / ranges of values
Source IP address	Source address of the IP packets **Note on user-specific IP rule sets** SCA. S If "Allow" is selected as the action, the entry "User IP address" is used as the source IP address. This means that the IP address of the device is used from which the user logged in to the Web page of the security module. If "Drop" is selected as the action, it is possible to select between the user IP address and all IP addresses.	Refer to the following section: • IP packet filter rules (Page 155) As an alternative, you can enter symbolic names. **Note on the ghost mode** S602 ≥V3.1 If ghost mode is activated, the IP address of the internal node is dynamically determined by the security module at runtime. Depending on the selected direction, you cannot make entries in the column "Source IP address" (for direction "From internal to external) or in the column "Target IP address" (for direction "From external to internal"). Instead, the IP address is inserted in the firewall rule automatically by the SCALANCE S itself.
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 • ICMP services • Service group including IP and/or ICMP services If you have not yet defined any services or want to define an additional service, click the "IP services…" button (in the "IP rules" tab) or "MAC services…" button (in the "MAC rules" tab).	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 Adv.: 0.001 ... 100 CP 1628 and SCALANCE S: 0.001 ... 1000 For rules in global and user-specific rule sets: 0.001 ... 100
Logging	Enable or disable logging for this rule. in Online mode, the "Packet filter log" tab displays the data packets to which the rule applies. For SCALANCE S modules, the numbers of the corresponding rules are displayed in the "Additional information" column. You will find further information on the logging settings in the following section: Logging events (Page 276)	

Name	Meaning/comment	Available options / ranges of values
No.	Automatically assigned number of the rule for assignment of the logged packets to a configured firewall rule. The numbers are recalculated when rules are moved.	
Stateful SCA. S	If this check box for an IP rule is disabled with the "Allow" action, no firewall Statesare generated by packets to which the allow rule applies. Firewall States automatically allow the responses to allowed packets. Can only be adapted if the "Allow" action is selected.	For allow rules: • enabled (default) • disabled For drop rules: • disabled (default)
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- 16 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- 17 SCALANCE S directions

Available options / ranges of values		Security module		
From	To	S602	S61x	S623 / S627-2M
Internal	External	x	x	x
	Tunnel	-	x	x
	Any	-	x	x
	DMZ	-	-	x
	Internal	x	x	x

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

Table 4- 18 Directions of IP packet filter rules of the user-specific firewall

Available options / ranges of values		Security module		
From	**To**	**S602**	**S61x**	**S623 / S627-2M**
Internal*	External	x	x	x
	DMZ	-	-	x
	Tunnel	-	x	x
External	Internal	x	x	x
	DMZ	-	-	x
DMZ	External	-	-	x
	Internal	-	-	x
Tunnel	External	-	x	x
	Internal	-	x	x
	DMZ	-	-	x

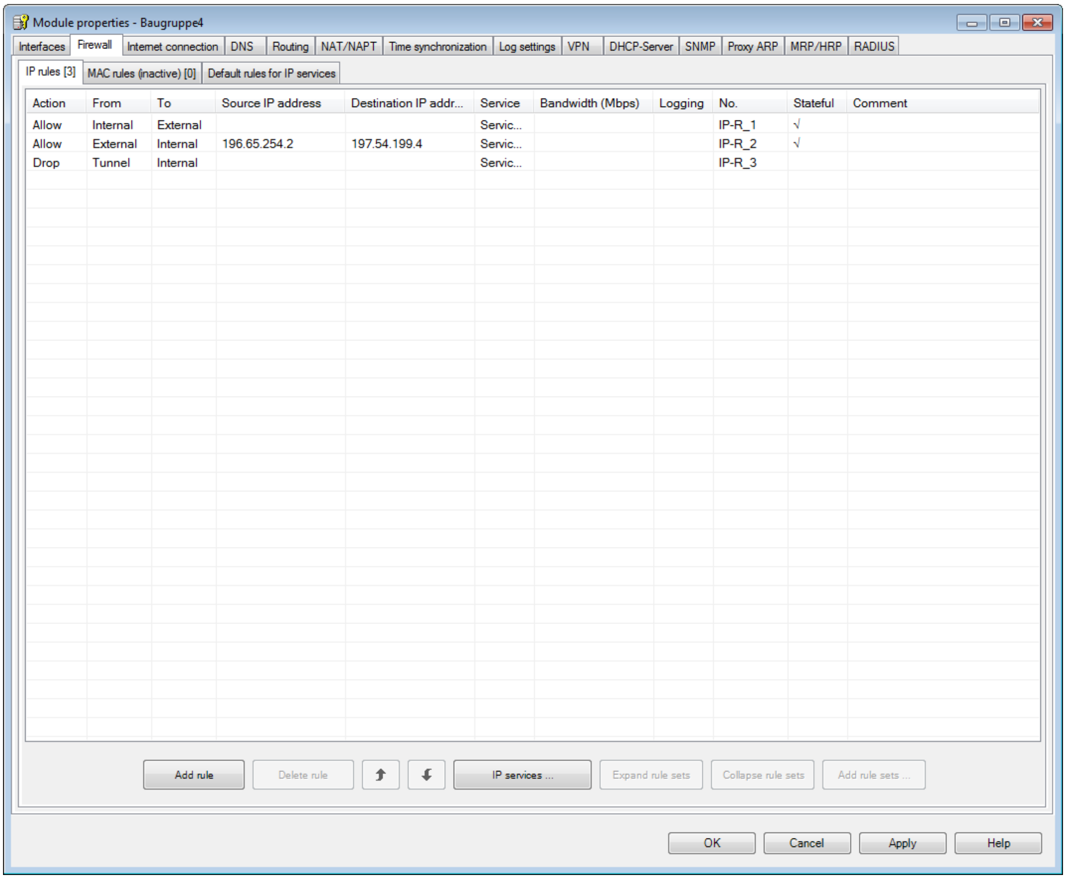
* Only available for drop rules

Order for rule evaluation by the security module

The packet filter rules are evaluated as follows:

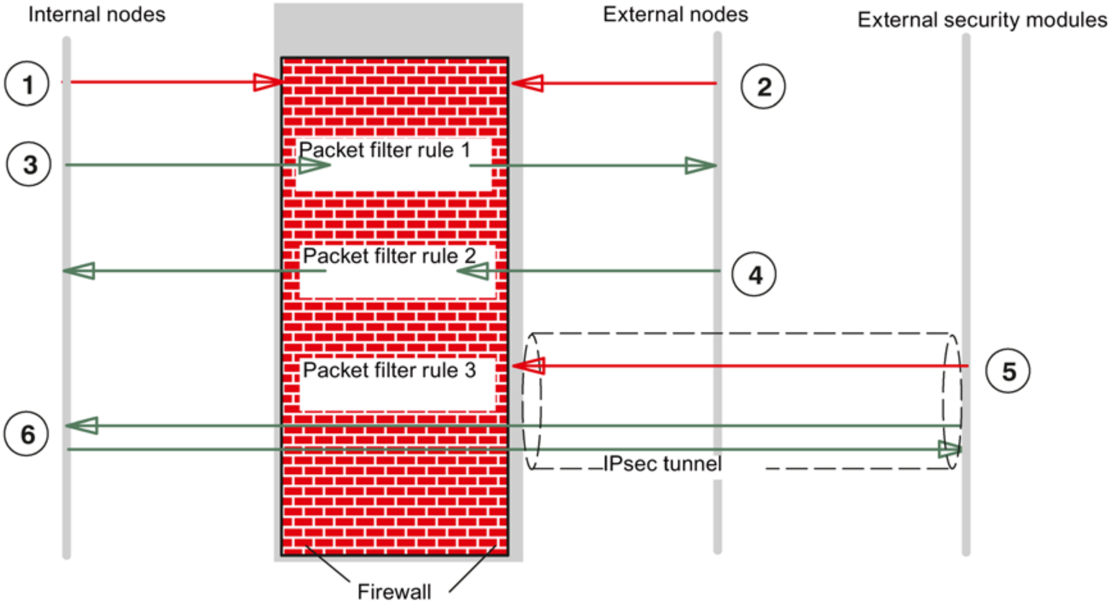
- The list is evaluated from top to bottom; if rules are contradictory (e.g entries with the same direction information but different actions), the rule higher in the list is therefore applied.
- In rules for communication between the internal network, external network and DMZ network, the following applies: All frames except for the frames explicitly allowed in the list are blocked.
- In rules for communication to and from the IPsec tunnel, the following applies: All frames except for the frames explicitly blocked in the list are allowed.

Example



Action	From	To	Source IP address	Destination IP addr...	Service	Bandwidth (Mbps)	Logging	No.	Stateful	Comment
Allow	Internal	External			Servic...			IP-R_1	√	
Allow	External	Internal	196.65.254.2	197.54.199.4	Servic...			IP-R_2	√	
Drop	Tunnel	Internal			Servic...			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 packets 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" sent from the VPN tunnel to the internal network.

⑥ IPsec tunnel communication is allowed as default except for the explicitly blocked frame types.

See also

MAC packet filter rules (Page 164)

Range of values for IP address, subnet mask and address of the gateway (Page 287)

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.

- Multiple IP addresses

  The rule applies to the specified addresses.

  The addresses are specified separated by a semicolon.
- 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 area

  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 the following section:

- Range of values for IP address, subnet mask and address of the gateway (Page 287)

Table 4- 19 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

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 rules, you use this name.

Parameters for IP services

You define the IP services using the following parameters:

Table 4- 20 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 All
Source port	TCP/UDP port or port range Filtering is based on the port numbers specified here; these define the service access at the frame sender.	With the protocol selection "All", it is not possible to specify a port. If the character "*" is specified, no ports are checked. Example of entering a port range: 78:99
Destination port	TCP/UDP port or port range Filtering is based on the port numbers specified here; these define the service access at the frame recipient.	With the protocol selection "All", it is not possible to specify a port. If the character "*" is specified, no ports are checked. Example of entering a port range: 78:99

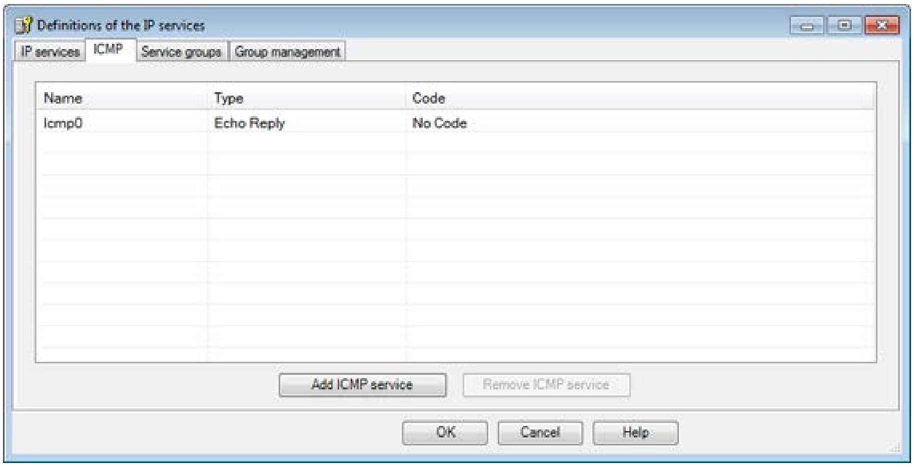
4.3.8 Defining ICMP services

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...", "ICMP" tab.

  or
- From the "IP rules" tab with the "IP services..." button, "ICMP" tab



Name	Type	Code
Icmp0	Echo Reply	No Code

Parameters for ICMP services

You define the ICMP services using the following parameters:

Table 4- 21 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

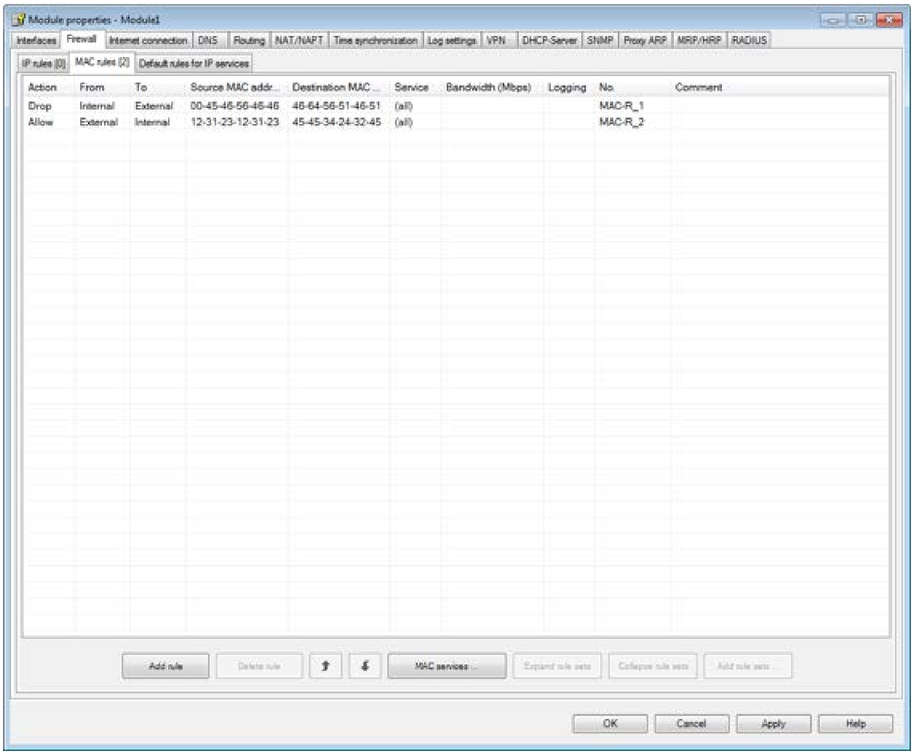
SCA. S

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

Dialog / tab

Select the security module to be edited.

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



Action	From	To	Source MAC addr...	Destination MAC ...	Service	Bandwidth (Mbps)	Logging	No.	Comment
Drop	Internal	External	00-45-46-56-46-46	46-64-56-51-46-51	(all)			MAC-R_1	
Allow	External	Internal	12-31-23-12-31-23	45-45-34-24-32-45	(all)			MAC-R_2	

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 firewall rule sets

Global firewall rule sets you have assigned to the module are automatically entered in the local rule list. If the assigned 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.

HLP
F1

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.

Configuring your own rules for ARP frames SCA. S

As default there are MAC packet filter rules on the security module that allow ARP frames from external to internal and from external to the security module. If you select the "Use your own ARP rules (the predefined ARP rules are disabled)" check box, these predefined ARP rules are disabled and you can define your own ARP rules by selecting the entry "ARP" as the service in a MAC packet filter rule. If the check box is selected, without your own ARP rules no communication with the security module or via the security module is possible. Your own ARP rules should also take into account the PC with which the security module is configured. For SCALANCE S602 modules in ghost mode, your own ARP rules are not supported.

MAC packet filter rules

The configuration of a MAC rule includes the following parameters:

Table 4- 22 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: CP • 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.
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 Adv.: 0.001 ... 100 CP 1628 and SCALANCE S: 0.001 ... 1000 For rules in global and user-specific rule sets: 0.001 ... 100
Logging	Enable or disable logging for this rule. in Online mode, the "Packet filter log" tab displays the data packets to which the rule applies. For SCALANCE S modules, the numbers of the corresponding rules are displayed in the "Additional information" column. You will find further information on the logging settings in the following section: Logging events (Page 276)	

Name	Meaning/comment	Available options / ranges of values
No.	Automatically assigned number for assignment to a configured firewall rule. The numbers are recalculated when rules are moved.	
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- 23 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- 24 Firewall directions SCALANCE S

Available options / ranges of values		Security module		
From	To	S602	S61x	S623 / S627-2M
Internal	External	x	x	x
	Tunnel	-	x	x
	Any	-	x	x
External	Internal	x	x	x
	Any	-	-	x
	Tunnel	-	-	x
Tunnel	Internal	-	x	x
	External	-	x	x
Any	Internal	-	x	x
	External	-	-	x

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 applied.
- The following applies to all frames not explicitly listed in the rules for communication in the direction to "External" or from "External": All frames except for the frames explicitly allowed in the list are blocked.
- The following applies to all frames not explicitly listed in the rules for communication in the direction to "Tunnel" or from "Tunnel": All frames except for the frames explicitly blocked in the list are allowed.

Note

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 155) 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- 25 MAC services - parameters

Name	Meaning/comment	Available options / ranges of values
Name	Name for the service that is used as identification in the rule definition or in the group.	Can be selected by user Exception: The name "ARP" is not permitted for MAC services.

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)	
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 IO
- SiCLOCK:

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

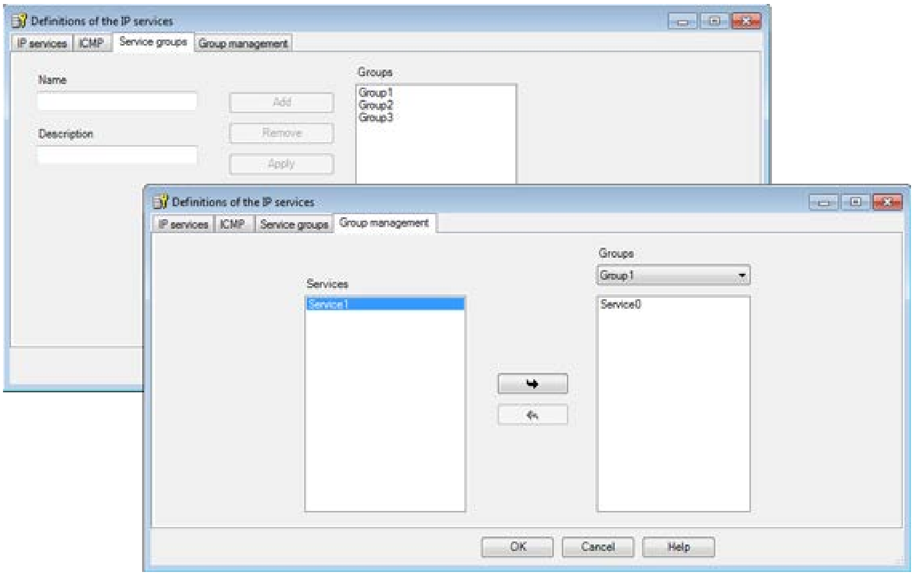
4.3.12 Setting up service groups

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

You open the dialog with the following menu command:
"Options" > "IP services..." or "MAC services...", "Service groups" tab. For MAC service groups the name "ARP" is not permitted.



4.3.13 Adjusting standard rules for IP services

~~PC CP~~

How to access this function:

1. Select the security module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Firewall" tab > "Default rules for IP services" tab.

Meaning of the advanced settings

Parameter	Meaning when activated
Use advanced status options	If you enable this check box, connections and firewall states are limited for network nodes. The limitations are as follows: • Max. 200 connections in 5 seconds • Max. 2000 firewall states If a network node exceeds one of these limits, its IP address is entered in the IP blacklist of the security module. The node can then no longer communicate via the security module. The IP blacklist of the security module can be viewed in online mode.
Log all activated rules	Packets that are allowed according to the default rules for IP services are logged.
Enable ICMP test for interfaces	Ping queries coming in on an interface of the security module can be forwarded to other interfaces. This means that, for example, ping queries can be made from the external network to the internal interface of the security module.

Meaning of the default firewall rules

This dialog allows you to adjust the service-specific firewall rules set as default for the interfaces of the security module. The standard settings of the dialog correspond to the standard firewall rules of the particular security module.

Default firewall rules for SCALANCE S

The following table lists the default firewall rules for SCALANCE S modules. In some cases, the firewall rules are only set if the relevant service is used by the security module (e.g. SNMP).

Service	Direction	X1 interface (red)	Interface X2 (green)	Interface X3 (yellow) S62x	Tunnel interface ~~S602~~
Interface rerouting	outgoing	-	x	-	-
HTTPS		x	x*	x	x*

Service	Direction	X1 interface (red)	Interface X2 (green)	Interface X3 (yellow) S62x	Tunnel interface ~~S602~~
ICMP	incoming	-	x	-	x
ICMP pathfinder S602 ≥V3.1	outgoing	-	x	-	-
SNMP	incoming	x	x	x	x
Syslog	outgoing	x	x	x	x
NTP	outgoing	x	x	x	x
DNS	outgoing	x	x	x	x
HTTP	outgoing	x	-	x	-
VPN (IKE)		x	-	x	-
VPN (NAT Traversal)		x	-	x	-
BootP Server	incoming	-	x	x	-
BootP Client	outgoing	-	x	x	-
RADIUS	outgoing	x	x	x	x
CARP S62x ≥ V4.0	outgoing	x*	x*	-	-
Pfsync S62x ≥ V4.0	outgoing	-	-	x*	-

x enabled as default

- disabled as default

* cannot be adapted

Default firewall rules for S7 CPs

The following table lists the default firewall rules for S7 CPs. In some cases, the firewall rules are only set if the relevant service is activated in the Security Configuration Tool.

Service	Direction	External (Gbit)	Internal (PN-IO)
VPN (IKE)		x*	-*
VPN (NAT traversal)		x*	-*
BootP Server	outgoing	x*	x*
BootP Client	incoming	x*	x*

x enabled as default

- disabled as default

* cannot be adapted

The two services "BootP Server" and "BootP Client" are both active together either on the external interface or on the internal interface. Accordingly, either both firewall rules are active on the external interface or they are both active on the internal interface.

Configuring additional module properties 5

5.1 Security module as router

5.1.1 Overview

Meaning

By using the security module as router, the networks become separate subnets on the internal, external and DMZ interface (SCALANCE S623/S627-2M only, see section below).

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 router to a different subnet, see following section:

- Specifying a standard router and routes (Page 174)

Enable routing mode or DMZ interface - "Interfaces" tab

SCA. S

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

For this mode, you need to configure an IP address and a subnet mask for addressing the router on the internal subnet and/or on the DMZ subnet for the internal interface and/or for the DMZ interface. 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.

Bridge and routing mode with SCALANCE S623/S627-2M

The DMZ network is always a separate subnet. The difference between bridge and routing mode lies in the division of the external and internal network:

- "Bridge" mode: Internal and external network are in the same subnet; DMZ network is in a separate subnet.
- "Routing" mode: Internal and external network are each in their own subnet; DMZ network is in an additional separate subnet.

5.1.2 Specifying a standard router and routes

SP

How to access this function

1. Select the security module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Routing" tab.
3. If you enter the IP address / FQDN for the standard router, all routes are directed via this router if no specific routes apply. You can enter specific routes in the "Routes" input area.
4. Click the "Add route" button.
5. Enter the following values:

Parameter	Function	Example of a value
Network ID	Requests to nodes of the subnet with the network ID and the subnet mask specified here are forwarded to the subnet via the specified router IP address. Based on the network ID, the router recognizes whether a target address is inside or outside the subnet. The specified network ID must not be located in the same subnet as the IP address of the security module.	192.168.11.0
Subnet mask	The subnet mask determines the network structure. Based on the network ID, the router recognizes whether a destination address is inside or outside the subnet. The subnet mask to be specified cannot be restricted to a single network node (255.255.255.255).	255.255.255.0
Router IP address	IP address / FQDN of the router that connects to the subnet. The IP address of the router must be in the same subnet as the IP address of the security module.	192.168.10.2 / my-router.dyndns.org
Activate rerouting	Select this check box if the frames of the entered route will enter and leave on the same interface of the security module (rerouting). Rerouting is only supported on the internal interface of the security module.	

Special features with a standard router

- If the IP assignment configured is via "PPPoE" in the "Interfaces" tab, a configured standard router is ignored because the standard route is always automatically via the PPPoE interface.
- If the address assignment configured in the "Interfaces" tab is via a "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.
- For security modules in ghost mode (SCALANCE S602 ≥ V3.1 only), no standard routers can be configured since these are identified during runtime. Specific routes cannot be configured for security modules in ghost mode.

5.1.3 NAT/NAPT routing

~~PC CP~~

~~CP 443-1 OPC UA~~

Requirement

- The project is in advanced mode.
- The security module is in routing mode or the DMZ interface is activated (SCALANCE S623 / S627-2M only).

How to access this function

1. Select the security module to be edited.
2. Select the "Edit" > "Properties..." menu command, "NAT/NAPT" tab.
3. When required, enable address translation according to NAT(Network Address Translation) or NAPT (Network Address Port Translation).

Address translation with NAT (Network Address Translation)

NAT is a protocol for address translation 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 on the Internet. As a result, the IP 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 addresses 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 destination IP address and the destination port to a communications relation (port forwarding).

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

Address translation in VPN tunnels

Address translations with NAT/NAPT can also be performed for communications relations established via a VPN tunnel. This is supported for connection partners of the type SCALANCE M (only 1:1-NAT) and SCALANCE S612 / S623 / S627-2M V4.

You will find further information on address translations in VPN tunnels in the following sections:

- Address translation with NAT/NAPT (Page 177)
- Address translation with NAT/NAPT in VPN tunnels (Page 183)

Conversion of NAT/NAPT rules from old projects

With SCT V4.0, the configuration mode of NAT/NAPT rules and the corresponding firewall rules was changed. If you want to adapt or expand the NAT/NAPT rules from a project created with SCT V3.0/V3.1 in SCT V4.0, you first need to convert the NAT/NAPT rules to SCT V4.0. To do this, select the menu command "Convert all NAT/NAPT rules to SCT V4" or "Convert selected NAT/NAPT rule to SCT V4" in the shortcut menu of a NAT/NAPT rule. SCT will then automatically generate firewall rules for the converted NAT/NAPT rules that enable communication in the configured address translation direction. Then modify or remove the firewall rules you created manually for the NAT/NAPT rules if these contradict the automatically generated firewall rules. Then make the required adaptations and/or expansions to the NAT/NAPT and firewall rules.

Consistency check - these rules must be adhered to

Among other things, remember the following rules to obtain consistent entries:

- The IP address of the internal interface must not be used in the NAT / NAPT table.
- An IP address used in the NAT/NAPT address conversion list must not be a multicast or broadcast address.
- The external ports assigned for the NAPT translation are in the range > 0 and ≤ 65535.

  Port 123 (NTP), 443 (HTTPS), 514 (Syslog), 161 (SNMP), 67+68 (DHCP) and 500+4500 (IPsec) are excluded if the relevant services are activated on the security module.

- The external IP address of the security module or the IP address of the DMZ interface may only be used in the NAT table for the action "Source NAT".
- Checking for duplicates in the NAT table

  An external IP address or an IP address in the DMZ network used in the direction "Destination NAT" or "Source NAT +Destination NAT" may only occur once in the NAT table for each specified direction.
- Checking for duplicates in the NAPT table
  – The port numbers or port ranges of the "Source port" column must not overlap for an interface.
- Internal NAPT ports can be in the range > 0 and ≤ 65535.

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

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

5.1.4 Address translation with NAT/NAPT

Enabling NAT

The input boxes for NAT are enabled. NAT address translations only take effect with the entries in the address translation list described below. After creating NAT rules, the corresponding firewall rules are generated and displayed in advanced mode, see section: Relationship between NAT/NAPT router and firewall (Page 186)

If PPPoE is activated for the external interface or the DMZ interface, the action "Destination NAT" cannot be configured. When configuring the action "Source NAT", the IP address cannot be entered in the "Source translation" input box because this is obtained dynamically during runtime.

Possible address translations for NAT

The following tables show the input options for address translation with NAT.

Action "Destination-NAT" - "Redirect"

The action "Destination NAT" can be performed in the following direction:

- External to internal

If the DMZ interface of the security module (SCALANCE S623/S627-2M only) is activated, the action "Destination NAT" can also be performed in the following directions.

- External to DMZ
- DMZ to internal
- DMZ to external

If the SCALANCE S module is in a VPN group (not for SCALANCE S602), the action "Destination NAT" can also be performed in the following directions:

- Tunnel to internal
- Tunnel to external
- Tunnel to DMZ (only if the DMZ interface is activated)

The following applies, for example for the direction "external to internal": The destination IP address of a frame coming from the external network is checked to see whether it matches the IP address specified in the "Destination IP address" input box. If it matches, the frame is forwarded into the internal network by replacing the destination IP address of the frame with the IP address specified in the "Destination translation" input box. Access from external to internal using the external address is possible.

The following table shows the input required for the action "Destination NAT".

Box	Possible entries	Meaning
Source IP address	Not relevant for this action.	-
Source translation	Not relevant for this action.	-
Destination IP address	IP address in the source network	Destination IP address in the source network with which an IP address in the destination network will be accessed. The destination IP address must not match the IP address of the security module in the source network. If the destination IP address in a frame matches the address entered, the address is replaced by the corresponding IP address in the destination network. The specified destination IP address becomes the alias address. This means that the specified IP address is also registered as an IP address on the selected interface. Alias addresses are also shown in the "Interfaces" tab of the security module. Make sure that the alias address does not cause an IP address conflict in the network.
Destination translation	IP address in the destination network	The destination IP address is replaced by the IP address specified here.
No.	-	Consecutive number assigned by SCT used to reference the firewall rule generated by SCT for the NAT rule.

Action "Source NAT" - "Masquerading"

The action "Source NAT" can be performed in the following direction:

- Internal to external

If the DMZ interface of the security module (SCALANCE S623/S627-2M only) is activated, the action "Source NAT" can also be performed in the following directions.

- Internal to DMZ
- External to DMZ
- DMZ to external

If the SCALANCE S module is in a VPN group (not for SCALANCE S602), the action "Source NAT" can also be performed in the following directions:

- Internal to tunnel
- Tunnel to internal
- External to tunnel
- DMZ to tunnel (only if the DMZ interface is activated)

The following applies, for example for the direction "internal to external": The source IP address of a frame coming from the internal network is checked to see whether it matches the IP address specified in the "Source IP address" input box. If it matches, the frame with the external IP address specified in the "Source translation" input box is forwarded to the external network as a new source IP address. In the external network, the external IP address is effective.

The following table shows the input required for the action "Source NAT".

Box	Possible entries	Meaning
Source IP address	IP address in the source network	The source IP address of the specified node is replaced by the IP address specified in the "Source translation" input box.
	IP address range / IP address band in the source network	The IP addresses of the IP address range / IP address band are replaced by the IP address specified in the "Source translation" input box.
Source translation	IP address in the destination network	Entry of the IP address that will be used as the new source IP address. If the IP 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 an IP address on the selected interface. Alias addresses are also shown in the "Interfaces" tab of the security module. Make sure that the alias address does not cause an IP address conflict in the network.
Destination IP address	Not relevant for this action.	Not relevant for this action.
Destination translation	Not relevant for this action.	Not relevant for this action.
No.	-	Consecutive number assigned by SCT used to reference the firewall rule generated by SCT for the NAT rule.

Note

You can configure an address translation to the module IP address in the destination network for all frames going from a source network to a destination network. The security module also assigns a port number for each frame. This is an n:1 NAT address translation in which multiple IP addresses of the source network are translated to one IP address of the destination network.

Enter, for example, the following parameters for the direction "internal to external":

- Action: "Source NAT"
- From: "Internal"
- To "External"
- Source IP address: "*"
- Source translation: External IP address of the security module

Action "Source NAT + Destination NAT" - "1:1-NAT"

The action "Source NAT + Destination NAT" can be performed in the following direction:

- Internal to external

If the DMZ interface of the security module (SCALANCE S623/S627-2M only) is activated, the action "Source NAT + Destination" can also be performed in the following directions.

- Internal to DMZ
- External to DMZ
- DMZ to external

If the SCALANCE S module is in a VPN group (not for SCALANCE S602), the action "Source NAT + Destination NAT" can also be performed in the following directions:

- External to tunnel
- Internal to tunnel
- DMZ to tunnel (only if the DMZ interface is activated)

The following applies, for example for the direction "internal to external": When accessing from internal to external, the action "Source NAT" is performed. When accessing from external to internal, the action "Destination NAT" is performed.

The following table shows the input required for the action "Source NAT + Destination NAT":

Box	Possible entries	Meaning
Source IP address	IP address in the source network	The configuration is always specified in the source NAT direction. The IP addresses of the destination NAT direction are then inserted automatically by
	IP address range in the source network	

Box	Possible entries	Meaning
Source translation	IP address in the destination network	
Destination IP address	Not relevant for this action.	
Destination translation	Not relevant for this action.	
No.	-	Consecutive number assigned by SCT used to reference the firewall rules generated by SCT for the NAT rule.

Action "Double NAT"

The action "Double NAT" can be performed for SCALANCE S modules in the following directions:

- Internal to external
- External to internal

If the DMZ interface of the security module (SCALANCE S623/S627-2M only) is activated, the action "Double NAT" can also be performed in the following directions.

- Internal to DMZ
- External to DMZ
- DMZ to internal
- DMZ to external

In every direction, Source and Destination NAT always take place at the same time.
The following applies, for example for the direction "external to internal": When accessing from external to internal, the source IP address of the external node is replaced (Source NAT). Access to the internal network also uses the external IP address specified in the "Destination IP address" input box (Destination NAT).

You can, for example, use this action if a standard router other than the security module is entered for a device to be accessed using Destination NAT. Response frames from this device are then not sent to the entered standard router but to the corresponding interface of the security module.

The following table shows the input required for the action "Double NAT".

Box	Possible entries	Meaning
Source IP address	IP address in the source network	IP address of the node in the source network
Source translation	-	The Source NAT address translation is always to the IP address of the security module in the destination network. For this reason, the "Source translation" input box cannot be configured.

Box	Possible entries	Meaning
Destination IP address	IP address in the source network	Destination IP address in the source network with which an IP address in the destination network will be accessed. If the destination IP address in a frame matches the IP address entered, the IP address is replaced by the IP address specified in the "Destination translation" input box. If the IP 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 an IP address on the selected interface. Alias addresses are also shown in the "Interfaces" tab of the security module. Make sure that the alias address does not cause an IP address conflict in the network.
Destination translation	IP address in the destination network	The destination IP address is replaced by the IP address specified here.
No.	-	Consecutive number assigned by SCT used to reference the firewall rule generated by SCT for the NAT rule.

Enabling NAPT

The input boxes for NAPT are enabled. NAPT translations only take effect with the entries in the list described below. After creating NAPT rules, the corresponding firewall rules are generated and displayed in advanced mode, see section:
Relationship between NAT/NAPT router and firewall (Page 186)

The IP address translation with NAPT can be performed in the following direction:

- External to internal

If the DMZ interface of the security module (SCALANCE S623/S627-2M only) is activated, the IP address translation with NAPT can also be performed in the following directions.

- External to DMZ
- DMZ to internal
- DMZ to external

If the SCALANCE S module is in a VPN group (not for SCALANCE S602), IP address translation with NAPT can also be performed in the following directions:

- External to tunnel
- Tunnel to internal
- Tunnel to external
- DMZ to tunnel (only if the DMZ interface is activated)
- Tunnel to DMZ (only if the DMZ interface is activated)

The following applies, for example for the direction "external to internal": Frames intended for the external IP address of the security module and for the port entered in the "Source port" column are forwarded to the specified destination IP address in the internal network and to the specified destination port.

The following table shows the input required for address translation with NAPT.

Box	Possible entries	Meaning
Source port	TCP/UDP port or port range Example of entering a port range: 78:99	A node in the source network can send a frame to a node in the destination network by using one of the specified port numbers.
Destination IP address	IP address in the destination network	Frames intended for the IP address of the security module in the source network and the TCP/UDP port specified in the "Source port" box are forwarded to the IP address specified here.
Destination port	TCP/UDP port or port range A port range can only be specified when a port range is also specified in the "Source port" column. Both port ranges must include the same number of ports. Example of entering a port range: 78:99	Port numbers to which the frames coming from the source network can be forwarded.
Protocol	• TCP+UDP • TCP • UDP	Selection of the protocol family for the specified port numbers
No.	-	Consecutive number assigned by SCT used to reference the firewall rule generated by SCT for the NAPT rule.

See also

IP packet filter rules (Page 155)

5.1.5 Address translation with NAT/NAPT in VPN tunnels

~~S602~~

S≥V4.0

Meaning

Address translations with NAT/NAPT can also be performed for communications relations established via a VPN tunnel.

Requirements

The following requirements apply generally to a SCALANCE S module that will perform an address translation with NAT/NAPT in a VPN tunnel:

- The SCALANCE S module is in a VPN group.
- The SCALANCE S module is in routing mode and/or the DMZ interface of the SCALANCE S module is activated.
- The tunnel interface is enabled.

Supported address translation directions

The address translation directions described in the following section are supported:
Address translation with NAT/NAPT (Page 177)

Supported address translation actions

With tunneled communications relations, the following address translation actions are supported:

- Destination NAT ("Redirect")
- Source NAT ("Masquerading")
- Source and Destination NAT ("1:1-NAT")
- NAPT ("Port forwarding")

You will find basic information on these address translation actions in the following section:
Address translation with NAT/NAPT (Page 177)

Supported VPN links

In conjunction with NAT/NAPT, the following VPN links are supported:

VPN link		VPN link is initiated by	Address translation is performed by
SCALANCE S (a)	SCALANCE S (b)	SCALANCE S (a) or SCALANCE S (b)	SCALANCE S (a) and/or SCALANCE S (b)
SCALANCE S	S7-CP / PC-CP	SCALANCE S or S7-CP / PC-CP	SCALANCE S
SCALANCE S	SCALANCE M	SCALANCE M	SCALANCE S and/or SCALANCE M*
SOFTNET Security Client	SCALANCE S	SOFTNET Security Client	SCALANCE S
SCALANCE S	NCP VPN client (Android)	NCP VPN client (Android)	SCALANCE S

* Only 1:1 NAT is supported.

SCALANCE S modules of the type SCALANCE S623 V4 and SCALANCE S627-2M V4 that have a VPN endpoint on the external interface and on the DMZ interface can perform address translations on both interfaces at the same time.

Address translation characteristics when involved in several VPN groups

If a SCALANCE S module is a member of several VPN groups, the address translation rules configured for the tunnel interface of the SCALANCE S module apply for all VPN connections of this SCALANCE S module.

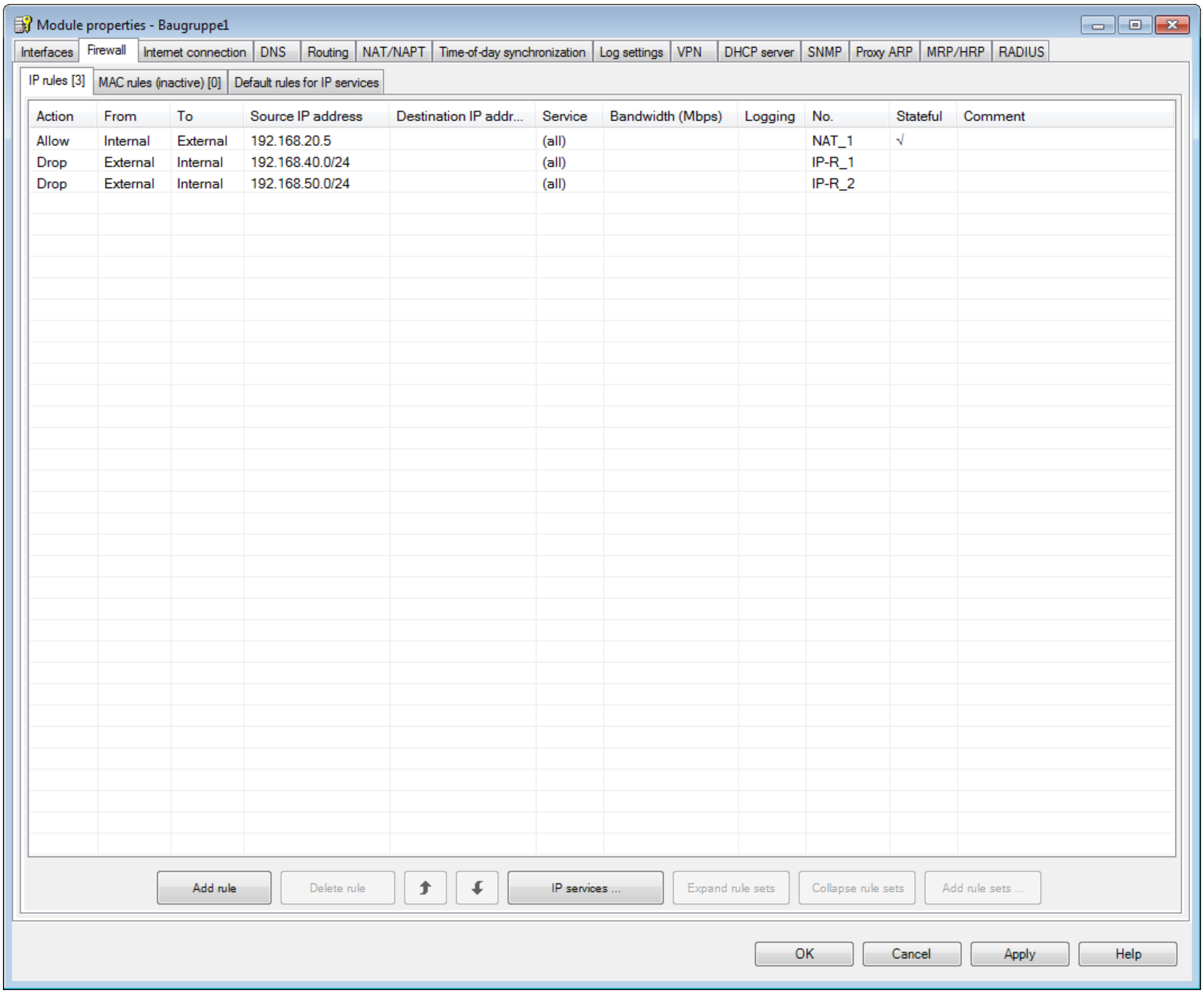
Note:

Once you have configured a NAT address translation to or from the direction of the tunnel, only the IP addresses involved in the NAT address translation rules can be reached via the VPN tunnel.

5.1.6 Relationship between NAT/NAPT router and firewall

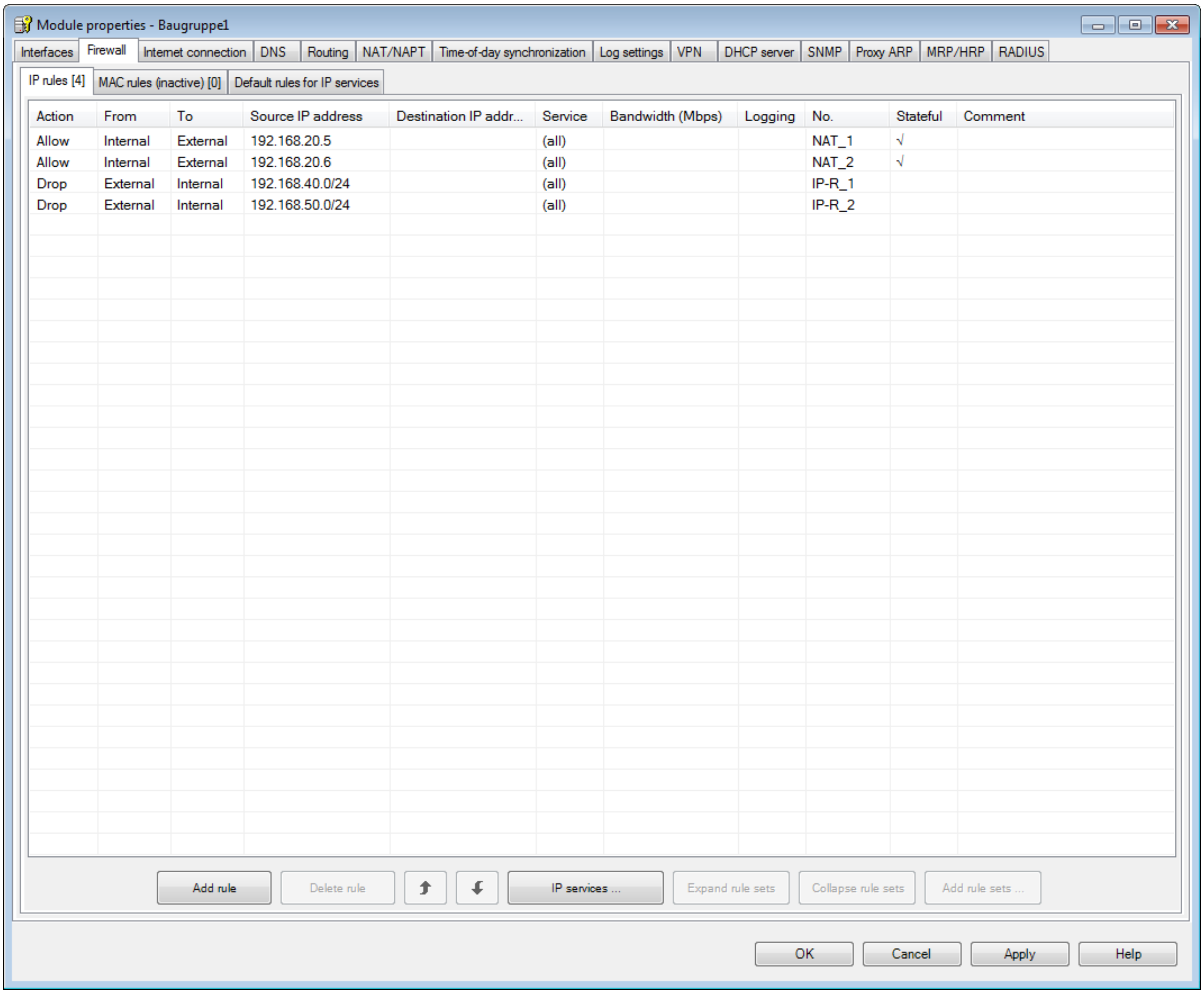
Meaning

After creating NAT/NAPT rules, SCT automatically generates firewall rules that enable communication in the configured address translation direction. To clarify the relationship between the NAT/NAPT rules and the corresponding firewall rules, the rules are identified by corresponding, consecutive numbers in the "NAT/NAPT" and "Firewall" tabs. The generated firewall rules can, if necessary, be expanded (additional IP addresses / IP address range / IP address band, services, bandwidth) and as default have the highest priority because SCT inserts them above existing firewall rules.



Action	From	To	Source IP address	Destination IP addr...	Service	Bandwidth (Mbps)	Logging	No.	Stateful	Comment
Allow	Internal	External	192.168.20.5		(all)			NAT_1	√	
Drop	External	Internal	192.168.40.0/24		(all)			IP-R_1		
Drop	External	Internal	192.168.50.0/24		(all)			IP-R_2		

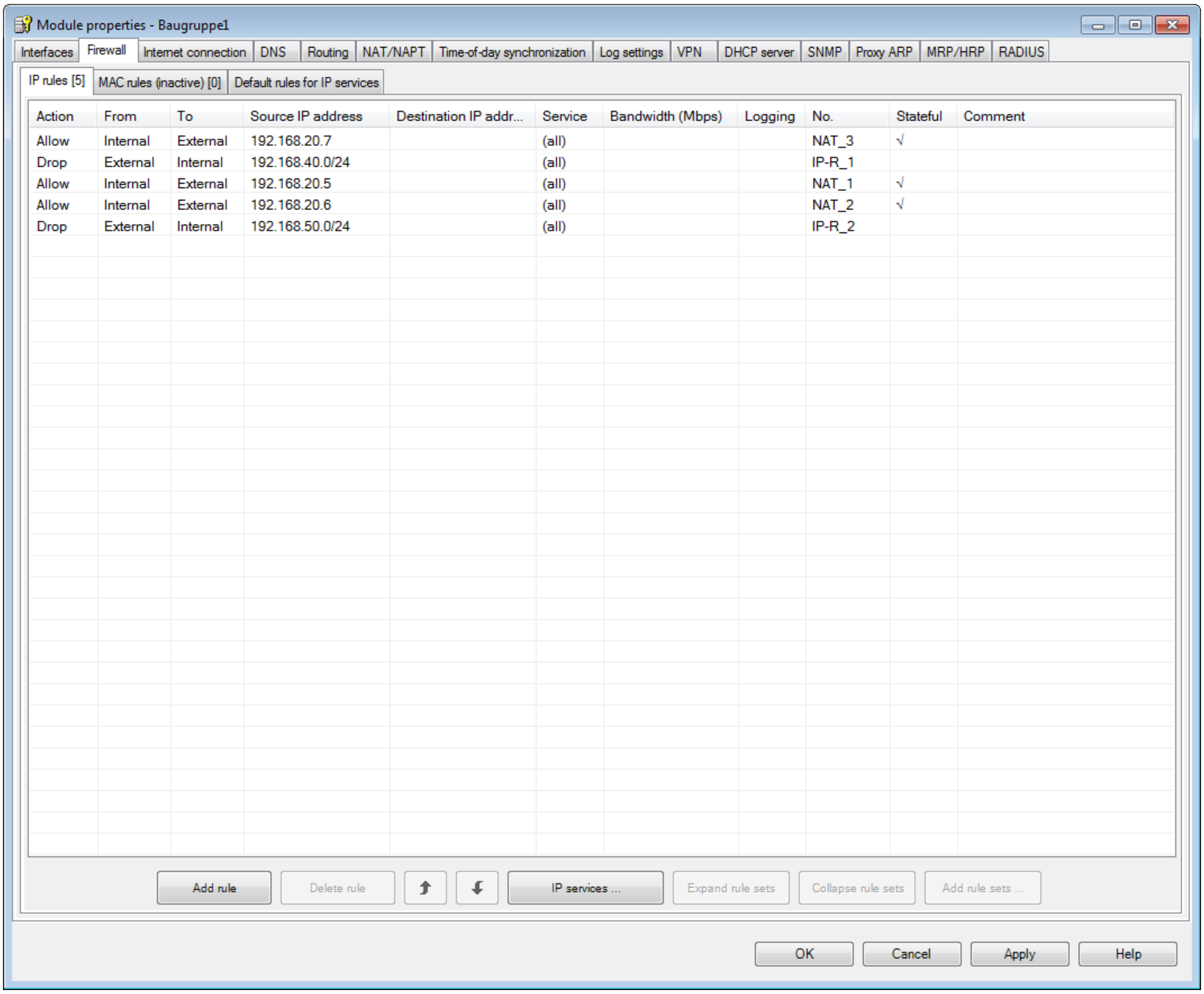
If firewall rules already exist that were generated by SCT for NAT/NAPT rules, firewall rules for further NAT/NAPT rules will be inserted by SCT below these firewall rules.



Action	From	To	Source IP address	Destination IP addr...	Service	Bandwidth (Mbps)	Logging	No.	Stateful	Comment
Allow	Internal	External	192.168.20.5		(all)			NAT_1	√	
Allow	Internal	External	192.168.20.6		(all)			NAT_2	√	
Drop	External	Internal	192.168.40.0/24		(all)			IP-R_1		
Drop	External	Internal	192.168.50.0/24		(all)			IP-R_2		

If firewall rules already exist that reference NAT/NAPT that were placed manually below firewall rules without NAT/NAPT reference, firewall rules for further NAT/NAPT rules will be placed by SCT above the firewall rules without NAT/NAPT reference.

)



Action	From	To	Source IP address	Destination IP addr...	Service	Bandwidth (Mbps)	Logging	No.	Stateful	Comment
Allow	Internal	External	192.168.20.7		(all)			NAT_3	√	
Drop	External	Internal	192.168.40.0/24		(all)			IP-R_1		
Allow	Internal	External	192.168.20.5		(all)			NAT_1	√	
Allow	Internal	External	192.168.20.6		(all)			NAT_2	√	
Drop	External	Internal	192.168.50.0/24		(all)			IP-R_2		

After creating NAT/NAPT rules check the position of the firewall rules generated by SCT for their priority. Firewall rules without NAT/NAPT reference that have higher priority than firewall rules with NAT/NAPT reference, can prevent the execution of NAT/NAPT.

Firewall parameters generated by SCT cannot be adapted. After deactivating NAT/NAPT, the firewall rules generated by SCT are removed.

The following table shows the system behind the firewall rules generated for NAT rules for SCALANCE S modules.

Table 5- 1 NAT address translation and corresponding firewall rules for SCALANCE S modules

NAT action	Created firewall rule				
	Action	**From**	**To**	**Source IP address**	**Destination IP address**
Destination NAT	Allow	Source network	Destination network	-	IP address specified in the "Destination IP address" input box
Source NAT	Allow	Source network	Destination network	IP address of the node specified in the "Source IP address" input box	-
Source NAT + Destination NAT	Allow	Source network	Destination network	IP address of the node specified in the "Source IP address" input box	-
	Allow	Destination network	Source network	-	IP address that was inserted in the "Destination IP address" input box by SCT
Double NAT	Allow	Source network	Destination network	IP address of the node specified in the "Source IP address" input box	IP address specified in the "Destination IP address" input box
	Allow	Source network	Destination network	IP address of the node specified in the "Source IP address" input box	IP address of the node specified in the "Destination translation" input box

The following table shows the system behind the firewall rules generated for NAT rules for CP x43-1 Adv.

Table 5- 2 NAT address translation and corresponding firewall rules for CP x43-1 Adv.

NAT action	Created firewall rule				
	Action	**From**	**To**	**Source IP address**	**Destination IP address**
Destination NAT	Drop	External	Station	-	-
	Allow	External	Any	-	IP address of the node specified in the "Destination translation" input box

NAT action	Created firewall rule				
	Action	**From**	**To**	**Source IP address**	**Destination IP address**
Source NAT	Allow	Any	External	IP address specified in the "Source translation" input box	-
Source NAT + Destination NAT	Allow	Any	External	IP address specified in the "Source translation" input box	-
	Drop	External	Station	-	-
	Allow	External	Any	-	IP address of the node specified in the "Destination translation" input box

The following table shows the system behind the firewall rules generated for NAT rules for SCALANCE S modules.

Table 5- 3 NAPT translation and firewall rules created for SCALANCE S modules

Created firewall rule					
Action	**From**	**To**	**Source IP address**	**Destination IP address**	**Service**
Allow	Source network	Destination network	-	IP address of the security module in the source network	[Service_NAPT_rule]

The following table shows the system behind the firewall rules generated for NAPT rules for CP x43-1 Adv.

Table 5- 4 NAPT translations and created firewall rules for CP x43-1 Adv.

Created firewall rules					
Action	**From**	**To**	**Source IP address**	**Destination IP address**	**Service**
Drop	External	Station	-	-	[Service_NAPT_rule]
Allow	External	Any	-	IP address of the node specified in the "Destination IP address" input box	[Service_NAPT_rule]

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 extra in the firewall rule and the NAT/NAPT address translation.

5.1.7 Relationship between NAT/NAPT router and user-specific firewall

Meaning

After creating NAT/NAPT rules, SCT automatically generates a user-specific IP rule set in the user-specific firewall that enables communication in the configured address translation direction. You can then assign this user-specific IP rule set to individual or multiple users and/or individual or multiple roles (only for SCALANCE S modules as of V4).

The generated firewall rules can, if necessary, be moved and expanded (additional IP address, services, bandwidth). Firewall parameters generated by SCT cannot be adapted. If the user-specific IP rule set is dragged ith the mouse to a security module with NAT/NAPT deactivated, the NAT/NAPT rules from the user-specific firewall are also applied to this security module.

Note

The address translation action "Double NAT" is not supported in conjunction with the user-specific firewall.

How to access this function

"NAT" or "NAPT" tab in the configuration dialog for user-specific IP rules sets, refer to the following section:
User-specific IP rule sets (Page 149)

Supported address translation directions for the action "Source NAT"

The action "Source NAT" can be performed in the following directions:

- External to DMZ
- DMZ to external

No IP address can be entered in the "Source IP address" box. This is entered automatically when the node logs on to the security module.

Supported address translation directions for the action "Destination NAT"

The action "Destination NAT" can be performed in the following directions:

- External to internal
- External to DMZ
- DMZ to internal
- DMZ to external
- Tunnel to internal (only SCALANCE S612/S623/S627-2M as of V4)
- Tunnel to external (only SCALANCE S612/S623/S627-2M as of V4)
- Tunnel to DMZ (only SCALANCE S612/S623/S627-2M as of V4)

Supported address translation directions for the action "Source NAT + Destination NAT"

The action "Source NAT + Destination NAT" can be performed in the following directions:

- External to DMZ
- DMZ to external

No IP address can be entered in the "Source IP address" box. This is entered automatically when the node logs on to the security module.

Supported address translation directions for NAPT

The address translation with NAPT can be performed in the following directions:

- External to internal
- External to DMZ
- DMZ to internal
- DMZ to external
- Tunnel to internal (only SCALANCE S612/S623/S627-2M as of V4)
- Tunnel to external (only SCALANCE S612/S623/S627-2M as of V4)
- Tunnel to DMZ (only SCALANCE S612/S623/S627-2M as of V4)

NAT/NAPT address translation and corresponding user-specific IP rule sets

In the firewall rules for user-specific IP rule sets generated based on NAT/NAPT rules, no IP address can be entered in the "Source IP address" box. This is entered automatically when the node logs on to the security module. The remaining properties are identical to the firewall rules generated locally for NAT rules of security modules. Refer to the section Relationship between NAT/NAPT router and firewall (Page 186)

5.2 Security module as DHCP server

5.2.1 Overview

SCA. S

Overview

You can operate the security module in the internal network and in the DMZ network as a DHCP server (DHCP = Dynamic Host Configuration Protocol). This allows IP addresses to be assigned automatically to the connected devices. To be able to do this the connected devices must be configured to obtain IP addresses from a DHCP server.

Simultaneous DHCP server operation on both interfaces is possible. S62x

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. If devices on the internal interface or on the DMZ interface should always be assigned the same IP address for firewall configuration, the address assignment must only be static based on the MAC address or based on the client ID.

See also

Consistency checks (Page 66)

5.2.2 Configuring a DHCP server

Requirement

The "DHCP server" tab is only displayed if the project is in advanced mode.

Note

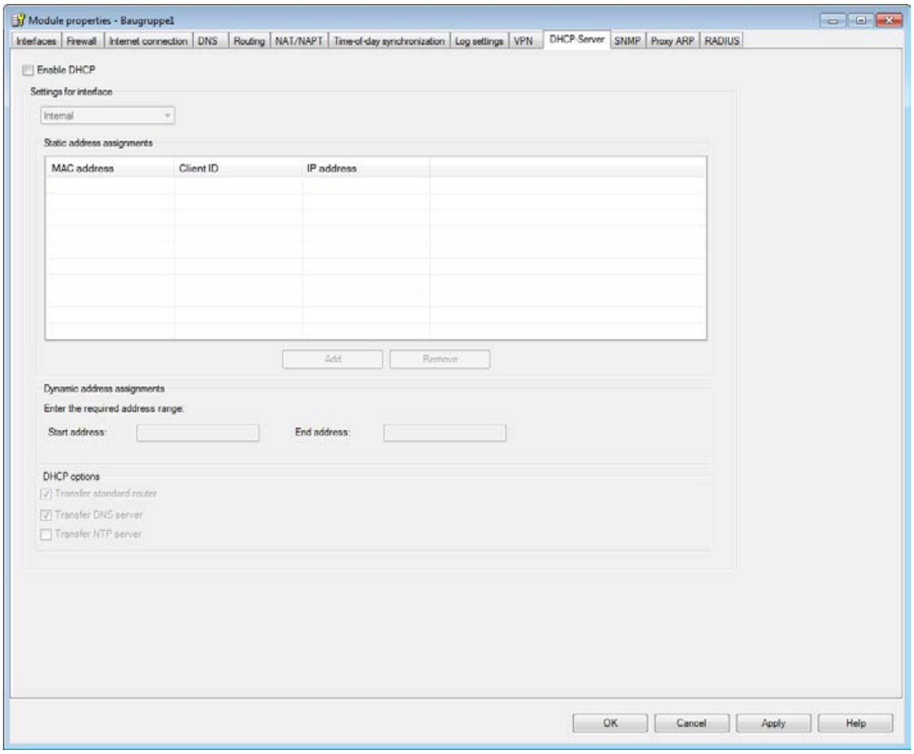
No return to standard mode possible

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 security module to be edited.
2. Select the "Edit" > "Properties..." menu command, "DHCP server" tab.



□ Enable DHCP

Settings for interface

Internal

Static address assignments

MAC address	Client ID	IP address

Dynamic address assignments

Enter the required address range:

Start address:

End address:

DHCP options

☑ Transfer standard router

☑ Transfer DNS server

□ Transfer NTP server

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 assignments

     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. This option makes sense with respect to firewall rules with explicit specification of source or destination IP address.

   – Dynamic address assignments

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

     Note

     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.

6. In the DHCP options, select which additional parameters should be transferred to the connected nodes.

- Transfer standard router

  If this check box is selected, connected devices have the IP address of the standard router transferred to them. This happens in the following situations:

  – The node is connected to the DMZ interface (SCALANCE S623/S627-2M only)
  In this case, the security module sends the IP address of the DMZ interface as the router IP address.

  – The node is connected to the internal interface and the security module is configured for router mode
  In this case, the security module sends the IP address of the internal interface as the router IP address.

  – The node is connected to the internal interface and the security module is not configured for router mode, there is, however, a standard router specified in the configuration of the security module.
  In this case, the security module transfers the IP address of the standard router as the router IP address.

  If the node is located on the internal interface of the security module, but the security module is not configured for router operation and no standard router is specified, no standard router is transferred to the connected node.

- Transfer DNS server:

  If this check box is selected, connected devices have the IP addresses of the preferred and alternative DNS server transferred to them.

- Transfer NTP server:

  If this check box is selected, connected devices have the IP addresses of the NTP servers assigned to the security module transferred to them.

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:

- 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.
- 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.
- IP addresses, MAC addresses and client IDs may only occur once in the "Static address assignments" input area (related to the security module).
- For the statically assigned IP addresses, you must specify either the MAC address or the client ID (computer name).

- 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.

- For the statically assigned IP addresses, you must specify the IP address.
- The following IP addresses must not be located in the range of the dynamic address assignments:
  - All router IP addresses in the "Routing" tab
  - Syslog server
  - Standard router
  - Address(es) of the security module
- DHCP is supported by the security module on the interface to the internal subnet and on the interface to the DMZ network. The following additional requirements for IP addresses in the range of the dynamic address assignments result from this operational behavior of the security module:
  - Bridge mode

    The range must be within the network subnet defined by the security module.
  - Routing mode

    The range must be within the internal subnet defined by the security module.

    Note

    The DMZ network always represents a separate subnet. When using DHCP on the DMZ interface, make sure that the free IP address range (dynamic IP addresses) is within the DMZ subnet.
- The free IP address range must be fully specified by entering the start address and the end address. The end address must be higher than the start address.
- The IP addresses you enter in the address list in the "Static address assignments" input area must be in the address range of the internal subnet or in the DMZ network of the security module.

Note the explanations in section Consistency checks (Page 66).

5.3 Time-of-day 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. With time-of-day synchronization the date and time of the security module can be adjusted to that of other system components.

The following alternatives can be configured:

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

Note

Before the security functions of a CP are used, this must receive a valid time-of-day synchronization frame from the time master.

Synchronization by an NTP server

The following rules apply when creating the NTP server:

- NTP servers can be created throughout a project using the SCT menu "Options" > "Configuration 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 are supported in the definition of NTP servers.
- FQDNs are supported in the definition of NTP servers.
- The IP address and the update interval of NTP servers already created in STEP 7 are migrated to SCT. CP
- If you select "Time-of-day synchronization with 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.

5.3.2 Configuring time-of-day synchronization

How to access this function

Menu command SCT:

1. Select the security module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Time-of day synchronization" tab.

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-of-day synchronization

The following alternatives can be configured:

Table 5- 5 Time-of-day synchronization for CPs

Possible selection	Meaning / effect
No time-of-day synchronization	No time-of-day 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-of-day synchronization using NTP (secured)	Automatic setting and periodic synchronization of the time using an NTP server (secure).

Table 5- 6 Time-of-day synchronization for SCALANCE S

Possible selection	Meaning / effect
No time-of-day synchronization	No time-of-day synchronization
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.
Time-of-day synchronization using NTP (secured) S≥V4.0	Automatic setting and periodic synchronization of the time using an NTP server (secure).

Selecting the mode of time-of-day synchronization

Follow these steps:

1. Select the synchronization mode.
   For SCALANCE S, 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.

   ---

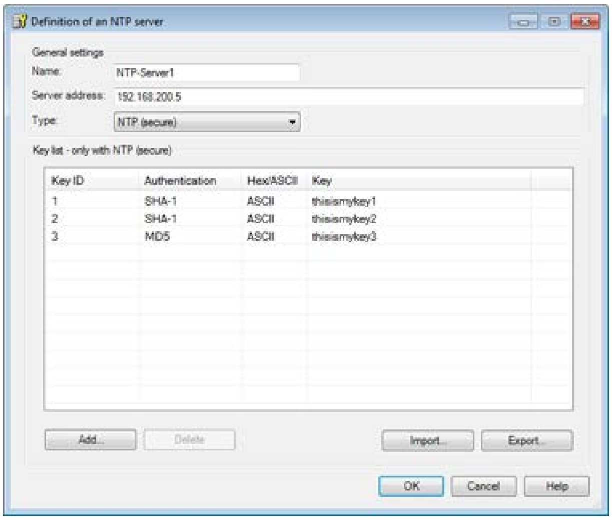
2. If you have selected the synchronization mode "Time-of-day synchronization with NTP" or "Time-of-day synchronization with NTP (secure)", with the "Add" button, you assign a previously created NTP server of the same type as in the "Synchronization mode" box to the security module.

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

5.3.3 Defining an NTP server

How to define a new NTP server:

1. Enter a name for the NTP server.



Definition of an NTP server

General settings

Name: NTP-Server1

Server address: 192.168.200.5

Type: NTP (secure)

Key list - only with NTP (secure)

Key ID	Authentication	Hex/ASCII	Key
1	SHA-1	ASCII	thisismykey1
2	SHA-1	ASCII	thisismykey2
3	MD5	ASCII	thisismykey3

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

Settings for NTP (secure)

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

Parameter	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

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 (Management Information Base) for which the user must have the required rights (SNMPv3).

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

HW Config: In the "SNMP" tab of the CP properties, the "Enable SNMP" check box is selected. If it is not enabled, SNMP cannot be configured in the Security Configuration Tool.

CP

Configuring SNMP - Follow the steps below:

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

   Note

   Encrypted data transfer with SNMPv3

   To increase security, you should use SNMPv3 since the data is then transferred unencrypted.

   – 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

     To enable write access using SNMP, select the "Allow write access" check box.

   – SNMPv3

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

     Authentication algorithm: none, MD5, SHA-1

     Encryption algorithm: none, AES-128, DES

     Note

     Avoiding the use of DES

     DES is not a secure encryption algorithm. It should therefore only be used where downwards compatibility is required.

     Note

     When using SNMPv3 no RADIUS authentication is possible.

5. In the "Advanced settings" area, configure module-specific information on the author, location and e-mail address that overwrites the information from the project properties. If you select the "Keep values written by SNMP set" check box, values written to the

security module with an SNMP tool using an SNMP-SET command are not overwritten when downloading an SCT configuration again to the security module. SCA. S

6. If you want to use SNMPv3, assign a user a role for which the corresponding SNMP rights are activated so that it can reach the security module via SNMP.

   For more detailed information on configuring users, rights and roles, refer to the next section:

   – Managing users (Page 70)

5.5 Proxy ARP

SCA. S

~~S602~~

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

How to access this function

This function is only available for the internal interface of a security module that is a member of a VPN group and is in bridge mode. The project must also be in advanced mode.

1. Select the security 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.

5.6 Security module as OPC UA server/client

5.6.1 OPC UA authentication and encryption

CP 443-1 OPC UA

Requirement

The "OPC UA" tab is only available if the OPC UA server function was enabled for the CP in STEP 7.

Meaning

Here you specify the Security profiles and access options for the UA server of the CP.

- **Securityprofile**
  - No security profile

    The CP does not use any Security profile.
  - Basic128Rsa15

    This corresponds to the Security profile "Basic128Rsa15" of the OPC UA specification.

    The CP uses signing and if configured 128 bit encryption.
  - Basic256

    This corresponds to the Security profile "Basic256" of the OPC UA specification.

    The CP uses signing and if configured 256 bit encryption.
  - Basic256Sha256

    This corresponds to the Security profile "Basic256Sha256" of the OPC UA specification.

    The CP uses signing and if configured 256 bit encryption using the hash algorithm SHA-256.

  If you enable several options, depending on the settings on the communications partner (client) the CP selects the profile with the highest possible security.

- **Security procedure of the server**
  - Sign

    The CP only allows communication with signed frames.
  - Sign and encrypt

    The CP only allows communication with signed and encrypted frames.
  - Best possible procedure

    Depending on the settings on the communications partner (client) the CP selects the procedure with the highest possible security. This can be:

    - Sign
      or
    - Sign and encrypt
- **Anonymous access**
  - Allow read access

    The CP allows read access to the data of its OPC UA server.
  - Allow write access

    The CP allows write access to the data of its OPC UA server.

5.6.2 Certificate validation

CP 443-1 OPC UA

In the "Certificate validation" tab you set the options for checking the certificates of the communications partner. You can set the options for the UA client and for the UA server function of the CP separately.

If you use the client function of the CP, you should also note the following: The value of the parameter "CheckServerCertificate" you programmed in the connection information (UASessionConnectInfo) for the client program block "UAConnect" will be overwritten by the settings in SCT for the certificate check. If the client is to check the certificates of the communications partner (server), you can ignore the parameter in the UDT "UASessionConnectInfo". For the certificate check only the settings in the SCT tab "Certificate validation" are relevant.

- Checking the certificates

  The CP always checks the certificate of the communications partner.

  If the partner certificate is invalid or is not trustworthy, communication is aborted.
- No strict certificate validation

  If the option is selected, the CP also allows communication in the following cases:
  - The IP address of the communications partner is not identical to the IP address in its certificate.

    Note: The OPC UA server does not check the IP address of the communications partner (client).

  - The use stored in the certificate (OPC UA client/server) differs from the function (OPC UA client/server) of the communications partner.
  - The current time on the CP is outside the period of validity of the partner certificate.

  Regardless of these exceptions, at least the following requirements must be met to establish a connection:

  - The application URI sent by the requesting client must match the URI of the server application of the CP.
  - If the partner certificate is not trustworthy, the CP must at least have stored a self-signed certificate of the partner.
  - If the partner certificate was issued by several CAs, all CAs must be saved in the certificate store of the CP.

- Do not check period of validity

  If the option is enabled, the CP checks the certificate of the communications partner. The CP also allows communication in the following situation:

  - The current time on the CP is outside the period of validity of the partner certificate.

If none of the three options is enabled, no certificates are checked.

5.6.3 S7 communication

CP 443-1 OPC UA

In the "S7 communication" tab, you make the settings for S7 communication via the CP and for protection of LAN access to the pages of the S7 special diagnostics on the CP.

- Disable S7 communication

  If the option is enabled, S7 communication via the CP is blocked.

- Disable online diagnostics via LAN

  If the option is enabled, access to the diagnostics pages of the S7 special diagnostics on the CP via LAN is blocked.

Secure communication in the VPN via an IPsec tunnel 6

~~S602~~

~~CP 443-1 OPC UA~~

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

As already described in the section on module properties, you can once again use the default settings to ensure secure communication in 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 - diagnostics and logging (Page 273)

6.1 VPN with security and SCALANCE M modules

Secure connection through an unprotected network

For security and SCALANCE M 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.

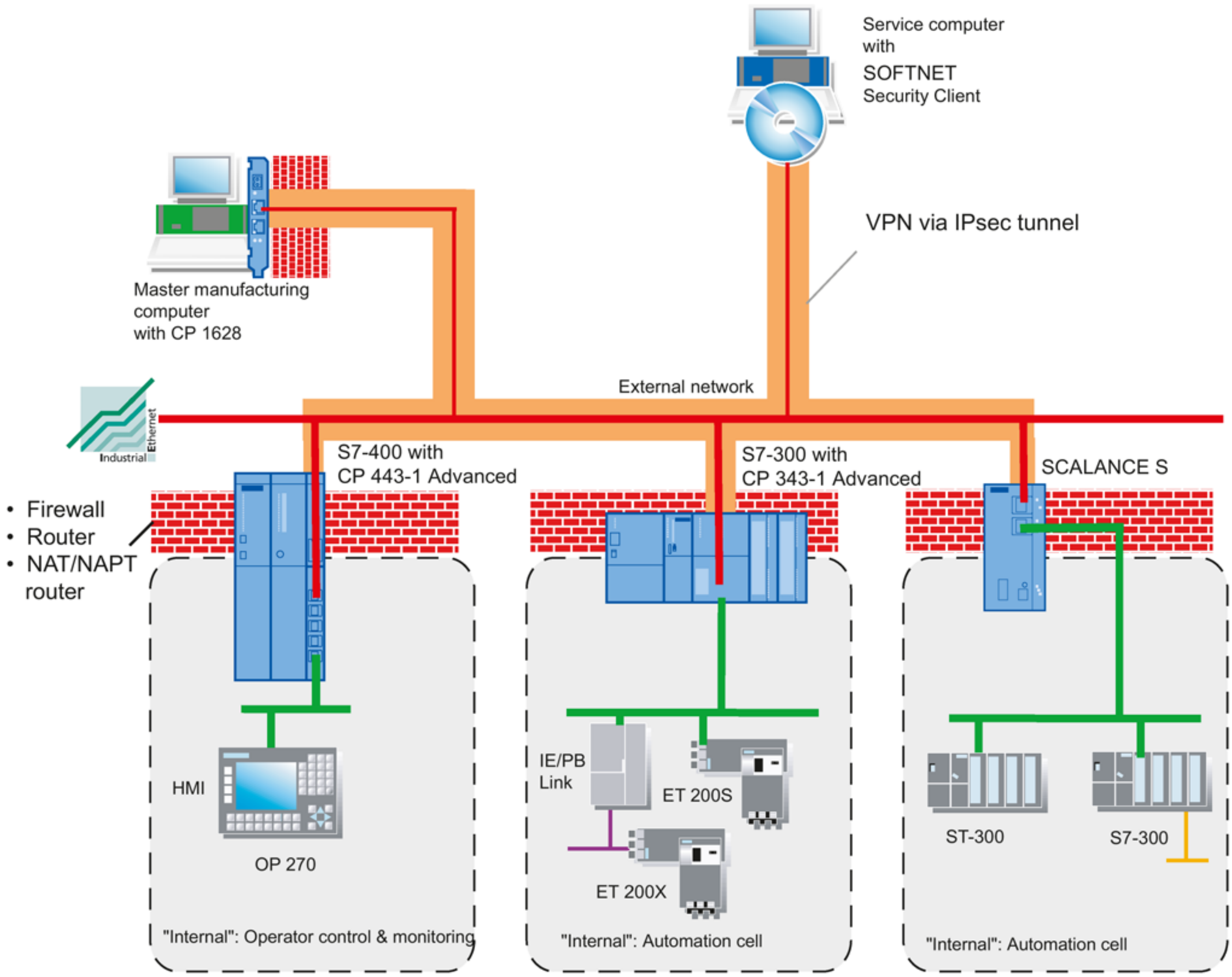
- Confidentiality

  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.

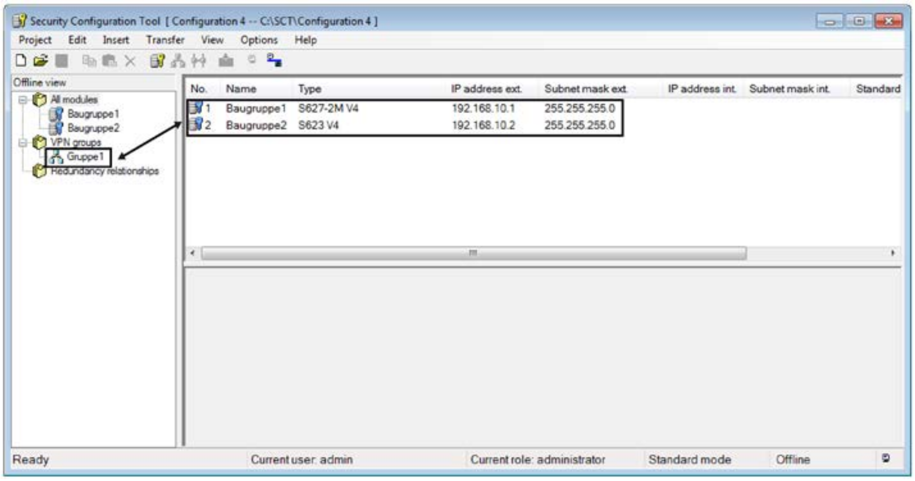
The module uses the IPsec protocol for tunneling (tunnel mode of IPsec).



Tunnel connections exist between modules in the same VPN group

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

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



No.	Name	Type	IP address ext.	Subnet mask ext.	IP address int.	Subnet mask int.	Standard
1	Baugruppe1	S627-2M V4	192.168.10.1	255.255.255.0			
2	Baugruppe2	S623 V4	192.168.10.2	255.255.255.0			

Note

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

If the name of a VPN group is changed, all modules of this VPN group must be reconfigured (menu command "Transfer" > "To all modules...").

Note

Layer 2 frames are also tunneled when there is a router between two 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 packets are transferred through a tunnel only when the devices that send or receive the packets were able to communicate previously; in other words, without using the modules.

6.2 Authentication method

Authentication method

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

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

- Pre-shared keys

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

  To do this, enter a password in the "Key" box of the "VPN group properties" dialog or generate a password using the "New..." button.

- Certificate

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

  – When you create a VPN group, a CA certificate is generated automatically for the VPN group.

  – Each module in the VPN group receives a VPN group certificate signed with the key of the certification authority of the VPN group.

  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.

Note

Restriction in VLAN operation

With IP packets through the VPN tunnel of the module, no VLAN tagging is transferred. The VLAN tags included in IP packets are lost when they pass through the modules because IPsec is used to transfer the IP packets.

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 packets 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 Rules for forming VPN groups

Remember the following rules:

- For SCALANCE S612 / S613 / S623 / S627-2M / SCALANCE M / VPN device

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

  If the first added SCALANCE S module is in routing mode or if the first module is a SCALANCE M module or a VPN device, then only SCALANCE S modules with activated routing or SCALANCE M modules or VPN devices can be
  added because SCALANCE M modules and VPN devices always operate in routing mode.
  If the first added SCALANCE S module is in bridge mode, then only SCALANCE S modules in bridge mode can be added.
  A CP or an SSC and an NCP VPN client (Android) can be added to a VPN group with a SCALANCE S in bridge or routing mode.

- For CP / SSC / NCP VPN client (Android)

  If a CP / SSC / NCP VPN client (Android) is the first module in a VPN group, modules in any mode can be added until a SCALANCE S or SCALANCE M module is added. From this point on, the rules for SCALANCE S and SCALANCE M modules apply, see above.

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

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

Table 6- 1 Rules for forming VPN groups

Module	The following can be included in a VPN group containing the following module:		
	SCALANCE S in bridge mode	**SCALANCE S in routing mode / SCALANCE M / VPN device / NCP VPN client (Android)**	**CP / SSC**
SCALANCE S in bridge mode	x	-	x
SCALANCE S in routing mode	-	x	x
CP x43-1 Adv.	x	x	x
CP 1628	x	x	x
SOFTNET Security Client 2005	x	-	-
SOFTNET Security Client 2008	x	x	x
SOFTNET Security Client V3.0	x	x	x
SOFTNET Security Client V4.0	x	x	x

Module	The following can be included in a VPN group containing the following module:		
	SCALANCE S in bridge mode	SCALANCE S in routing mode / SCALANCE M / VPN device / NCP VPN client (Android)	CP / SSC
SCALANCE M / VPN device	-	x	x
NCP VPN client (Android)	-	x	x

6.3.2 Supported tunnel communication relations

Meaning

The following tables show which tunnel interfaces can establish a tunnel between them. Here, a distinction is made depending on whether the SCALANCE S module is in routing or in bridge mode.

Regardless of the interface via which the VPN tunnel is established, as default the nodes of the internal subnets of the security modules can always communicate with each other. If communication via the VPN tunnel should also extend to other subnets, these can be enabled for tunnel communication in the "VPN" tab in the advanced module properties, see following section:

- Configuring other nodes and subnets for the VPN tunnel (Page 243)

Subnets that need to be enabled for tunnel communication are as follows:

- Subnet on the external interface (if the external interface is not a VPN endpoint)
- Subnet on the DMZ interface (if the DMZ interface is not a VPN endpoint)
- Other subnets that can be reached by the router on the various interfaces (if these are not VPN endpoints)

Table 6- 2 Tunnel communication between CPs, SCALANCE M modules, SOFTNET Security Clients and SCALANCE S modules in routing mode

	Responder interface				
Initiator interface	**External (SCALANCE M875)**	**External (SCALANCE M-800)**	**GBit, IE (CP)**	**External (SCALANCE S)**	**DMZ (SCALANCE S623 / S627-2M)**
PC/PG (SSC)	x	x	x	x	x
External (SCALANCE M875)	-	x	x	x	x

	Responder interface				
Initiator interface	**External (SCALANCE M875)**	**External (SCALANCE M-800)**	**GBit, IE (CP)**	**External (SCALANCE S)**	**DMZ (SCALANCE S623 / S627-2M)**
External (SCALANCE M-800)	-	x	x	x	x
Gbit, IE (CP)	-	-	x	x	x
External (SCALANCE S)	-	-	x	x	x
DMZ (SCALANCE S623 / S627-2M)	-	-	x	x	x

x is supported

- is not supported

Table 6- 3 Tunnel communication between CPs, SOFTNET Security Clients and SCALANCE S modules in bridge mode

	Responder interface		
Initiator interface	**GBit, IE (CP)**	**External (SCALANCE S)**	**DMZ (SCALANCE S623 / S627-2M)**
PC/PG (SSC)	x	x	-
GBit, IE (CP)	x	x	-
External (SCALANCE S)	x	x	-
DMZ (SCALANCE S623 / S627-2M)	-	-	-

x is supported

- is not supported

6.3.3 Creating VPN groups and assigning modules

~~S602~~

~~CP 443-1 OPC UA~~

Note

SCALANCE S V1/V2 modules

SCALANCE S V1/V2 modules are no longer supported as of SCT V5.0. Existing SCALANCE S V1/V2 modules from projects of older SCT versions can therefore no longer be inserted in VPN groups. It is also not possible to add SCALANCE S modules to a VPN group in which there is a SCALANCE S V1/V2 module. The SCALANCE S V1/V2 must first be removed from the VPN group or replaced by a SCALANCE S module with a higher firmware version.

Requirement

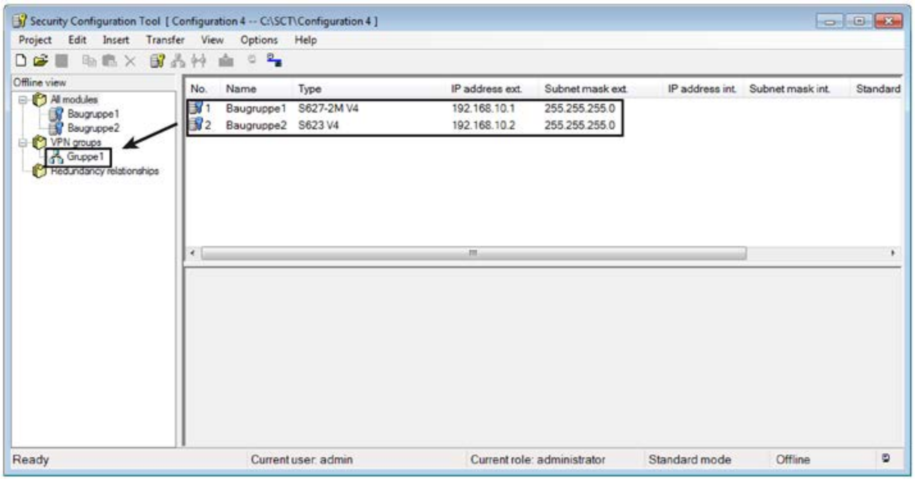
Note

Current date and current time of day on the modules

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

How to access this function

1. Create a VPN group with the "Insert" > "Group" menu command.
2. Assign the modules, SOFTNET Security Clients, VPN devices and NCP VPN clients (Android) intended for a VPN group to the group by dragging the modules to the required VPN group with the mouse.



No.	Name	Type	IP address ext.	Subnet mask ext.	IP address int.	Subnet mask int.	Standard
1	Baugruppe1	S627-2M V4	192.168.10.1	255.255.255.0			
2	Baugruppe2	S623 V4	192.168.10.2	255.255.255.0			

Ready | Current user: admin | Current role: administrator | Standard mode | Offline

Configuring properties

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

- **Standard mode**

  In standard mode, you retain the defaults set by the system. Even without expert knowledge, you can configure IPsec tunnels in this way and operate secure data communication.

- **Advanced mode**

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

Displaying all configured VPN groups and their properties

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

The following properties of the groups are displayed in columns:

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

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 panel, select the VPN group for which you want to configure a certificate.
2. Right-click on the security module in the content area and select the "New certificate…" command 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. You will find more information on certificates, in the following section:

- Managing certificates (Page 85)

6.4 Tunnel configuration in standard mode

Opening the dialog for displaying default values

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

The display of the VPN group properties is identical to the display in advanced mode; you cannot, however, change the values in standard mode.

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 the project 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 VPN group properties

6.5.1.1 VPN connection establishment by Known Peers and Unknown Peers

The properties of a VPN group are made up of the selected authentication method and the configured parameters for IKE phase 1 and 2 and during loading are transferred to all VPN group nodes. On the responder the IP addresses of the security modules that may initiate the VPN connection establishment with the configured properties of the VPN group are stored in addition. When a security module attempts to establish a VPN connection to the responder, this first checks whether the IP address of the initiator is known to it. If this is the case, the initiator is a Known Peer. If the VPN group properties proposed by this Known Peer match those stored on the responder for the Known Peer, the responder allows the VPN connection establishment. In addition to the properties of a VPN group, fallback VPN profiles can be selected for a VPN group. VPN profiles contain predefined properties for the authentication method, IKE phase 1 and 2. Fallback VPN profiles can be used as alternative configurations for VPN connection establishment. These come into play when VPN properties of the initiator do not match the VPN properties of the responder. In such cases, fallback VPN profiles ensure the VPN connection establishment. The configured fallback VPN profiles just as the properties of the VPN group are transferred to all VPN group nodes. The fallback VPN profiles and the properties of the VPN group must not differ in the authentication method.

If the IP address of the initiator is not known to the responder because the initiator in productive mode for example is connected via a NAT translation, the initiator is an Unknown Peer (Road Warrior). As default the responder allows connection establishment by Unknown Peers. In the module-specific VPN properties of the responder you can specify whether and with which VPN group properties connection establishment by Unknown Peers is allowed by the responder, see section Configuring module-specific VPN properties (Page 230).

6.5.1.2 Configuring VPN group properties

Note

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 VPN group properties can be set in advanced mode:

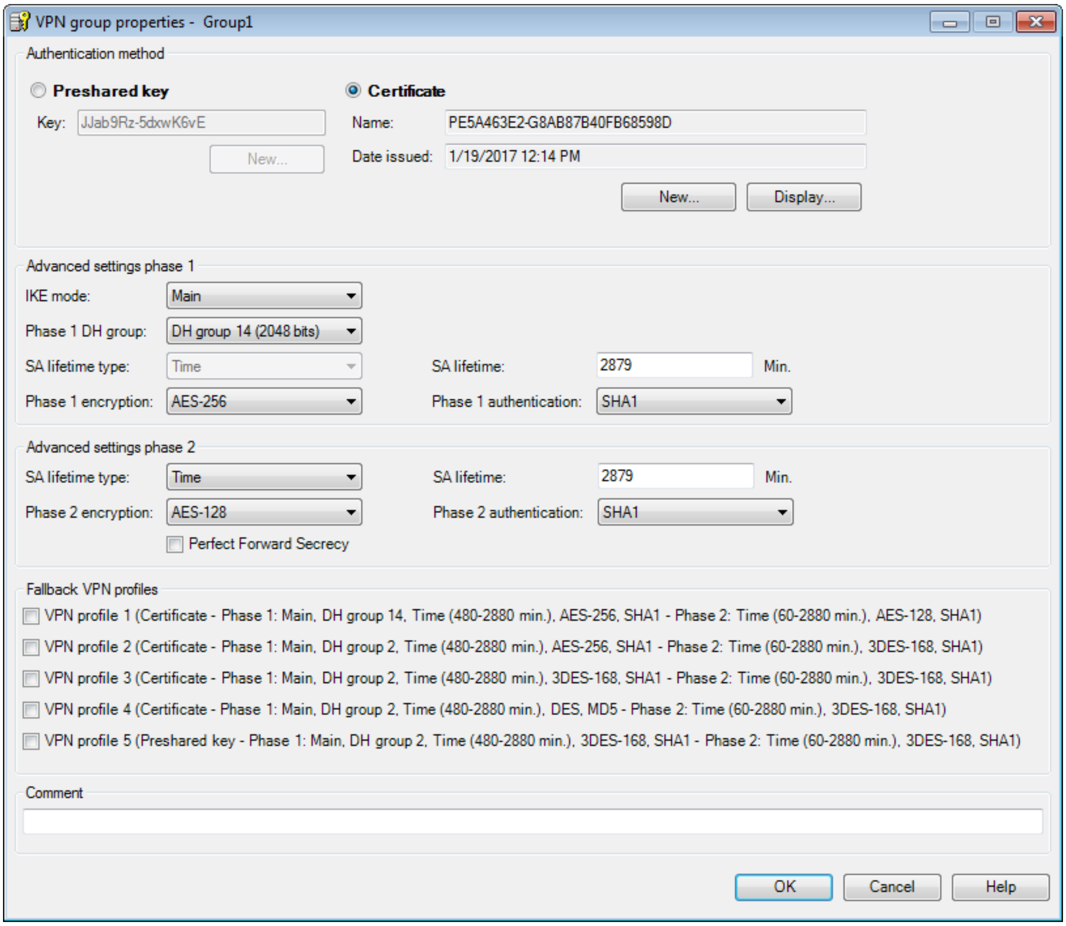
- Authentication method
- IKE settings (dialog area: Advanced Settings Phase 1)
- IPsec settings (dialog area: Advanced Settings Phase 2)
- Fallback VPN profiles

If the VPN group properties you have configured are less secure than the recommended properties, SCT makes this known to you with an appropriate message text.

The VPN group properties of a VPN group in which there is a SCALANCE S V1/V2 module cannot be modified. The SCALANCE S V1/V2 must first be removed from the VPN group or replaced by a SCALANCE S module with a higher firmware version.

How to access this function:

1. In the navigation panel, select the VPN group you want to edit.
2. Select the "Edit" > "Properties..." menu command.



VPN group properties - Group1

Authentication method

○ **Preshared key**

Key: JJab9Rz-5dxwK6vE

● **Certificate**

Name: PE5A463E2-G8AB87B40FB68598D

Date issued: 1/19/2017 12:14 PM

Advanced settings phase 1

IKE mode: Main

Phase 1 DH group: DH group 14 (2048 bits)

SA lifetime type: Time

SA lifetime: 2879 Min.

Phase 1 encryption: AES-256

Phase 1 authentication: SHA1

Advanced settings phase 2

SA lifetime type: Time

SA lifetime: 2879 Min.

Phase 2 encryption: AES-128

Phase 2 authentication: SHA1

□ Perfect Forward Secrecy

Fallback VPN profiles

□ VPN profile 1 (Certificate - Phase 1: Main, DH group 14, Time (480-2880 min.), AES-256, SHA1 - Phase 2: Time (60-2880 min.), AES-128, SHA1)

□ VPN profile 2 (Certificate - Phase 1: Main, DH group 2, Time (480-2880 min.), AES-256, SHA1 - Phase 2: Time (60-2880 min.), 3DES-168, SHA1)

□ VPN profile 3 (Certificate - Phase 1: Main, DH group 2, Time (480-2880 min.), 3DES-168, SHA1 - Phase 2: Time (60-2880 min.), 3DES-168, SHA1)

□ VPN profile 4 (Certificate - Phase 1: Main, DH group 2, Time (480-2880 min.), DES, MD5 - Phase 2: Time (60-2880 min.), 3DES-168, SHA1)

□ VPN profile 5 (Preshared key - Phase 1: Main, DH group 2, Time (480-2880 min.), 3DES-168, SHA1 - Phase 2: Time (60-2880 min.), 3DES-168, SHA1)

Comment

3. Select whether a pre-shared key or certificate will be used for authentication. For more detailed information, refer to the following section:
   – Authentication method (Page 212).

Advanced settings phase 1

Phase 1: IKE negotiation of the Security Association (SA) for phase 2:

Here you set the parameters for negotiating the security parameters to be used in phase 2: Note the permitted settings for nodes with an unknown IP address, see section Including module in configured VPN group (Page 229).

Parameter	Description
IKE mode	• Main mode (default setting) • Aggressive mode Selection of the mode IKE phase 1. In Main mode, the VPN connection partners exchange their identities encrypted, in Aggressive mode unencrypted. In Aggressive mode IKE phase 1 runs faster but is less secure than in the alternative Main mode.
Phase 1 DH group	Groups selectable for the Diffie-Hellman key exchange: • Group 1* • Group 2* • Group 5 • Group 14 (default setting) • Group 15
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 setting: 2879)
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 (default setting): 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 (default setting)

* The setting is classified as less secure. It is recommended that you use a more secure setting.

Advanced settings phase 2

Phase 2: IKE negotiation of the Security Association (SA) for IPsec data exchange:

Here, you set the parameters for negotiating the security parameters used for the IPsec data exchange with ESP (Encapsulating Security Payload) and AH (Authentication Header). Communication in phase 2 is already encrypted.

Parameter	Description
SA lifetime type	Phase 2 Security Association (SA): • Time (default setting): Time limit in minutes The use of the current key material has a time limit. When the time expires, the key material is re-negotiated. • Limit: Limitation of the data volume in MB
SA lifetime	Numeric value: • Range of values for time: 60 … 16666666 minutes (default setting: 2879) • Range of values for limit: 2000 ... 500000 MB (default setting: 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 (default setting): Advanced Encryption Standard (128-bit key length, mode CBC)
Phase 2 authentication	Authentication algorithm: • MD5*: Message Digest Algorithm 5 • SHA1 (default setting): Secure Hash Algorithm 1
Perfect Forward Secrecy	If you enable this check box, new Diffie-Hellmann public key values are exchanged for recalculation of the keys. If the check box is disabled, the values already exchanged in phase 1 are used for recalculation of the keys.

* The setting is classified as less secure. It is recommended that you use a more secure setting.

Configuring fallback VPN profiles

In addition to the properties of a VPN group, fallback VPN profiles can be selected for a VPN group. VPN profiles contain predefined properties for the authentication method, IKE phase 1 and 2. Fallback VPN profiles can be used as alternative configurations for VPN connection establishment. These come into play when VPN properties of the initiator do not match the VPN properties of the responder. In such cases, fallback VPN profiles ensure the VPN connection establishment. The configured fallback VPN profiles just as the properties of the VPN group are transferred to all VPN group nodes. The fallback VPN profiles and the properties of the VPN group must not differ in the authentication method.

The following fallback VPN profiles are available:

Table 6- 4 VPN profile 1

Parameter	Setting
Authentication method	Certificate
IKE mode	Main

Parameter	Setting
Phase 1 DH group	Group 14
Phase 1 encryption	AES-256
Phase 1 SA lifetime	SA lifetime proposed by the initiator: 480 minutes Range permitted by the responder for the SA lifetime: 480 … 2880 minutes
Phase 1 authentication	SHA1
Phase 2 SA lifetime type	Time
Phase 2 encryption	AES-128
Phase 2 SA lifetime	SA lifetime proposed by the initiator: 240 minutes Range permitted by the responder for the SA lifetime: 60 … 2880 minutes
Phase 2 authentication	SHA1
Perfect Forward Secrecy	Disabled

Table 6- 5 VPN profile 2

Parameter	Setting
Authentication method	Certificate
IKE mode	Main
Phase 1 DH group	Group2
Phase 1 encryption	AES-256
Phase 1 SA lifetime	SA lifetime proposed by the initiator: 480 minutes Range permitted by the responder for the SA lifetime: 480 … 2880 minutes
Phase 1 authentication	SHA1
Phase 2 SA lifetime type	Time
Phase 2 encryption	3DES-168
Phase 2 SA lifetime	SA lifetime proposed by the initiator: 2880 minutes Range permitted by the responder for the SA lifetime: 60 … 2880 minutes
Phase 2 authentication	SHA1
Perfect Forward Secrecy	Disabled

Table 6- 6 VPN profile 3

Parameter	Setting
Authentication method	Certificate
IKE mode	Main
Phase 1 DH group	Group2
Phase 1 encryption	3DES-168

Parameter	Setting
Phase 1 SA lifetime	SA lifetime proposed by the initiator: 480 minutes Range permitted by the responder for the SA lifetime: 480 … 2880 minutes
Phase 1 authentication	SHA1
Phase 2 SA lifetime type	Time
Phase 2 encryption	3DES-168
Phase 2 SA lifetime	SA lifetime proposed by the initiator: 2880 minutes Range permitted by the responder for the SA lifetime: 60 … 2880 minutes
Phase 2 authentication	SHA1
Perfect Forward Secrecy	Disabled

Table 6- 7 VPN profile 4

Parameter	Setting
Authentication method	Certificate
IKE mode	Main
Phase 1 DH group	Group2
Phase 1 encryption	DES
Phase 1 SA lifetime	SA lifetime proposed by the initiator: 480 minutes Range permitted by the responder for the SA lifetime: 480 … 2880 minutes
Phase 1 authentication	MD5
Phase 2 SA lifetime type	Time
Phase 2 encryption	3DES-168
Phase 2 SA lifetime	SA lifetime proposed by the initiator: 2880 minutes Range permitted by the responder for the SA lifetime: 60 … 2880 minutes
Phase 2 authentication	SHA1
Perfect Forward Secrecy	Disabled

Table 6- 8 VPN profile 5

Parameter	Setting
Authentication method	Pre-shared key
IKE mode	Main
Phase 1 DH group	Group2
Phase 1 encryption	3DES-168
Phase 1 SA lifetime	SA lifetime proposed by the initiator: 480 minutes Range permitted by the responder for the SA lifetime: 480 … 2880 minutes

Parameter	Setting
Phase 1 authentication	SHA1
Phase 2 SA lifetime type	Time
Phase 2 encryption	3DES-168
Phase 2 SA lifetime	SA lifetime proposed by the initiator: 2880 minutes Range permitted by the responder for the SA lifetime: 60 … 2880 minutes
Phase 2 authentication	SHA1
Perfect Forward Secrecy	Disabled

Restrictions for the SOFTNET Security Client and SCALANCE M

Configured fallback VPN profiles are not included in the configuration files for the Roadwarrior modules SOFTNET Security Client and SCALANCE M For the SOFTNET Security Client and SCALANCE M modules the following applies:

- Select the VPN profile to be used for VPN connections of SOFTNET Security Client / SCALANCE M modules to SCALANCE S / CPs in the responder settings, see section Configuring module-specific VPN properties (Page 230).
- For VPN connections from SCALANCE M modules to SCALANCE M modules, the configured VPN group settings are used.
- For VPN connections from SOFTNET Security Client to SCALANCE M modules the settings of VPN profile 3 are always used.
- With VPN connections from SOFTNET Security Client modules for which you have selected the firmware release V4/V5 when selecting the module, in terms of the supported VPN profiles the Security Configuration Tool assumes firmware release V5. If you want to use the configuration file in SOFTNET Security Client V4, in the responder settings, there must be no VPN profiles activated that use DH group 14.

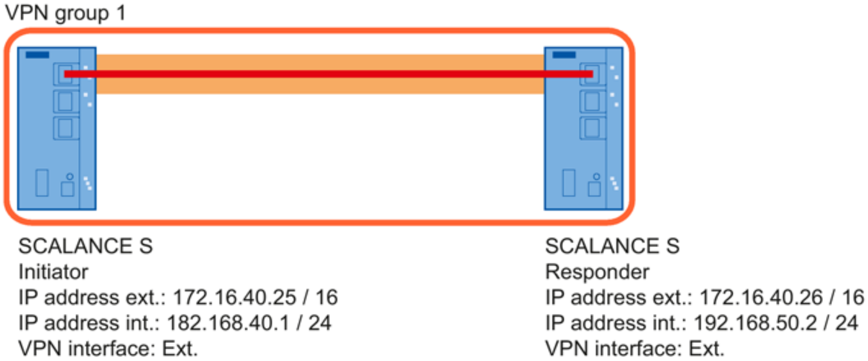
For the SOFTNET Security Client and SCALANCE M, the following settings are not supported:

Module	Phase 1 DH group	Phase 1 encryption	Phase 2 encryption
SOFTNET Security Client (Windows XP)	Group5 Group15	AES 128 AES 192 AES 256	AES 128
SOFTNET Security Client (Windows 7)	Group5 Group15	-	-
SCALANCE M875	Group 14 Group15	-	-
SCALANCE M-800	-	DES	DES

6.5.1.3 Examples of the configuration of VPN group properties

Example 1: VPN connection establishment by Known Peer

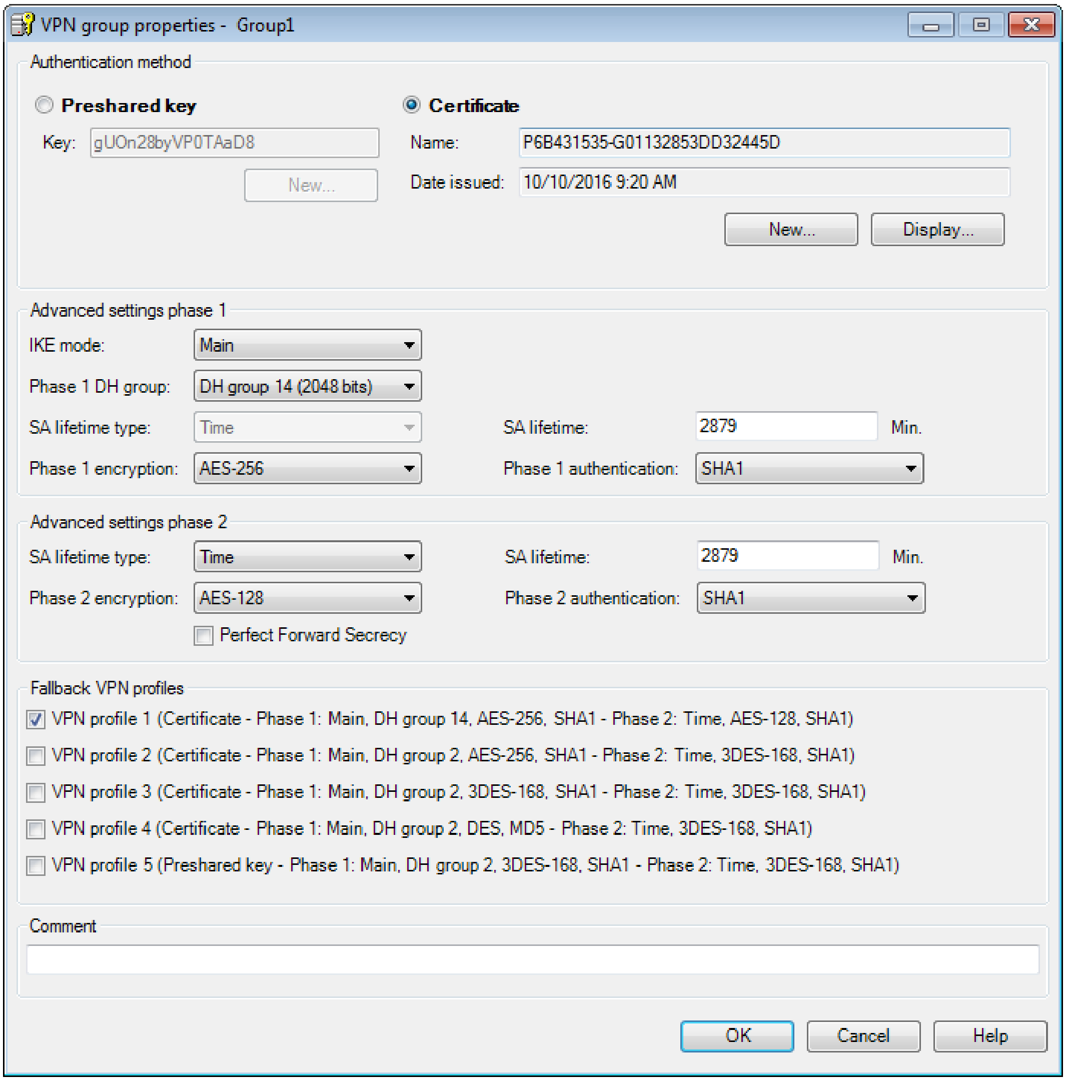
The following figure illustrates the network establishment between an initiator and a responder. The initiator is a Known Peer and is intended to establish a VPN connection to the responder with the properties of the VPN group "VPN Group 1".


VPN group 1
SCALANCE S
Initiator
IP address ext.: 172.16.40.25 / 16
IP address int.: 182.168.40.1 / 24
VPN interface: Ext.
SCALANCE S
Responder
IP address ext.: 172.16.40.26 / 16
IP address int.: 192.168.50.2 / 24
VPN interface: Ext.

Since the initiator is a Known Peer and both security modules are in "VPN Group 1", the VPN connection can be established with the properties of this VPN group without any further configuration.

Expansion of example 1: Expansion with a fallback VPN profile

The initiator from example 1 has already established a VPN connection to the responder with the properties of the VPN group "VPN Group 1". The properties of the VPN group will now be changed and downloaded to the responder via a PC connected locally to the responder module. The VPN group configuration now differs between the responder and initiator, and for this reason the VPN tunnel is terminated. The changed VPN group configuration can now no longer be loaded on the remote initiator module via the VPN tunnel. So that in the case described, the VPN tunnel can be re-established even without loading the initiator module, a fallback VPN profile can be selected in the properties of the VPN group and downloaded to the nodes of the VPN group. With the properties of this VPN profile, the VPN connection in the case described above is re-established.



Authentication method

○ **Preshared key**

Key: gUOn28byVP0TAaD8

● **Certificate**

Name: P6B431535-G01132853DD32445D

Date issued: 10/10/2016 9:20 AM

Advanced settings phase 1

IKE mode: Main

Phase 1 DH group: DH group 14 (2048 bits)

SA lifetime type: Time

SA lifetime: 2879 Min.

Phase 1 encryption: AES-256

Phase 1 authentication: SHA1

Advanced settings phase 2

SA lifetime type: Time

SA lifetime: 2879 Min.

Phase 2 encryption: AES-128

Phase 2 authentication: SHA1

□ Perfect Forward Secrecy

Fallback VPN profiles

☑ VPN profile 1 (Certificate - Phase 1: Main, DH group 14, AES-256, SHA1 - Phase 2: Time, AES-128, SHA1)

□ VPN profile 2 (Certificate - Phase 1: Main, DH group 2, AES-256, SHA1 - Phase 2: Time, 3DES-168, SHA1)

□ VPN profile 3 (Certificate - Phase 1: Main, DH group 2, 3DES-168, SHA1 - Phase 2: Time, 3DES-168, SHA1)

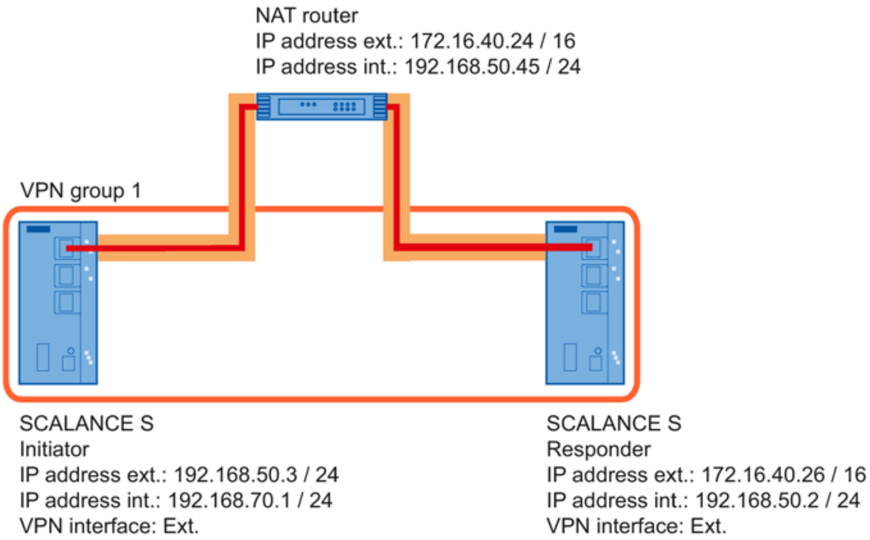
□ VPN profile 4 (Certificate - Phase 1: Main, DH group 2, DES, MD5 - Phase 2: Time, 3DES-168, SHA1)

□ VPN profile 5 (Preshared key - Phase 1: Main, DH group 2, 3DES-168, SHA1 - Phase 2: Time, 3DES-168, SHA1)

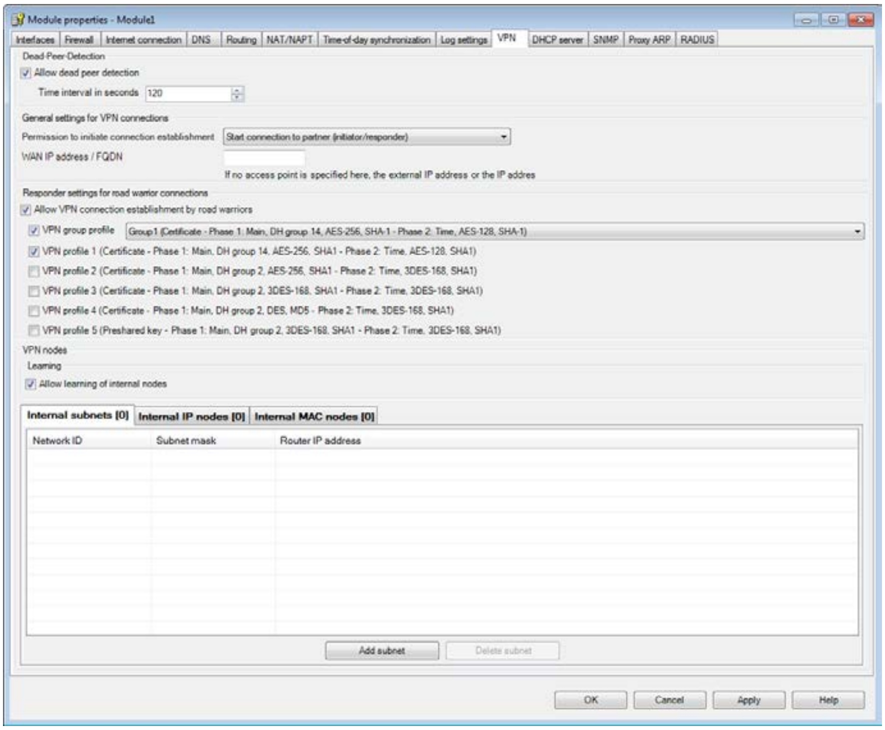
Comment

Example 2: VPN connection establishment by Unknown Peer

The following figure illustrates the network establishment between an initiator and a responder. The initiator is an Unknown Peer and is intended to establish a VPN connection to the responder with the properties of the VPN group "VPN Group 1".


NAT router
IP address ext.: 172.16.40.24 / 16
IP address int.: 192.168.50.45 / 24
VPN group 1
SCALANCE S
Initiator
IP address ext.: 192.168.50.3 / 24
IP address int.: 192.168.70.1 / 24
VPN interface: Ext.
SCALANCE S
Responder
IP address ext.: 172.16.40.26 / 16
IP address int.: 192.168.50.2 / 24
VPN interface: Ext.

As default, the responder allows VPN connection establishment by Unknown Peers with the properties of the predefined VPN profile 1. To allow the VPN connection establishment with the properties of the VPN group "VPN Group 1", this VPN group must be selected in the module-specific properties of the responder.



Dead-Peer-Detection

☑ Allow dead peer detection

Time interval in seconds: 120

General settings for VPN connections

Permission to initiate connection establishment: Start connection to partner (initiator/responder)

WAN IP address / FQDN:

If no access point is specified here, the external IP address or the IP addres

Responder settings for road warrior connections

☑ Allow VPN connection establishment by road warriors

☑ VPN group profile: Group1 (Certificate - Phase 1: Main, DH group 14, AES-256, SHA-1 - Phase 2: Time, AES-128, SHA-1)

☑ VPN profile 1 (Certificate - Phase 1: Main, DH group 14, AES-256, SHA1 - Phase 2: Time, AES-128, SHA1)

☐ VPN profile 2 (Certificate - Phase 1: Main, DH group 2, AES-256, SHA1 - Phase 2: Time, 3DES-168, SHA1)

☐ VPN profile 3 (Certificate - Phase 1: Main, DH group 2, 3DES-168, SHA1 - Phase 2: Time, 3DES-168, SHA1)

☐ VPN profile 4 (Certificate - Phase 1: Main, DH group 2, DES, MD5 - Phase 2: Time, 3DES-168, SHA1)

☐ VPN profile 5 (Preshared key - Phase 1: Main, DH group 2, 3DES-168, SHA1 - Phase 2: Time, 3DES-168, SHA1)

VPN nodes

Learning

☑ Allow learning of internal nodes

Network ID	Subnet mask	Router IP address

6.5.2 Including module in configured VPN group

The configured group properties are adopted for modules to be included in an existing VPN group.

Including active nodes in a VPN group

If an active node is added to an existing VPN group, this can reach the group nodes without needing to download the project to all nodes of the VPN group again.

Note

If you remove an active node from an existing VPN group, this can still establish a connection to the group nodes even if you have downloaded the project to all nodes of the VPN group again.

If you do not want the removed active node to be able to establish a connection any longer, renew the CA certificate of the VPN group and download the project again to the nodes of the VPN group.

The CA certificate of the VPN group can be renewed in the group properties of the VPN group or in the certificate manager, "Certification authorities" tab.

Follow the steps below

During this procedure, the following distinctions must be made:

- **Case a:** If you have not changed the group properties and the module to be added establishes the connection actively to the already configured modules:

1. Add the new module to the VPN group.
2. Download the configuration to the new module.

- **Case b:** If you have changed the group properties or the module to be added does not establish the connection actively to the already configured security modules actively:

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

Advantage in case a

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

6.5.3 Configuring module-specific VPN properties

Meaning

You can configure the following module-specific properties for data exchange via the IPsec tunnel in the VPN:

- Dead peer detection ~~SC M~~
- Permission to initiate connection establishment ~~M875~~
- WAN IP address / FQDN for communication via Internet gateways ~~M875~~
- Responder settings for Road Warrior connections
- VPN nodes ~~SC M~~

Requirements

- You can only make settings in the "VPN" tab if the module you are configuring is in a VPN group.
- The "VPN nodes" dialog area in the "VPN" tab is only displayed if the project is in advanced mode. ~~SC M~~

How to access this function

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

   The settings made here are adopted as settings for the entire module for settings that can be made for specific connections. Settings for specific connections can overwrite settings for the entire module and can be configured in the Details window. You will find further information on configuring settings for specific connections in the following section: Configuring VPN properties for specific connections (Page 234)

Dead peer detection (DPD) ~~SC M~~

As default, DPD is enabled. For DPD to operate reliably, it must be activated on both security modules involved.

If DPD is activated, the security modules exchange additional messages at selectable intervals when there is currently no data traffic via the VPN tunnel. 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 setting the SA lifetime, see the following section
Configuring VPN group properties (Page 219)

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 for the setting of the parameter described is the assignment of the 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 partner (initiator/responder) (default)	If this option is selected, the module is "active", in other words, it attempts to establish a connection to a partner. The reception of requests for VPN connection establishment is also possible. This option is recommended if the module being configured is assigned a dynamic IP address by the ISP. The partner is addressed using its configured WAN IP address, its configured external module IP address or the configured DNS name.
Wait for partner (responder)	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 if the module being configured is assigned a static IP address by the ISP.

Note

Make sure that you do not set all the modules in a VPN group to "Wait for partner" otherwise no connection is established.

WAN IP address / FQDN - 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 public IP addresses of the partner modules in the VPN that need to be reached via the Internet.

Note

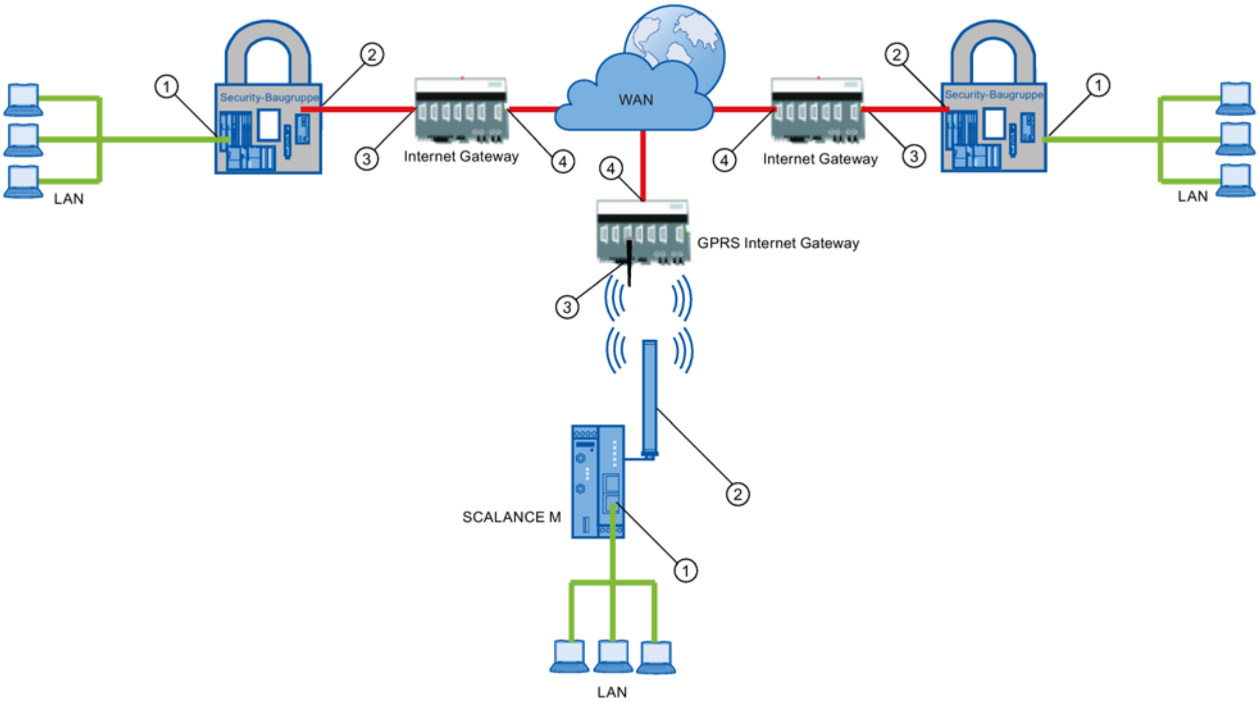
If you use a DSL router as Internet gateway, the following ports (at least) must be opened on it as described in the relevant documentation and the data packets forwarded to the module:

- Port 500 (ISAKMP)
- Port 4500 (NAT-T)

To do this, it is possible to specify a "WAN IP address" in the configuration of the security or SCALANCE M modules. When you download the module configuration, the group members are then informed of the WAN IP addresses of the partner modules. As an alternative to a WAN IP address, you can also enter an FQDN. If you have configured dynamic DNS on the security module at the same time, this FQDN must match the FQDN entered in the "DNS" tab that is registered with a provider for dynamic DNS.

Whether the external IP address, the IP address of the DMZ interface (only SCALANCE S623 / S627-2M) or the WAN IP address / the FQDN will be used can be specified in the VPN properties for specific connections. For more detailed information on VPN properties for specific connections, refer to the following section:
Configuring VPN properties for specific connections (Page 234)

If you do not enter an access point here, the external IP address or the IP address of the DMZ interface (SCALANCE S623/S627-2M only) will be used as the VPN endpoint. For SCALANCE M-800 modules configured as responders, an access point must be specified.



① Internal IP address - of a security module
② External IP address - of a module
③ IP address of an Internet gateway (for example GPRS gateway)
④ IP address (WAN IP address) of an Internet gateway (for example DSL router)

Responder settings for Road Warrior connections

The VPN connection establishment by Unknown Peers (Road Warriors) is allowed by the responder as default with the secure VPN properties of VPN profile 1. You can allow or block the VPN connection establishment by Unknown Peers and the properties used by selecting a VPN group profile and by selecting VPN profiles.

Check box	Meaning
Allow VPN connection establishment by Road Warriors	The responder allows VPN connection establishment by Unknown Peers.
VPN group profile	The responder allows VPN connection establishment by Unknown Peers with the properties of the VPN group selected in the drop-down list. The VPN groups can be selected in which the responder is located. If VPN connection establishment by Unknown Peers with the properties of the VPN group in which the responder and the Unknown Peers are located is to be allowed, this VPN group must be selected in the drop-down list.
VPN profile 1 - 5	The responder allows VPN connection establishment by Unknown Peers with the properties of the predefined VPN profiles 1 - 5. The properties of these VPN profiles correspond to the properties of the fallback VPN profiles that you can select for VPN groups, see section Configuring VPN group properties (Page 219).

For VPN connections from SOFTNET Security Client / SCALANCE M-800 modules to SCALANCE S / CPs the selected VPN profile with the highest priority is always used and read out. The authentication method of the selected VPN profile must match the authentication method of the corresponding VPN group. The priority of the VPN profile is as follows:

1 Selected VPN group profile
2. VPN profile 1
3. VPN profile 2
4. VPN profile 3
5. VPN profile 4
6. VPN profile 5

For VPN connections from SCALANCE M875 modules to SCALANCE S / CPs, VPN profile 3 must be selected if the authentication method of the corresponding VPN group is "Certificate". If the authentication method of the corresponding VPN group is "Preshared key", VPN profile 5 must be selected.

Configuring VPN nodes ~~SCA-M~~

In the "VPN nodes" dialog area, you enable the subnets or nodes for VPN tunnel communication.

Which nodes and subnets need to be enabled and how they are enabled for VPN tunnel communication is explained in the following sections:

Configuring other nodes and subnets for the VPN tunnel (Page 243)

Configuring internal network nodes (Page 242)

See also

Including module in configured VPN group (Page 229)

6.5.4 Configuring VPN properties for specific connections

Meaning

While module-specific VPN properties are configured for a specific module, connection-specific VPN properties relate to the VPN connections of a module. If a module establishes several tunnel connections to other modules, with connection-specific VPN properties, it is possible, for example, to configure which connections the module initiates and which it does not.

Requirements

- The module is a member of a VPN group.

How to access this function

1. Select the VPN group in the navigation panel to which the module you are editing belongs.
2. In the content area, select the module whose properties you want to configure.

   In the Details window, you can now configure the connection-specific VPN properties. The default values were taken from the module-specific VPN properties.

Parameter

Parameter	Meaning
Initiator/Responder	Specifies the permission to initiate connection establishment
Partner module	Display of the module name of the partner module.
Type of transferred packets	Display of the layer on which the packets are transferred.
Local interface	Specifies the interface that will be used as the VPN endpoint on the selected partner module. If a WAN access point (IP address / FQDN) is configured for the module, this can also be selected here.
Partner interface	Specifies the interface that will be used as the VPN endpoint on the partner module. If a WAN access point (IP address / FQDN) is configured for the VPN partner, this can also be selected here.

6.6 Configuration data for SCALANCE M modules

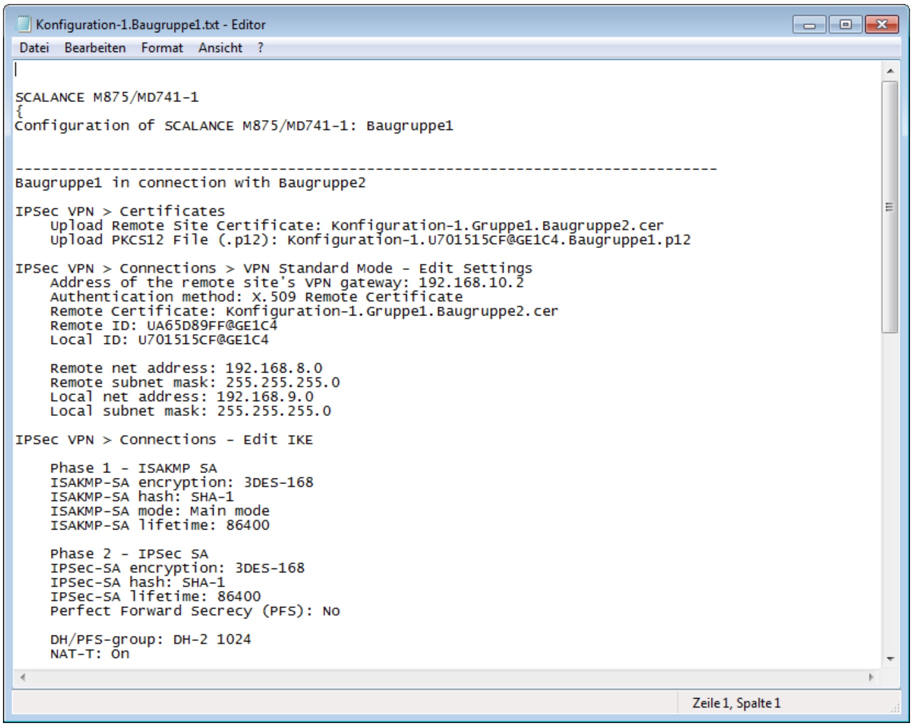
SCA. M

Meaning

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

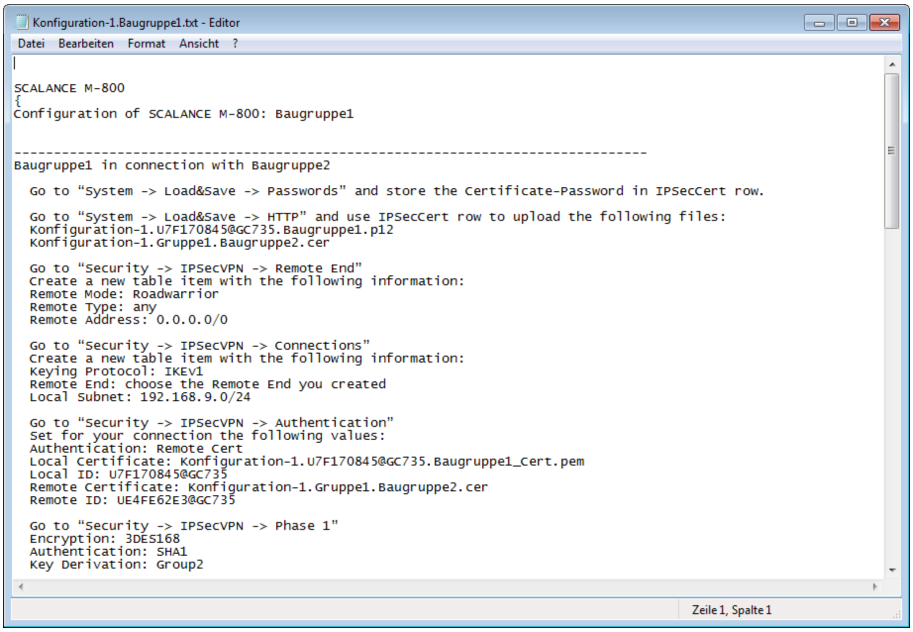
The following file types are generated:

- 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.
  - Export file for SCALANCE M875 modules:



```
SCALANCE M875/MD741-1
{
Configuration of SCALANCE M875/MD741-1: Baugruppe1


--------------------------------------------------------------------------------
Baugruppe1 in connection with Baugruppe2

IPSec VPN > Certificates
    Upload Remote Site Certificate: Konfiguration-1.Gruppe1.Baugruppe2.cer
    Upload PKCS12 File (.p12): Konfiguration-1.U701515CF@GE1C4.Baugruppe1.p12

IPSec VPN > Connections > VPN Standard Mode - Edit Settings
    Address of the remote site's VPN gateway: 192.168.10.2
    Authentication method: X.509 Remote Certificate
    Remote Certificate: Konfiguration-1.Gruppe1.Baugruppe2.cer
    Remote ID: UA65D89FF@GE1C4
    Local ID: U701515CF@GE1C4

    Remote net address: 192.168.8.0
    Remote subnet mask: 255.255.255.0
    Local net address: 192.168.9.0
    Local subnet mask: 255.255.255.0

IPSec VPN > Connections - Edit IKE

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

    Phase 2 - IPSec SA
    IPSec-SA encryption: 3DES-168
    IPSec-SA hash: SHA-1
    IPSec-SA lifetime: 86400
    Perfect Forward Secrecy (PFS): No

    DH/PFS-group: DH-2 1024
    NAT-T: On
```

  - Export file for SCALANCE M-800 modules:



```
SCALANCE M-800
{
Configuration of SCALANCE M-800: Baugruppe1


--------------------------------------------------------------------------------
Baugruppe1 in connection with Baugruppe2

  Go to “System -> Load&Save -> Passwords” and store the Certificate-Password in IPSecCert row.

  Go to “System -> Load&Save -> HTTP” and use IPSecCert row to upload the following files:
  Konfiguration-1.U7F170845@GC735.Baugruppe1.p12
  Konfiguration-1.Gruppe1.Baugruppe2.cer

  Go to “Security -> IPSecVPN -> Remote End”
  Create a new table item with the following information:
  Remote Mode: Roadwarrior
  Remote Type: any
  Remote Address: 0.0.0.0/0

  Go to “Security -> IPSecVPN -> Connections”
  Create a new table item with the following information:
  Keying Protocol: IKEv1
  Remote End: choose the Remote End you created
  Local Subnet: 192.168.9.0/24

  Go to “Security -> IPSecVPN -> Authentication”
  Set for your connection the following values:
  Authentication: Remote Cert
  Local Certificate: Konfiguration-1.U7F170845@GC735.Baugruppe1_Cert.pem
  Local ID: U7F170845@GC735
  Remote Certificate: Konfiguration-1.Gruppe1.Baugruppe2.cer
  Remote ID: UE4FE62E3@GC735

  Go to “Security -> IPSecVPN -> Phase 1”
  Encryption: 3DES168
  Authentication: SHA1
  Key Derivation: Group2
```

- VPN group certificates for the module
  - File type of the private key: *.p12 file
  - The file contains the VPN group certificate of the module and the relevant key material.
  - Access is password protected.
- CA certificates of VPN groups
  - File type: *.cer file

Note

Configuration files are not transferred to the module. An ASCII file is generated with which you can configure the VPN-relevant properties of 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.

Note

Protecting exported configuration files from unauthorized access

Configuration files for SCALANCE M exported from the Security Configuration Tool can contain security related information. You should therefore make sure that these files are protected from unauthorized access. This is particularly important when passing on the files.

Generating configuration files

1. Select the module to be edited.
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 following dialog specify whether a separate password should be created for the VPN group certificate of the module.

   If you select "No", the project name is assigned as the password (for example SCALANCE_M_configuration1), 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 relevant SCALANCE M modules.

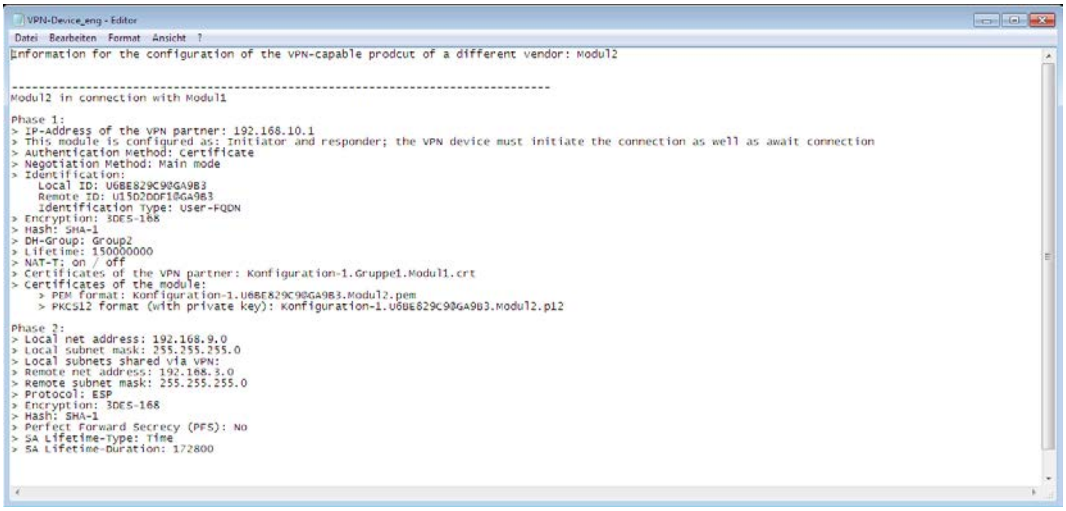
6.7 Configuration data for VPN devices

Meaning

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

The following files are generated:

- Export file with the configuration data
  - File type: *.txt file in ASCII format
  - Contains the exported configuration information for the VPN device including information on the additionally generated certificates.



```
Information for the configuration of the VPN-capable prodcut of a different vendor: Modul2


--------------------------------------------------------------------------------
Modul2 in connection with Modul1

Phase 1:
> IP-Address of the VPN partner: 192.168.10.1
> This module is configured as: Initiator and responder; the VPN device must initiate the connection as well as await connection
> Authentication Method: Certificate
> Negotiation Method: Main mode
> Identification:
    Local ID: U6BE829C90GA9B3
    Remote ID: U15D2DDF10GA9B3
    Identification Type: User-FQDN
> Encryption: 3DES-168
> Hash: SHA-1
> DH-Group: Group2
> Lifetime: 150000000
> NAT-T: on / off
> Certificates of the VPN partner: Konfiguration-1.Gruppe1.Modul1.crt
> Certificates of the module:
    > PEM format: Konfiguration-1.U6BE829C90GA9B3.Modul2.pem
    > PKCS12 format (with private key): Konfiguration-1.U6BE829C90GA9B3.Modul2.p12

Phase 2:
> Local net address: 192.168.9.0
> Local subnet mask: 255.255.255.0
> Local subnets shared via VPN:
> Remote net address: 192.168.3.0
> Remote subnet mask: 255.255.255.0
> Protocol: ESP
> Encryption: 3DES-168
> Hash: SHA-1
> Perfect Forward Secrecy (PFS): No
> SA Lifetime-Type: Time
> SA Lifetime-Duration: 172800
```

Figure 6-1 Export file for a VPN device

- VPN group certificates of the VPN device
- VPN group certificates of partner modules
- Private keys
- CA certificates of VPN groups

Configuring file types

For VPN devices, you can specify the file types in which the generated data is saved.

To do this, select the VPN device you want to edit and then select the menu command "Edit" > "Properties...".

- VPN group certificates of the VPN device
  - *.crt file: Base64-coded certificate
  - *.crt file: DER coded certificate
  - *.pem file: Base64-coded certificate
  - *.cer file: CER coded certificate
  - *.der file: DER coded certificate
- VPN group certificates of partner modules:
  - *.crt file: Base64-coded certificate
  - *.crt file: DER coded certificate
  - *.pem file: Base64-coded certificate
  - *.cer file: CER coded certificate
  - *.der file: DER coded certificate
- Private keys:
  - *.p12 file: Password-protected PKCS12 archive with private key
  - *.key: Unprotected Base64-coded private key
- Certification authorities of the VPN groups:
  - *.crt file: Base64-coded certificate
  - *.crt file: DER coded certificate
  - *.pem file: Base64-coded certificate
  - *.cer file: CER coded certificate
  - *.der file: DER coded certificate

Note

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

Configuring subnets to be released

In the properties of the VPN device, enter the subnets that need to be released for tunnel communication.

Generating configuration files

1. Select the VPN device to be edited.
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 project name is assigned as the password (for example VPN_project_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.

6.8 Configuration data for NCP VPN clients (Android)

NCP Secure VPN Client for Android

The NCP Secure Android Client allows a highly secure VPN connection to central data networks of companies and organizations. Access to several different data networks is possible using a separate VPN profile.

Based on the IPsec standard, tablets and smart phones can establish encrypted data connections to VPN gateways of all well-known providers.

The client can be obtained in two variants from the Google Play Store:

- NCP Secure VPN Client for Android (authentication with pre-shared key)
- NCP Secure VPN Client Premium for Android (authentication with pre-shared key or certificate)

You will find further information on NCP Secure Android Clients here:

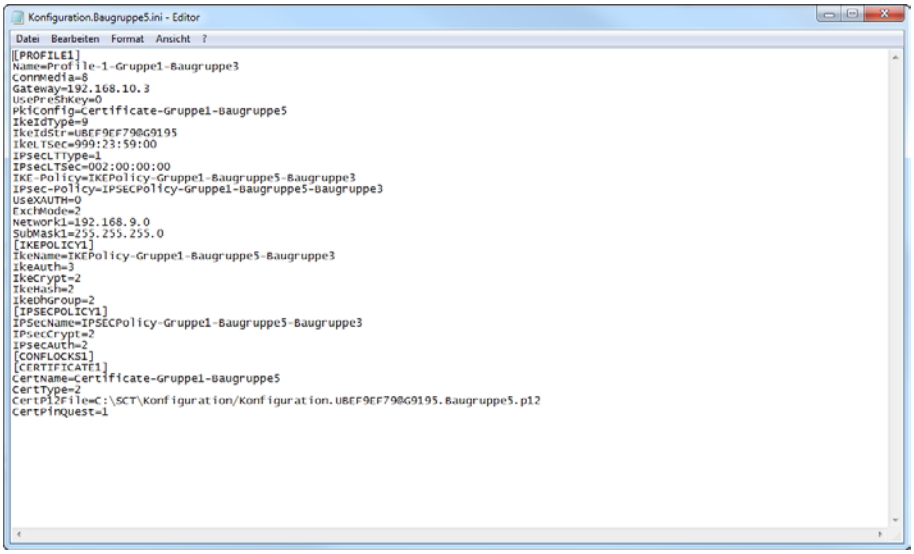
NCP Secure VPN Client for Android (http://www.ncp-e.com/en/products/ipsec-vpn-client-for-android.html)

Meaning

You can generate the VPN information for the assignment of parameters to an NCP VPN client (Android) using the Security Configuration Tool. With the generated files, you can then configure the NCP VPN client software.

The following file types are generated:

- Export file with the configuration data
  - File type: *.ini file in UTF-8 format
  - Contains the exported configuration information for the NCP VPN client (Android) including information on the additionally generated certificates.
- VPN group certificates for the module
  - File type of the private key: *.p12 file
  - The file contains the VPN group certificate of the module and the key material.
  - Access is password protected.
- CA certificates of VPN groups:
  - File type *.crt file



```
[PROFILE1]
Name=Profile-1-Gruppe1-Baugruppe3
ConnMedia=8
Gateway=192.168.10.3
UsePreShKey=0
PkiConfig=Certificate-Gruppe1-Baugruppe5
IkeIdType=9
IkeIdStr=UBEF9EF798G9195
IkeLTSec=999:23:59:00
IPsecLTType=1
IPsecLTSec=002:00:00:00
IKE-Policy=IKEPolicy-Gruppe1-Baugruppe5-Baugruppe3
IPsec-Policy=IPSECPolicy-Gruppe1-Baugruppe5-Baugruppe3
UseXAUTH=0
ExchMode=2
Network1=192.168.9.0
SubMask1=255.255.255.0
[IKEPOLICY1]
IkeName=IKEPolicy-Gruppe1-Baugruppe5-Baugruppe3
IkeAuth=3
IkeCrypt=2
IkeHash=2
IkeDhGroup=2
[IPSECPOLICY1]
IPSecName=IPSECPolicy-Gruppe1-Baugruppe5-Baugruppe3
IPsecCrypt=2
IPsecAuth=2
[CONFLOCKS1]
[CERTIFICATE1]
CertName=Certificate-Gruppe1-Baugruppe5
CertType=2
CertP12File=C:\SCT\Konfiguration/Konfiguration.UBEF9EF798G9195.Baugruppe5.p12
CertPinQuest=1
```

Figure 6-2 Export file for an NCP VPN client (Android)

Note

Configuration files are not transferred to the NCP VPN client (Android). An ASCII file is generated with which you can configure the NCP VPN client (Android). To allow this, the NCP VPN client (Android) must be located in at least one VPN group with a security module.

Configuring the storage path

With the menu command "Edit" > "Properties", you can configure the storage path on the NCP VPN client (Android).

Generating configuration files

1. In the content area, select the NCP VPN client (Android) you want to edit.
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 project name is assigned as the password (for example NCP_project_02), not the project password.

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

Result: The files are stored in the folder you specify.

6.9 Configuring internal network nodes

~~SCA-M~~

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.

SCALANCE S

Apart from the static configuration of the network nodes, a SCALANCE S module also provides the option of learning these automatically.
How to configure the network nodes is described in the following section:
Configuring other nodes and subnets for the VPN tunnel (Page 243)

For more information on automatic learning of internal network nodes, refer to the following section:
How the learning mode works (Page 244)

CP x43-1 Adv. and CP 1628

- CP x43-1 Adv.

  Decide whether or not tunnel communication to the CP and/or to the internal subnet is permitted for VPN connection partners in routing mode (SCALANCE S / M / VPN device / NCP VPN client (Android)).
- CP 1628

  Enter the NDIS nodes you want to be reachable through the tunnel of VPN connection partners in routing mode (SCALANCE S / M / VPN device / NCP VPN client (Android)).

6.9.1 Configuring other nodes and subnets for the VPN tunnel

SCA. S

Meaning

By adding a security module to a VPN group, the local, internal network nodes/subnets of the security module are automatically enabled for VPN tunnel communication. To allow communication via the VPN tunnel with other subnets or nodes of another subnet, these subnets or nodes need to be enabled for VPN tunnel communication in the configuration.

A subnet that needs to be enabled in the configuration may be as follows:

- A subnet that is reachable via the local network on the internal interface if a VPN tunnel terminates on the external interface or on the DMZ interface.
- A subnet that can be reached via the DMZ interface if a VPN tunnel terminates at the external interface.
- A subnet that can be reached via the external interface if a VPN tunnel terminates at the DMZ interface.

Requirement

Before the nodes or subnets can be enabled for tunnel communication, the following requirements must be met:

- The security module is in a VPN group.
- The "VPN nodes" dialog area in the "VPN" tab is only displayed if the project is 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 - Bridge mode

Note: If nodes or subnets connected to the DMZ interface (SCALANCE S623/S627-2M only) need to be enabled, follow the description for the routing mode.

1. Select the security module to be edited.
2. Select the "Edit" > "Properties..." menu command, "VPN" tab.
   You enable nodes and subnets during configuration in the "VPN nodes" dialog area.
3. If you want to enable entire subnets for tunnel communication, enter these in the "Internal subnets" tab. If you want to enable individual nodes for tunnel communication, enter the nodes in the "Internal IP nodes" or Internal MAC nodes" tab.

Note: Before subnets specified here can be reached, a router must also be entered in the "Routing" tab for them. In addition to this, the firewall must also allow communication with the nodes.

How to access this function - Routing mode

1. Select the security module to be edited.
2. Select the "Edit" > "Properties..." menu command, "VPN" tab.
   You enable subnets during configuration in the "VPN nodes" dialog area.
3. In the "Subnets to be reached through tunnel" tab, enter the network ID and the subnet mask of the subnet to be included in tunnel communication.

Note: Before subnets specified here can be reached, a router must also be entered in the "Routing" tab for them. In addition to this, the firewall must also allow communication with the subnets.

6.9.2 How the learning mode works

SCA. S

Finding nodes for tunnel communication automatically (SCALANCE S in bridge mode only)

One great advantage of configuration and operation of tunnel communication is that SCALANCE S modules can find nodes in the internal network automatically. This means that you do not need to configure the internal network nodes involved in tunnel communication manually.

New nodes are detected by the SCALANCE S module during operation. The detected nodes are signaled to the SCALANCE S module belonging to the same group. This allows data exchange within the tunnels of a VPN 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 an ICMP response to the ICMP subnet broadcast is sent.

  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 statically.

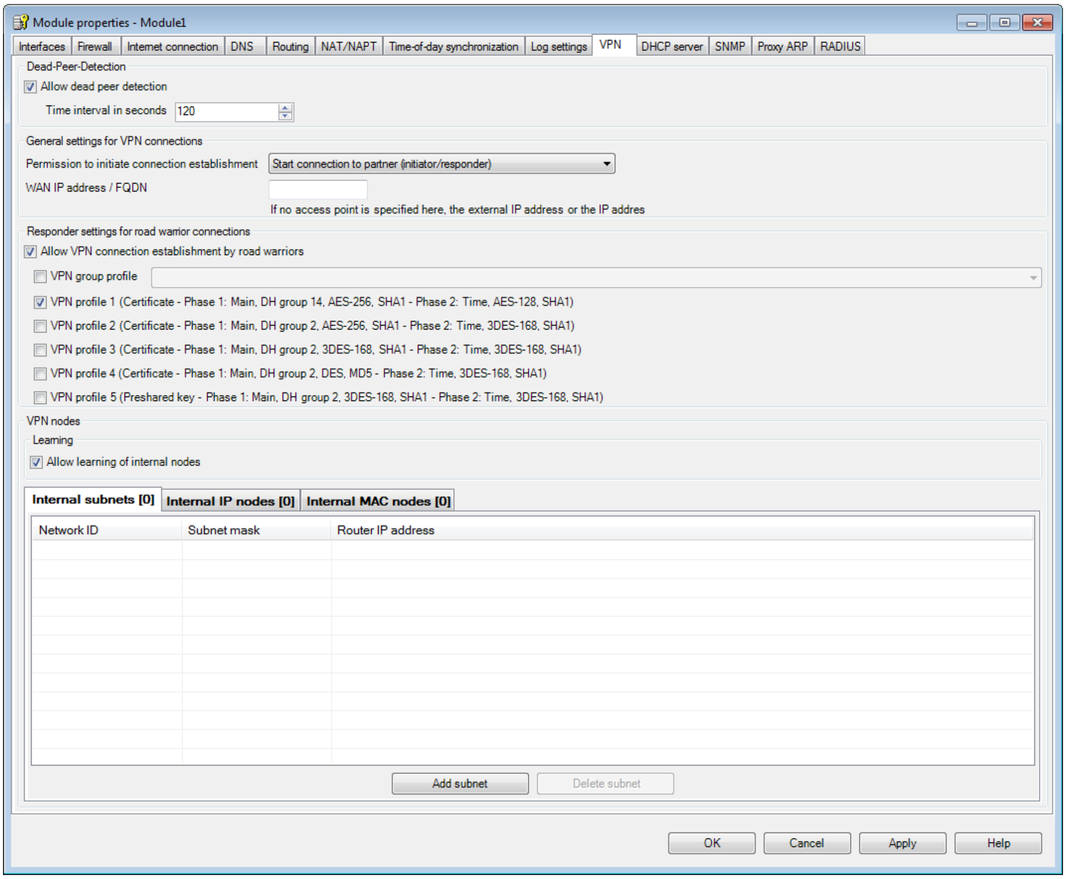
Note

No learning mode for VPN tunnel on DMZ interface S62x

The learning of internal nodes is supported only on interfaces that are connected in bridge mode. The DMZ interface is always connected in routing mode.

How to access the function

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



Dead-Peer-Detection

☑ Allow dead peer detection

Time interval in seconds 120

General settings for VPN connections

Permission to initiate connection establishment: Start connection to partner (initiator/responder)

WAN IP address / FQDN

If no access point is specified here, the external IP address or the IP addres

Responder settings for road warrior connections

☑ Allow VPN connection establishment by road warriors

☐ VPN group profile

☑ VPN profile 1 (Certificate - Phase 1: Main, DH group 14, AES-256, SHA1 - Phase 2: Time, AES-128, SHA1)

☐ VPN profile 2 (Certificate - Phase 1: Main, DH group 2, AES-256, SHA1 - Phase 2: Time, 3DES-168, SHA1)

☐ VPN profile 3 (Certificate - Phase 1: Main, DH group 2, 3DES-168, SHA1 - Phase 2: Time, 3DES-168, SHA1)

☐ VPN profile 4 (Certificate - Phase 1: Main, DH group 2, DES, MD5 - Phase 2: Time, 3DES-168, SHA1)

☐ VPN profile 5 (Preshared key - Phase 1: Main, DH group 2, 3DES-168, SHA1 - Phase 2: Time, 3DES-168, SHA1)

VPN nodes

Learning

☑ Allow learning of internal nodes

Network ID	Subnet mask	Router IP address

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 is 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 network nodes in the internal network resulting from the learning packets. The performance of the SCALANCE S module is also improved since it does not need to process the learning frames.

Note: In learning mode, all network nodes in the internal network are detected. The information relating to VPN configuration limits relates only to network nodes that communicate over VPN in the internal network.

Note

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.

Network nodes that cannot be learnt

There are nodes in the internal network that cannot be learnt. This involves nodes of subnets located in the local internal network of the SCALANCE S module (for example downstream from routers). These subnets can also not be learnt. Nodes and subnets that cannot be learnt must be configured statically in advanced mode.

Note

No return to standard mode possible

If you switch to 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.

6.9.3 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.

   Result: The found internal network nodes are displayed.

Router and firewall redundancy 7

7.1 Overview

Meaning

Failures of the security modules SCALANCE S623 as of V4 and SCALANCE S627-2M as of V4 can be automatically compensated by routers and firewall redundancy during operation. To do this, group two security modules of the type SCALANCE S623 or SCALANCE S627-2M in a redundancy relationship and then decide which will be the active security module of the redundancy relationship during normal operation. If the active security module fails, the passive security module automatically takes over its function as firewall and (NAT/NAPT) router. To ensure the identical configuration of both security modules, these are connected together via their DMZ interfaces and their configurations are synchronized during operation. In this case, the DMZ interfaces of the security modules involved cannot be used for other purposes.

Address redundancy

In addition to their module IP addresses, the two security modules share a common IP address on the external and on the internal interface so that if one of the security modules fails, the IP addresses do not need to be changed. To do this, you need to configure an IP address for the external and for the internal interface of the redundancy relationship.

Configuring redundancy relationships and the security modules involved

After the security modules have been included in a redundancy relationship, part of the module properties is configured solely based on the redundancy relationship. This part of the module properties is disabled for the individual security modules and only becomes active and editable again after removing the security modules from the redundancy relationship. The following properties are configured based on the redundancy relationship:

- Basic settings of the redundancy relationship (network parameters, primary module)
- Firewall
- Routing
- NAT/NAPT routing (not 1:1 NAT)

The settings listed below remain active for the individual security modules even after including them in a redundancy relationship. These settings can still be adapted separately for both security modules.

- Interface settings (it is not possible to deactivate interfaces)
- Standard rules for IP services (firewall)
- DDNS
- Time-of-day synchronization

- Log settings
- SNMP
- MRP/HRP
- RADIUS

Note

Loading a configuration on security modules of a redundancy relationship (only SCALANCE S623/S627-2M as of V4)

The configured properties of a redundancy relationship must be loaded on both security modules. To load the configuration, the physical IP address via which your engineering station can reach the security module must be used. The virtual IP addresses of the redundancy relationship cannot be used for loading.

Note

Configuring routing when using router and firewall redundancy

In a redundancy relationship only routing information is synchronized between the security modules that was configured statically in the properties of the redundancy relationship in the “Routing” tab. Routing entries resulting dynamically due to using standard routers are not synchronized. When using routers and firewall redundancy it is therefore recommended that you configure all known routers statically.

7.2 Creating redundancy relationships and assigning security modules

Requirements

Security modules can only be assigned to a redundancy relationship if they meet the following requirements:

- Security module is of the type "S623 V4" or "S627-2M V4"
- The security module is in routing mode.
- All interfaces of the security module are active
- IP assignment method "static address" is configured for all interfaces
- The security module is not a member of a VPN group.
- The security module is not assigned to any other redundancy relationship

Procedure

1. Select the "Redundancy relationships" object in the navigation panel.
2. Select the menu command "Insert redundancy relationship..." in the shortcut menu (right mouse key) of the object.

   Result: The created redundancy relationship is shown in the navigation panel.
3. Assign the security modules to the redundancy relationship by selecting them in the content area and dragging them to the created redundancy relationship in the navigation panel.
4. in the "Configuration of the redundancy relationship" dialog, you have the following options for configuring the redundancy relationship:
   – Adoption of the configuration from the "Firewall", "Routing" and "NAT/NAPT" tabs of a security module for the redundancy relationship. From the drop-down list, you can select the security module whose configuration you want to use for the redundancy relationship. This overwrites an existing configuration of the redundancy relationship.
   – Creation of the assigned security module within the redundancy relationship. This is possible only when only one security module is assigned to a created redundancy relationship.

   As an alternative, you can configure the redundancy relationship later using the properties of the redundancy relationship, see section:
   Configuring redundancy relationships (Page 251)

Result: You have created a redundancy relationship and assigned the required security modules to it.

7.3 Configuring redundancy relationships

How to access this function

Select the redundancy relationship in the navigation panel and select the "Edit" > "Properties..." menu command.

Configuring network parameters of the redundancy relationship

Table 7- 1 Parameters in the "Basic settings" tab

Configurable parameter	Meaning
Primary module	Selection of the security module that will be the active security module in normal operation.
Activate virtual router ID (only SCALANCE S623/S627-2M as of firmware V4.0.1)	If you enable this check box, you can adapt the virtual router IDs of the virtual interfaces. Using a virtual router ID, the virtual MAC address of a virtual interface is specified. Possible values: 01...FF
IP address	Virtual IP address of the external or internal interface of the redundancy relationship

Configurable parameter	Meaning
Subnet mask	Subnet mask of the virtual external or internal interface of the redundancy relationship
Comment	Optional comment
Virtual router ID (only SCALANCE S623/S627-2M as of firmware V4.0.1)	Using a virtual router ID, the virtual MAC address of a virtual interface is specified.

For general information on configuring network parameters, refer to the following section:
Creating modules and setting network parameters (Page 91)

Configuring the firewall

The configuration of IP packet filter rules for redundancy relationships is basically the same as when configuring IP packet filter rules for individual security modules. The communications directions "From external to internal" and "From internal to external" are available.

For general information on configuring IP packet filter rules in advanced mode, refer to the following section:
IP packet filter rules (Page 155)

Configuring address translation with NAT/NAPT

The configuration of address translation with NAT/NAPT for the redundancy relationship is basically the same as configuring the address translation with NAT/NAPT for individual security modules. For redundancy relationships, only Source NAT and NAPT can be configured. With Source NAT, source IP addresses in the internal subnet can only be replaced with the virtual external IP address of the redundancy relationship. No alias IP addresses can be registered on the external interface of the redundancy relationship. With NAPT, only the "External to internal" address translation direction can be configured.

For general information on configuring address translations with NAT/NAPT, refer to the following section:
Address translation with NAT/NAPT (Page 177)

Configuring routing

The configuration of routes for the redundancy relationship is basically the same as when configuring routes for individual security modules.

For general information on configuring routing, refer to the following section:
Specifying a standard router and routes (Page 174)

See also

MAC packet filter rules (Page 164)

8 SOFTNET Security Client

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.

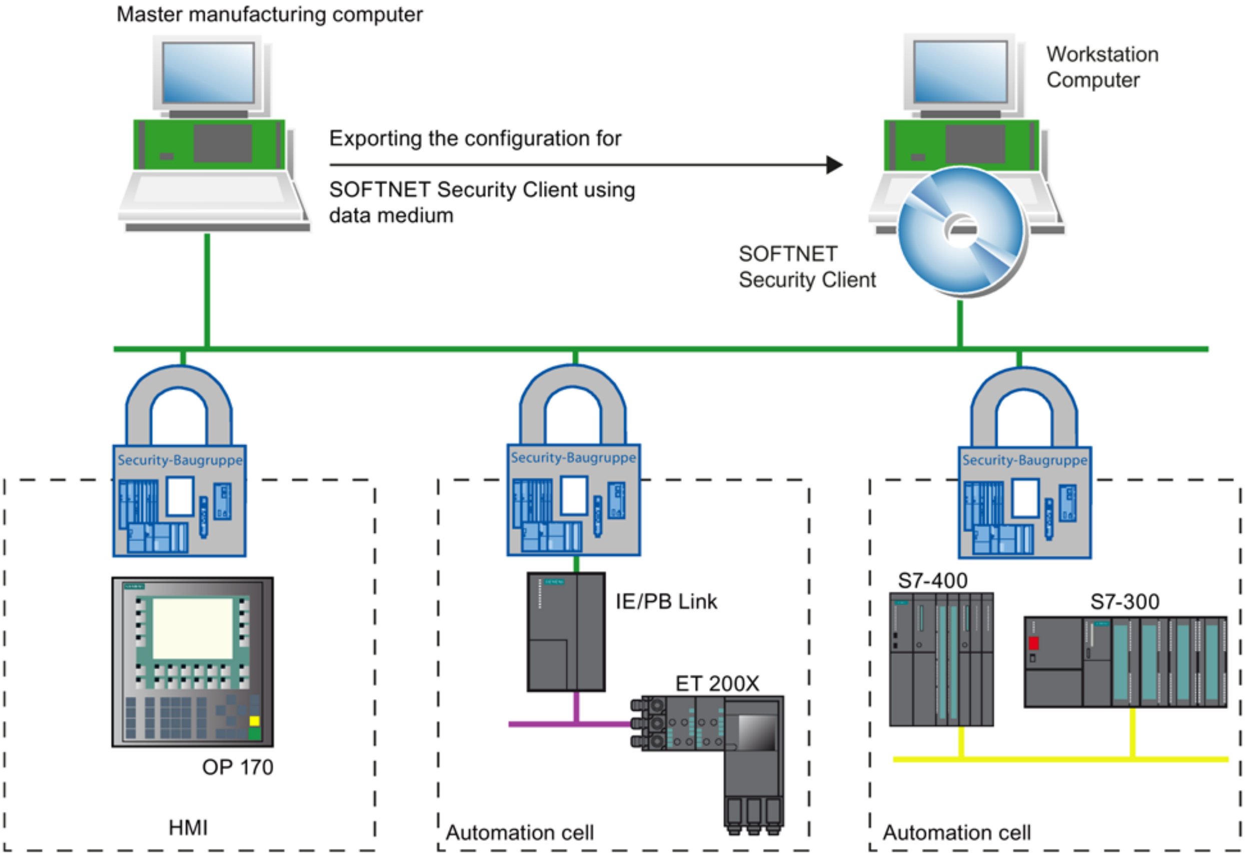
You can call this with the F1 key or using the "Help" button in the relevant dialog.

8.1 Using the SOFTNET Security Client

Area of application - access over VPN

With the SOFTNET Security Client, you configure a PC/PG so that it can automatically establish a secure IPsec tunnel connection in the VPN (Virtual Private Network) to 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.

Note

Via the IPsec tunnel, IP-based communication is possible only between SOFTNET Security Client and the security modules as well the internal nodes downstream from the security modules. Layer 2 communication is not possible with the SOFTNET Security Client.

Details in the online help

HELP
F1

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?

In the first step the configuration file is created for the SOFTNET Security client with the Security Configuration Tool or with STEP 7 as of V12.

The SOFTNET Security client then reads in the created configuration 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 services on and downstream from the security modules using IP addresses.

If the 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. The security policies of the newly learned internal nodes must be enabled manually.

Result: Applications such as STEP 7 communicate with the programmable controllers via VPN.

Supported operating systems

The SOFTNET Security Client is suitable for use with the following operating systems:

- Microsoft Windows 7 32/64-bit + Service Pack 1
- Microsoft Windows Server 2012 R2

If you use Microsoft Windows XP, use an earlier SSC version, e.g. SSC V4.0 for Windows XP 32-bit + Service Pack 3.

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.

8.2 Installation of the SOFTNET Security Client

8.2.1 Installing SOFTNET Security Client

Core statement

You install the SOFTNET Security Client PC software from the product DVD.

1. First read the information in the README file of your SCALANCE S DVD 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 DVD → this is started automatically when you insert the DVD or can be opened from the start.exe file. You can then select the entry "Installation SOFTNET Security Client" directly

NOTICE
Incompatibility with other VPN client software If other VPN client software is installed on your PC in addition to the SOFTNET Security Client, it may no longer be possible to establish VPN tunnels using the SOFTNET Security Client. You should therefore uninstall this VPN client software before using the SOFTNET Security Client.

Startup behavior

Downloading the security rules can take some time. The CPU of the PG/PC is utilized up to 100% during this time.

8.2.2 Uninstalling SOFTNET Security Client

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

8.3 Creating a configuration file with the Security Configuration Tool

Configuring SOFTNET Security Client in the SCT project

The SOFTNET Security Client is created as a module in the SCT project. In contrast to the other security modules, you do not need to configure any further properties.

Assign the created SOFTNET Security Client 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 VPN groups are adopted.

Note

Refer to the information on parameters in the following section:

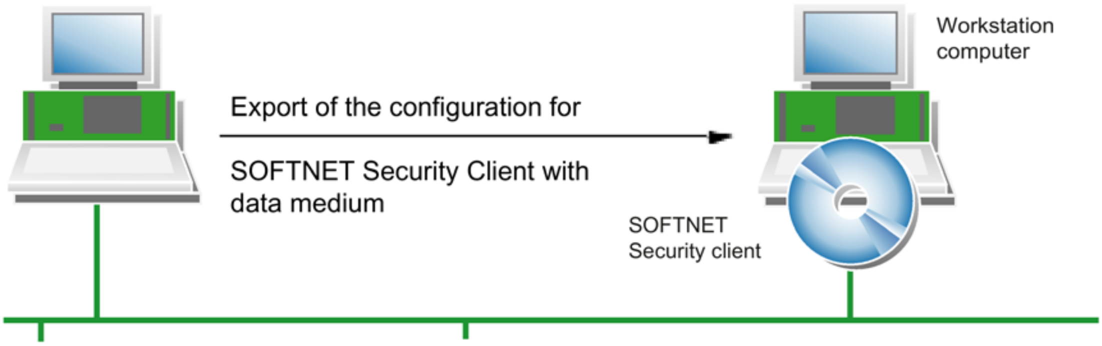
- Including module in configured VPN group (Page 229)

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.


Workstation computer
Export of the configuration for
SOFTNET Security Client with data medium
SOFTNET Security client

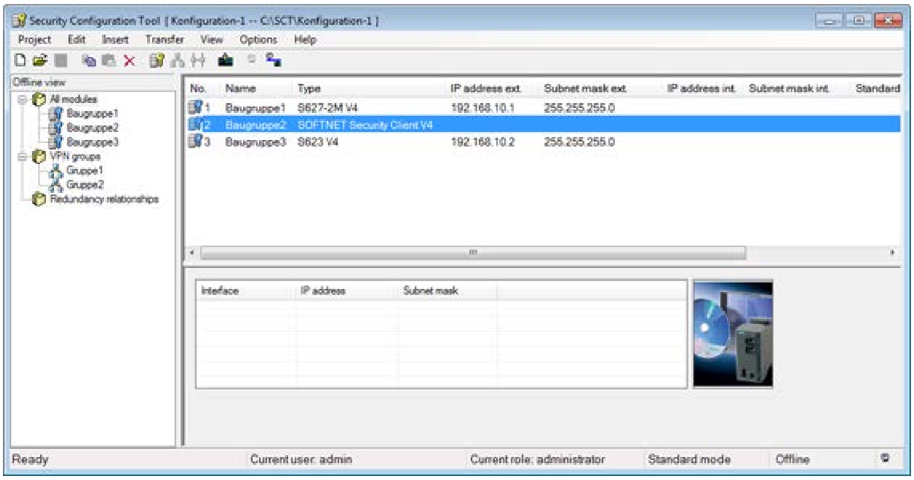
The configuration is stored in the following file types:

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

Procedure

To generate the configuration files, perform the following steps in SCT:

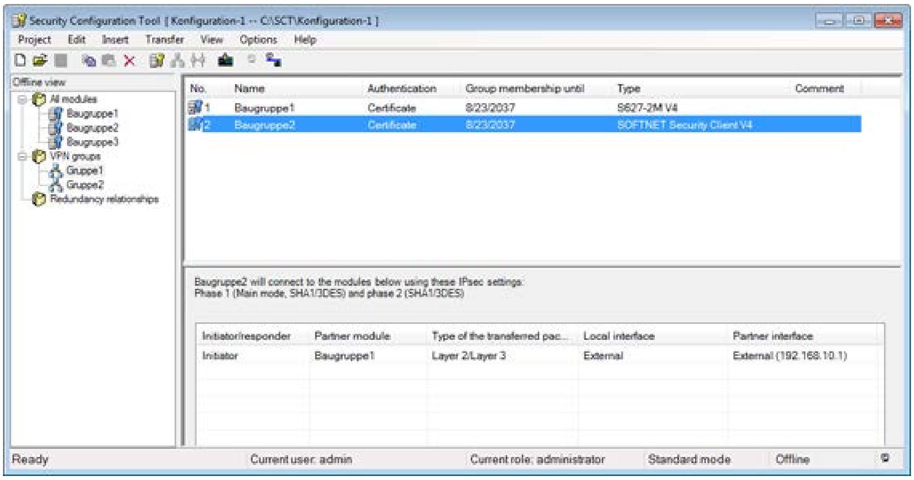
1. Create a module of the type SOFTNET Security Client in SCT.



No.	Name	Type	IP address ext.	Subnet mask ext.	IP address int.	Subnet mask int.	Standard
1	Baugruppe1	S627-2M V4	192.168.10.1	255.255.255.0			
2	Baugruppe2	SOFTNET Security Client V4					
3	Baugruppe3	S623 V4	192.168.10.2	255.255.255.0			

Interface	IP address	Subnet mask

2. Assign the SSC module to the VPN groups in which the PG/PC will communicate over IPsec tunnels.



No.	Name	Authentication	Group membership until	Type	Comment
1	Baugruppe1	Certificate	8/23/2037	S627-2M V4	
2	Baugruppe2	Certificate	8/23/2037	SOFTNET Security Client V4	

Baugruppe2 will connect to the modules below using these IPsec settings:
Phase 1 (Main mode, SHA1/3DES) and phase 2 (SHA1/3DES)

Initiator/responder	Partner module	Type of the transferred pac...	Local interface	Partner interface
Initiator	Baugruppe1	Layer 2/Layer 3	External	External (192.168.10.1)

3. Select the "Project" > "Save" menu command.

4. Select the module of the type "SOFTNET Security Client" and select the menu command "Transfer" > "To module(s)...".

5. Select the storage location for the configuration files.

6. In the following dialog specify whether a separate password should be created for the VPN group certificate of the module.

   If you select "No", the project name is assigned as the password (for example SCALANCE_SSC_configuration1), not the project password.

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

7. Transfer the files of the type *.dat, *.p12, *.cer to the PG/PC on which you want to operate the SOFTNET Security Client. Files of the type *.p12 only exist if you have selected "Certificate" as the authentication method in the Security Configuration Tool.

8.4 Main dialog of the 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 of a project or individual security modules. The PC/PG can access the security modules and the internal nodes via this IPsec tunnel.
- Enabling and disabling existing secure connections.
- Only possible when the learning mode is enabled: Setting up connections after adding end devices later.
- Checking a configuration; in other words, which connections are set up or possible.

Table 8- 1 Display boxes / options in the main dialog

Display box / option	Meaning
Started with user	User name of the user with whose logon data the SOFTNET Security Client was started. This logon data decides which SOFTNET Security Client configuration is called up. If the user name of the user that started SOFTNET Security Client differs from the user logged on to Windows, the displayed user name is highlighted in red.
Managed configuration	The configuration called up for a user or a group is displayed in the "Managed configuration" area. Every setting made in SOFTNET Security Client is then automatically adopted in this configuration. The "Type" box specifies whether the managed configuration involves a single or a group configuration. Only privileged users can change the managed configuration in the "Manage users and groups" dialog. You can open this using the menu command "Users/groups > Manage users and groups". You will find detailed information on the configuration privileges in SOFTNET Security Client in the section Setting a managed configuration - "Manage users and groups" dialog (Page 265)
SOFTNET Security client status	• Service: Indicates whether the SOFTNET Security Client service is running. • License: Indicates the license status of the SOFTNET Security Client. • Privileges: Indicates whether the user with whose logon data the SOFTNET security client was started currently has rights for the SOFTNET Security client to load from VPN configuration files and for extended SOFTNET Security Client settings. If the user has these rights in principle but did not start SOFTNET Security Client as an administrator, the user can have his or her privileges ranked higher using the "Elevate" button. You will find detailed information on the configuration privileges in SOFTNET Security Client in the section Setting a managed configuration - "Manage users and groups" dialog (Page 265)
Minimize	The user interface of the SOFTNET Security Client is minimized. The symbol for the SOFTNET Security Client remains visible in the Windows taskbar.
Quit	The user interface of the SOFTNET Security Client is closed. If the option "Limited" is enabled in the SOFTNET Security Client settings, all existing VPN tunnel connections are also terminated.

The following options are available in the “VPN control" if the SOFTNET Security client was started by a user with administrative rights.

Table 8- 2 Options in the dialog area "VPN control"

Option	Meaning
Load Configuration	With this button you open a file dialog for selecting the configuration file created with the Security Configuration Tool.
Disable / Enable	Disable / enable all secure tunnels.
Tunnel Overview	Dialog for setting up and diagnostics of the tunnel. In this dialog, you will find a list of the secure tunnels that can be set up.

If the SOFTNET Security client was started by a user without administrative rights only the button “Tunnel Overview" is available in the “VPN Diagnostics” dialog area.

NOTICE

Incompatibility with other VPN client software

If other VPN client software is installed on your PC in addition to the SOFTNET Security Client, it may no longer be possible to establish a VPN tunnel using the SOFTNET Security Client. You should therefore uninstall this VPN client software before using the SOFTNET Security Client.

8.5 Loading the configuration file and setting up tunnel connections

The following provides an overview of the steps involved in setting up tunnel connections. When you follow these steps, you will work through several dialogs for which you can call up specific additional information using the F1 key.

Requirement

You have started the SOFTNET Security Client with administrative rights.

Follow the steps below

1. With the "Load Configuration" button, open the dialog for importing the configuration file.
2. Select the configuration file created with the Security Configuration Tool.
3. If configuration data already exists in SOFTNET Security Client, you will be prompted to decide how to handle the new configuration data. If the VPN tunnel connections are to be established to all internal nodes of the security module, enable the check box "Establish VPN tunnel to the internal nodes". If you do not yet enable this here, you can do this later in the tunnel overview.
4. Select the network adapter from whose IP address the VPN tunnel connections will be established. In the tunnel overview, you can make this setting for specific modules using the shortcut menu of a module.

5. If you have selected Certificate as the authentication method in the Security Configuration Tool, you will now be prompted to enter your password.
6. If you have configured a SCALANCE M875 module, SCALANCE M-800 module or an S7 CP with DHCP activated on the Gbit interface in the Security Configuration Tool, the "DNS/IP settings" dialog opens. Follow the steps below depending on the configured module type:
   – For SCALANCE M875 modules and SCALANCE M-800 modules: Decide whether or not the tunnel to the module will be established using the IP address obtained from the ISP at runtime or alternatively using a DNS name.
   – For S7 CPUs with DHCP activated on the Gbit interface: Enter the IP address assigned using DHCP.

   Note

   Setting the firewall under Windows 7

   If you are asked for the networks in which you want to allow communication of the SOFTNET Security Client in Windows 7, you will need to allow communication of the SOFTNET Security Client in public networks otherwise the SOFTNET Security Client does not display learned nodes in the tunnel overview.

7. Now open the "Tunnel Overview" dialog with the "Tunnel Overview" button.
   In the table, you can see the security modules and nodes with status information about the tunnel connections.

See also

Setting a managed configuration - "Manage users and groups" dialog (Page 265)

8.6 Diagnosing and configuring a tunnel - "Tunnel Overview" dialog

Meaning

In the table that opens, you will see the modules and nodes with status information on the tunnel connections.

"Delete" button

With this, you delete all the IP security policies set up by the SOFTNET Security Client completely.

Selecting and working with a tunnel entry

You can select an entry and use the following shortcut menu commands:

Menu command	Meaning
Enable all members / disable all members	You can terminate set-up tunnel connections with the "Disable all Members" entry. Result: The symbol in the "Status" column of the tunnel overview is replaced. The security policy is disabled on the PC. To undo the change and to reactivate the tunnel connections, click the "Enable all Members" entry.
Select Network Device...	If you are using more than one network card in your PC, you can use this command to select the network card via which the selected node can be accessed.
Reachability test	A ping command is sent to the selected module.
Extended diagnostics	The "Extended Diagnostics" dialog is called up. In this dialog the module selected in the tunnel overview is selected.
Delete Entry	The IP security policy of the selected entry is deleted.

Note

Extension of the security policy when activating internal nodes

Please note that the security policy in the system is extended each time the internal nodes are activated. Deactivation of the overall system (via the shortcut menu of the higher-level SCALANCE S) does not result in the adjustment of the security policy but only to deactivation of the policy. This means that the deactivated overall security policy plus the additional internal node are activated when an internal node is activated. If you want to make sure that the established security policy completely refers to the nodes you activated, close the SOFTNET Security Client and reopen it.

Detecting expected members that are not displayed

If you recognize that required nodes are not displayed in the table, follow the steps outlined below:

Send a ping to the required node using the command line.

As a result of the ping, the security module learns the node and passes this information on to SOFTNET Security Client. If it is nevertheless not learned, you should configure the node statically in the VPN tab of the Security Configuration tool.

Note

Statically configured nodes and subnets

If you configure nodes or subnets statically at a later point in time, you will also need to download the configuration for a SOFTNET Security Client used in the VPN again.

Parameter

Parameter	Meaning / range of values
Status	You will find the meaning of the status displays in the following table.
Name	Name of the module or the node taken from the configuration file of the Security Configuration Tool.
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	IP address of the network card of your PC from where the VPN tunnel is established.

Table 8- 3 **Status information***

Symbol	Meaning
✕	There is no connection to the module or node.
➡	There are further nodes that are not displayed. Double-click on the symbol to display further nodes.
	Tunnel to node is disabled. There is no IP security policy set up in the system. You communicate with this node without encryption.
	Tunnel to node is enabled. There is an IP security policy set up in the system. You communicate with encryption and therefore securely with this node.
	Tunnel to SCALANCE S module is disabled. There is no IP security policy set up in the system. You communicate with this module without encryption.
	Tunnel to SCALANCE S module is enabled. There is an IP security policy set up in the system. You communicate with encryption and therefore securely with this module.
	Tunnel to SCALANCE S M875/M-800 module is disabled. There is no IP security policy set up in the system. You communicate with this module without encryption.
	Tunnel to SCALANCE S M875/M-800 module is enabled. There is an IP security policy set up in the system. You communicate with encryption and therefore securely with this module.
	Tunnel to CP343-1 Advanced is disabled. There is no IP security policy set up in the system. You communicate with this CP without encryption.
	Tunnel to CP 343-1 Advanced is enabled. There is an IP security policy set up in the system. You communicate with encryption and therefore securely with this CP.
	Tunnel to CP 443-1 Advanced is disabled. There is no IP security policy set up in the system. You communicate with this CP without encryption.
	Tunnel to CP 443-1 Advanced is enabled. There is an IP security policy set up in the system. You communicate with encryption and therefore securely with this CP.
	Tunnel to CP 1628 / CP 1243-1 / CP 1543-1 is disabled. There is no IP security policy set up in the system. You communicate with this CP without encryption. Note: The creation of configuration files for the SOFTNE Security client with which VPN tunnels can be established to the CP 1243-1 and CP 1543-1 is possible as of STEP 7 V12 SP1.

Symbol	Meaning
🔒	Tunnel to CP 1628 / CP 1243-1 / CP 1543-1 is enabled. There is an IP security policy set up in the system. You communicate with encryption and therefore securely with this CP. The creation of configuration files for the SOFTNE Security client with which VPN tunnels can be established to the CP 1243-1 and CP 1543-1 is possible as of STEP 7 V12 SP1.
🖧	Tunnel to internal subnet is disabled. There is no IP security policy set up in the system.
🖧	Tunnel to internal subnet is enabled. There is an IP security policy set up in the system.
🔴	Module / node cannot be reached.
🟡	Module / node can be reached, tunnel to module / node is, however, disabled. There is no IP security policy set up in the system. You communicate with this module / node without encryption.
🟢	Module / node can be reached, tunnel to module / node is enabled.
●	Reachability test disabled. No statement can be made as to whether the node can be reached.

* In Windows 7 SP1 and higher, the table is valid if the Windows firewall is enabled.

Logging Console

In the "Settings" dialog, you can select which entries are displayed in the log console. You can open this dialog in the main dialog with the menu command "Settings" > "SOFTNET Security Client settings".

The following information is shown:

- Diagnostics information about connection establishment with the configured security modules and internal nodes / subnets.
- Date and time stamp at the time of the events
- Establishment and termination of a security policy
- Negative reachability test (test ping) to the configured nodes
- Download configuration files
- Learn / unlearn internal nodes/subnets

Further notes

- Nodes that are still entered in the list, but no longer exist in the subnet, remain in the list for approximately 10 minutes during which time, they are checked to find out whether or not they are available again. If it can no longer be reached, the entry is removed from the list and a corresponding entry appears in the logging console.

8.7 Setting a managed configuration - "Manage users and groups" dialog

Privileged / non privileged users

In SOFTNET Security Client, a distinction is made between privileged and non-privileged users. Privileged users are users with administrator rights in Windows.

Privileged users

Privileged users can make all settings in SOFTNET Security Client, load VPN configuration files and diagnose the VPN tunnel in the tunnel overview.

The "Manage users and groups" dialog provides privileged users with the option of creating configurations for non-privileged users that automatically become active when this user logs on in Windows. This means that non-privileged users can also use VPN tunnel connections.

Privileged users also have the option of putting users together to form groups to then be able to create the VPN group configurations for these groups. This can reduce the configuration effort.

Non privileged users

Non-privileged users have only restricted rights to the configuration of the SOFTNET Security Client and cannot load VPN configuration files. The rights of non-privileged users include the following:

- Use a VPN tunnel and diagnose its status in the tunnel overview.
- Enable/disable VPN tunnel in the main dialog.
- Activate connections to specified internal nodes in the tunnel overview.
- Making settings for the log console and for the language in the "Settings" dialog
- Accessing the diagnostics information of the "Extended diagnostics" and "Log files" dialogs

"Currently managed configuration" dialog area

This area shows the name and the type of configuration currently being managed. This configuration can be changed in the open dialog.

"VPN group configurations" dialog area

In this area, you specify groups that users can be assigned to. A created group is enabled for management using the "Edit" button and then displayed in the "Currently managed configuration" dialog area. Every change made from now on in SOFTNET Security Client is automatically adopted in this group configuration. When a user of this group logs onto Windows, the group configuration is called up automatically. The number of devices for the associated configuration, as well as the last configuration file loaded is shown for each group.

Note

Changing VPN group configurations

If a user with administrative rights makes changes to a VPN group configuration, the changes also affect all members of this group.

"VPN single configurations" dialog area

This area shows all users who have logged on to Windows at least once and have therefore become recognizable for the SOFTNET Security Client. The management can be enabled for these with the "Edit" button. The configuration is then displayed in the "Currently managed configuration" dialog area. Every change made from now on in SOFTNET Security Client is automatically adopted in this single configuration. When the user logs on to Windows, the single configuration is called up automatically. The number of devices for the associated configuration, as well as the last configuration file loaded is shown for each user.

Under the entry "User accounts unknown to the SOFTNET Security Client", all users are shown that have been created in Windows but that have never logged on.

8.8 Run extended diagnostics - "Extended diagnostics" dialog

Opening extended diagnostics

Select the menu command "Diagnostics" > "Extended Diagnostics..." in the main dialog of the SOFTNET Security Client. As an alternative you can call up diagnostics using the shortcut menu of an entry in the tunnel overview.

In extended diagnostics, you can find out the status of your system in terms of a configured module. This view is intended for diagnostics of your system status and can be helpful if have a query for Customer Support.

- **Module-specific parameters**
  Here, you select the module whose current system status you want to diagnose.
- **Routing settings (module-specific parameters)**
  Here, you can see settings of the module relating to its interfaces and internal nodes/subnets obtained from the configuration.
- **Active Main Modes / Active Quick Modes**
  Here, you can see the active main modes and quick modes in detail as soon as they

have been set up for the selected module on the PG/PC.
This also shows how many main modes or quick modes suitable for the selected module were found on the system.

- **Routing Settings (network settings of the computer)**
  Here, you can see the current routing settings of your computer.
  With the "Show entire Routing Table" option, you can also show the routing settings that were hidden to make the display clearer to read.
- **Assigned IP Addresses**
  Here, a list of the network interfaces known to your computer in conjunction with the configured or assigned IP addresses is displayed.

8.9 Accessing log files - "Log files" dialog

Accessing log files

Select the menu command "Diagnostics" > "Log files" in the main dialog of the SOFTNET Security Client.

In this dialog, you have access to all log files of the SOFTNET Security Client.

You can:

- Update the preview of the message window of the selected log file.
- Have the content of the message window scrolled down automatically.
- Save the log files in a text editor.
- Access the directories where the log files are saved.

You will find the possible functions in the following table:

Function	Description / options
SOFTNET Security Client service: General log file	Information on the starting and exiting the SOFTNET Security Client. The log file, for example, contains information on starting the SOFTNET Security client, on the license check and loading the configuration data. Interaction of the SOFTNET Security client with the user and the security modules: Detect new device, enable/disable existing device, automatic network card discovery, setting up and removing security policies.
SOFTNET Security Client service: Computer configuration	The current status of your system is detected. The contents of this log file are used to diagnose your system status if problems occur. The log file supports customer service when eliminating the problems and includes among other things the firewall configuration, the route and operating system settings of your system and the programs installed on your PC.
SOFTNET Security Client service: VPN tunnel	All log messages in the log console of the tunnel overview: Response times with negative feedback from Ping queries, resolved DNS names.

Function	Description / options
SOFTNET Security Client service: Reachability test	Reachability test of the internal nodes and security modules; response times of the positive and negative feedback from Ping queries.
SOFTNET Security Client GUI: General log file	Information on the starting and exiting the SOFTNET Security Client. The log file contains, for example, information on starting the SOFTNET Security Client, on the license check and on loading the configuration data.
SOFTNET Security Client: SCP	Logging data of the SCP protocol. SCP is used for the tunneled transfer of information about internal nodes between the security modules involved if the internal nodes are not configured statically on these security modules.

8.10 Activate Windows firewall rule - "Windows firewall parameter assignment" dialog

Windows firewall rule for the SOFTNET Security Client service

Select the menu command "Settings" > "Windows firewall parameter assignment" in the main dialog of the SOFTNET Security Client.

In this dialog, you can enable a Windows firewall rule for the SOFTNET Security Client service. This Windows firewall rule allows the SOFTNET Security Client service to receive incoming SCP packets. The SCP protocol is used to transfer information about the internal nodes of security modules tunneled between these security modules if the internal nodes are not configured statically on these security modules.

Note

Note the "Security instructions" and notes on firewall parameter assignment

The SOFTNET Security Client can support you only within certain limits when assigning parameters for the Windows firewall in terms of the secure operation of plants, solutions, machines, devices and/or networks.

Note the "Security instructions" and notes on firewall parameter assignment in the configuration manual and in the online help of the SOFTNET Security Client.

You will find the possible functions in the following table:

Function	Description / options
Parameter of the firewall rule	
Name, program (SOFTNET_Security_Client_Service.exe), description	Descriptive information relating to the SOFTNET Security Client firewall rule

Function	Description / options
Partner IP address, partner port, local IP address, local port, direction, protocol type	The set parameters of the SOFTNET Security Client firewall rule for protocols and ports are displayed grayed out. If you want to change these parameters, you can make the changes with the "Advanced Windows firewall" button.
Profile and interface type	Specify the profiles and interface types for which the SOFTNET Security Client firewall rule will apply.
Global Windows firewall status	Windows firewall profile Using the "Windows Firewall profiles" button, you can enable or disable the Windows firewall of your system. If you have enabled the Windows firewall rule of the SOFTNET Security Client, the Windows firewall must be enabled for the relevant network: The Windows firewall setting must be "active". Advanced Windows firewall With the "Advanced Windows firewall" button, you have access to the incoming rules of the Windows firewall with extended security. If you have enabled the Windows firewall rule of the SOFTNET Security Client, you can adapt the properties of the rule in the incoming rules.

Interaction of the SOFTNET Security Client with firewall software of third-parties.

Basically the use of the SOFTNET Security Client with firewall software of third-parties is possible.. To allow or block the functions of the SOFTNET Security Client, the following parameters must be taken into account in the firewalll:

Protocol	Local port	Partner port	Direction	Function	Comment
UDP	All	500	outgoing	IKE / IPSec	Negotiation of the IKE / IPSec VPN tunnel
UDP	All	4500	outgoing	IKE / IPSec	Negotiation of the IKE / IPSec VPN tunnel Necessary when at least one NAT device is on the VPN tunnel line.
UDP	All	53	outgoing	DNS	Resolution of DNS module names in IP addresses.
ESP	*not applicable*	*not applicable*	both ends	IPSec	User data traffic of the VPN tunnel

UDP	All	3820	Incoming	SCP	Automatic learning of internal nodes of the VPN devices.
ICMP	*not applicable*	*not applicable*	both ends	Reachability test	ICMP packets of the SOFTNET Security Client reachability test.

8.11 SOFTNET Security Client settings - "Settings" dialog

Settings for the SOFTNET Security Client

Select the menu command "Settings" > "SOFTNET Security Client settings" in the main dialog of the SOFTNET Security Client.

In this dialog, you make settings that will be retained after closing and opening the SOFTNET Security Client.

You will find the possible functions in the following table:

Function	**Description / options**
Log console in the tunnel overview	
The following log messages are output in the log console of the tunnel overview: • Negative reachability test (ICMP) • Creation/deletion of main modes (phase 1) • Creation/deletion of quick modes (phase 2) • Download configuration files • Learn internal nodes	Selection of the types of messages displayed in the log console of the tunnel overview.
Number of displayed messages	Number of messages that will be extracted from the log files and displayed in the log console of the tunnel overview.
Log files	
File size	Size of the log file shown with "Diagnostics" > "Log files" for messages about important system events. Since the log data is saved in the file via a ring buffer, use the file size to select how long the log data remains saved in the file.
Message category	Messages about important system events. Messages on warnings, system errors and information are displayed.
Open directory	
• Service log files • GUI log files	All log files are stored in these two directories. The log files of the SOFTNET Security Client GUI are stored separate from the log files of the SOFTNET Security Client service.
Language	

Function	Description / options
Program language	Selection of the language setting of the software user interface (GUI). The selectable languages are German and English. If the language is changed, the SOFTNET Security Client requires a restart.
SCP learning functionality	
Learn internal nodes	If the learning mode is enabled in the configuration of the security modules, you can also use the learning mode in the SOFTNET Security Client. This automatically provides you with the information about the dynamic internal nodes of the security modules. The display box below the check box shows whether the corresponding SSC firewall is active. You can adapt this with the the “Change” button.
Show tunnel overview automatically in the foreground if an internal node changes	When this function is enabled: If a new internal node is detected, the "Tunnel overview" dialog is displayed.
Global reachability test	
• Enabled • Disabled	If you disable this function, the reachability test is disabled globally for all the configurations contained in the SOFTNET Security Client. The disabled reachability test is indicated in the tunnel overview by a gray circle. Advantage of disabling: Disabling has the advantage that no additional packets generate data volume. Disadvantage of disabling: In the tunnel overview, there is no longer a feedback message to indicate whether a tunnel partner can be reached or not.
Waiting time for response	Selectable waiting time for the ping that checks whether a tunnel partner can be reached. **Note** With tunnel connections via slow transmission paths (mobile wireless networks: UMTS, GPRS) select a waiting time of ≥ 1500 ms. On these transmission paths, the run time of the data packets is significantly increased. The "Waiting time for response" therefore directly influences the display of the reachability in the tunnel overview.

Function	Description / options
Run time of the VPN tunnel	
• Permanent • Limited	**Permanent use of the VPN tunnel** The VPN tunnels are enabled when the user logs on to the operating system. When the user logs off from the operating system, the VPN tunnels are disabled. **Time limited use of the VPN tunnel** The VPN tunnels can only be enabled when the user interface of the SOFTNET Security client is running. When you exit the user interface, existing VPN tunnels are terminated.

9 Online functions - diagnostics and logging

For test and monitoring purposes, the security module has diagnostics 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 on a Syslog 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 local buffers 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 in the network to which the events are sent. You specify the events that can be sent in the log settings of 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 open this in offline mode. To do this, select the menu command "Options" > "Log files..." and select the log file to be opened using the "Open..." button. For more detailed information, refer to the following section:

- Overview of the functions in the online dialog (Page 274)

Diagnostics in ghost mode S602 ≥V3.1

After obtaining an IP address from the internal node, the security module has an IP address on the external interface that can differ from the IP address with which the security module was initially configured. Before you can run diagnostics via the external interface, you first need to replace the IP address initially configured for the external interface with the IP address obtained by the security module during runtime from the internal node in the Security Configuration Tool.

Protecting exported log files from unauthorized access

Log files exported from the Security Configuration Tool can contain security related information. You should therefore make sure that these files are protected from unauthorized access. This is particularly important when passing on the files.

9.1 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 9- 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. S	Date and time of day	Date and time setting.
SCA. S	Interface settings	Overview of the settings of the individual interfaces.
SCA. S	Dynamic DNS	Overview of the settings for dynamic DNS
SCA. S	ARP table	Display of the ARP table of the security module.
SCA. S	Logged-on users	Shows the users logged on to the Internet page for user-specific IP rule sets.
~~S602~~ ~~CP 443-1 OPC UA~~	Communications status	Display of the communication status and the internal network nodes of security modules located in the same VPN group as the selected security module.
~~S602~~ ~~PC CP~~ ~~CP 443-1 OPC UA~~	Internal nodes	Display of the internal network nodes of the security module.
CP x43-1 Adv.	Dynamically updated firewall rules	Display of the IP addresses enabled dynamically by HTTP or HTTPS or downloaded later by a user. The IP addresses in this tab can be updated by the following events: • Expansion/modification of the IP access control list • Updating he firewall rules • Dynamic expansions entered by the CP during runtime, for example PROFINET IO devices Since this tab only shows the dynamically updated firewall rules, to gain an overall view of the current firewall status of the module, the firewall rules that were configured offline must also be included.

Function / tab in the online dialog		Meaning
S602 ≥V3.1	Ghost mode	Dialog for the ghost mode of the SCALANCE S602 with information on the IP address of the internal node (identical to the external IP address of the security module) and on IP address changes at the internal node.
S≥V4.0	IP blacklist	Display of the IP addresses that were entered in the blacklist of the firewall.
Logging functions		
	System log	Display of logged system events as well as starting and stopping the display.
	Audit log	Display of logged security events as well as starting and stopping the display.
~~CP 443-1 OPC UA~~	Packet filter log	Display of logged data packets as well as starting and stopping the display.

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 active in the Security Configuration Tool or the module-specific online diagnostics was opened using the shortcut menu.
- For CPs the diagnostics access must be opened in the firewall (TCP 443)

Note

Requirement for online diagnostics in ghost mode S602 ≥V3.1

Online diagnostics is only available in ghost mode if the security module has learnt the IP address of the internal node and has adopted this as its external interface. After this, the security module can be reached via the IP address of the external interface.

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.

Display of the logging status

The current logging status results from the loaded configuration or from the reconfiguration in the online dialog. Possible buffer settings are ring buffers or linear buffers. You can see which setting is currently active as follows:

1. Change the mode using the "View" > "Online" menu command.
2. Select the security 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 buffer setting of the selected security module in the lower part of the tab:

Online settings are not saved in the configuration

Settings that you make in online mode (for example buffer settings for logging functions) are not stored in the configuration on the security module. Following a module restart, the settings from the offline configuration are therefore always effective.

9.2 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 the logging functions can be enabled or disabled in the "Log settings" tab of a selected module; packet filter events must also be selected and activated 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	How it works
Packet filter events (firewall) ~~CP 443-1 OPC UA~~	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 activating or deactivating packet logging.
System events	The system log automatically records system events, for example the start of a process or actions for which a user has not been authenticated correctly using a password. 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 in advanced mode, you can enable local logging for the event classes in the log settings in the module properties 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.

Display of the logging status

Online settings are not saved in the configuration.

9.2.1 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.

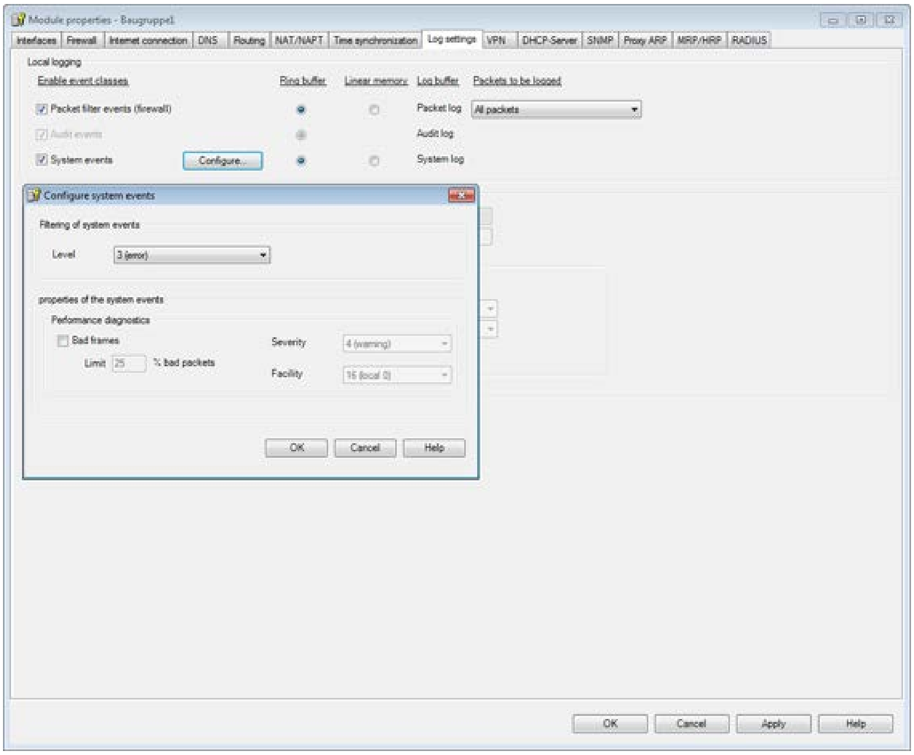
Log settings in standard mode

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:



Local logging

Enable event classes	Ring buffer	Linear memory	Log buffer	Packets to be logged
☑ Packet filter events (firewall)	●	○	Packet log	All packets
☑ Audit events	●		Audit log	
☑ System events	●	○	System log	

Filtering of system events

Level: 3 (error)

properties of the system events

Performance diagnostics

☐ Bad frames

Limit: 25 % bad packets

Severity: 4 (warning)

Facility: 16 (local 0)

Configuring event classes

Table 9- 2 Local log - overview of the functions

Function / tab in the online dialog	Project engineering	Remarks
Packet filter events (firewall) ~~CP 443-1 OPC UA~~	You enable options using the check boxes. You select the storage mode using the check boxes. In the "Packets to be logged" drop-down list, you can specify the data packets to be logged: • "All packets": The data packets that are logged are those to which a configured firewall rule (standard mode or advanced mode) applies. In addition to this, all the response packets to such packets are recorded that have passed the firewall according to a configured allow rule. • "Status generating packets": The only data packets that are logged are those to which a configured firewall rule (standard mode or advanced mode) applies.	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. **Note on CPs:** The audit log data is not retentive on CPs. A syslog server should therefore be used to back up the data.
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. The system events are recorded that have the same priority as the selected filter level and that have a higher priority than the selected filter level. The lower the value of the filter level, the higher its priority and therefore less events are recorded. As default, the following values are set: • SCALANCE S: Level 3 • CP: Level 3	Select "Error" as the filter level or a filter level with a higher priority to prevent recording of general non-critical 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.

9.2.2 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

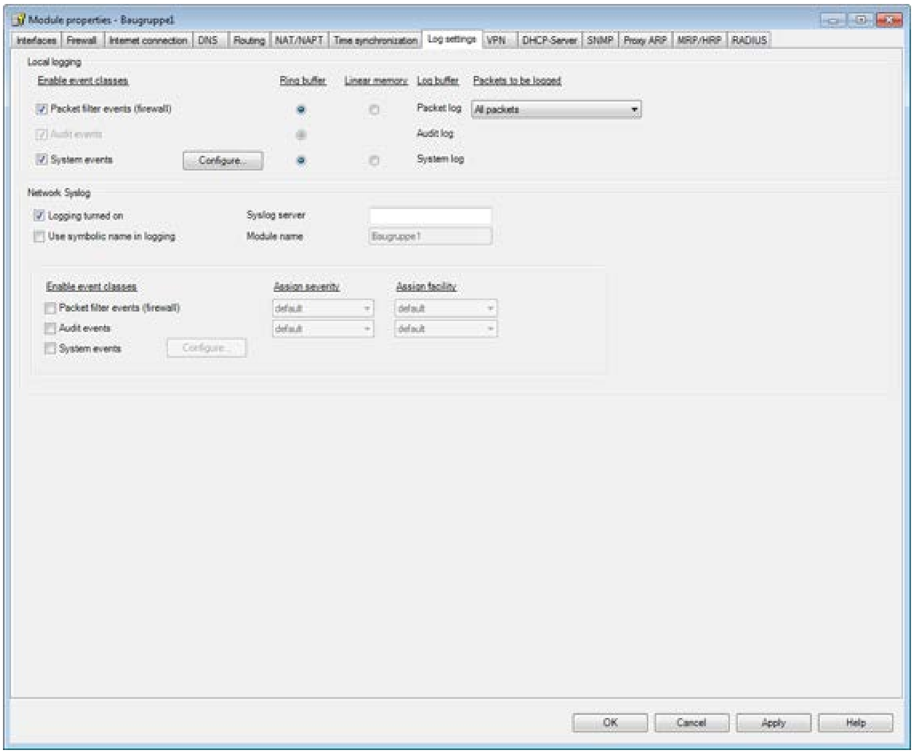
No return to standard mode possible

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 security 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:



Local logging

Enable event classes	Ring buffer	Linear memory	Log buffer	Packets to be logged
☑ Packet filter events (firewall)	●	○	Packet log	All packets
☑ Audit events	●		Audit log	
☑ System events	●	○	System log	

Network Syslog

☑ Logging turned on — Syslog server:

□ Use symbolic name in logging — Module name: Baugruppe1

Enable event classes	Assign severity	Assign facility
□ Packet filter events (firewall)	default	default
□ Audit events	default	default
□ System events		

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 / FQDN 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

~~CP~~

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 frames.

Note

Longer a processing time when using symbolic names

If the "Use symbolic name in logging" check box 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 9- 3 Network Syslog - overview of the functions

Function / tab in the online dialog	Project engineering	Remarks
Packet filter events (firewall) ~~CP 443-1 OPC UA~~	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.

Function / tab in the online dialog	Project engineering	Remarks
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. The system events are recorded that have the same priority as the selected filter level and that have a higher priority than the selected filter level. The lower the value of the filter level, the higher its priority and therefore less events are recorded. As default, the following values are set: • SCALANCE S: Level 3 • CP: Level 3	Select "Error" as the filter level or a filter level with a higher priority to prevent recording of general non-critical 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 recorded by the Syslog server.

9.2.3 Configuring packet logging

~~CP 443-1 OPC UA~~

Configuring logging in standard mode

You will find information on logging IP and MAC rule sets in the following sections:

- SCALANCE S in standard mode (Page 128)
- CPs in standard mode (Page 117)

Note

CP

Relationship between log settings in standard mode and firewall rules

Log settings in standard mode do not affect firewall rules generated automatically during connection configuration. This means, for example, that tunneled frames of a configured connection cannot be logged. In advanced mode, logging can be extended to the automatically generated firewall rules of connections.

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 "Logging" 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 decimal = 11111111.11111111.00000000.00000000 binary

255.255.128.0 decimal = 11111111.11111111.10000000.00000000 binary

255.254.0.0 decimal = 11111111.11111110.00000000.00000000 binary

Incorrect value:

255.255.1.0 decimal = 11111111.11111111.00000001.00000000 binary

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 to 127	255.x.x.x
128 to 191	255.255.x.x
192 to 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 this address range is reserved for other tasks and with some configuration tools (e.g. STEP 7), there is no check of 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 141.30.128.254 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: 141.30.0.254

A.3 MAC address

Note on the structure of the MAC address:

MAC addresses are hardware addresses for identifying network nodes. A MAC address consists of six byes separated by hyphens in hexadecimal notation.

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.

Adapting the MTU (Maximum Transmission Unit)

The MTU specifies the permitted size of a data packet for transmission in the network. When these data packets are then transferred from SCALANCE S via the IPsec tunnel, the original data packet becomes larger as a result of the additional header information and may need to be segmented for further transfer. This depends on the MTU specifications in the connected network. However, a necessary segmentation may lead to noticeable losses in performance or cancelation of the data transfer.

Avoid this by adapting the MTU format, i.e. reducing it in such a way that the data packets received by SCALANCE S can be supplemented by the required additional information without the need for subsequent segmentation. A reasonable size is in the range of between 1000 and 1400 bytes.

References B

B.1 Introduction - without CD/DVD

Finding the SIMATIC NET documentation

- **Catalogs**

  You will find the order numbers for the Siemens products of relevance here in the following catalogs:

  – SIMATIC NET Industrial Communication / Industrial Identification, catalog IK PI

  – SIMATIC Products for Totally Integrated Automation and Micro Automation, catalog ST 70

  You can request the catalogs and additional information from your Siemens representative.

  You can go to the Industry Mall on the Internet at the following address:

  Link to Siemens Industry Mall (http://www.siemens.com/industrymall)

- **Documentation on the Internet**

  You will find SIMATIC NET manuals on the Internet pages of Siemens Automation Customer Support:

  Link to Customer Support (http://support.automation.siemens.com/WW/view/en)

  Go to the required product group and make the following settings:

  "Entry list" tab, Entry type "Manuals / Operating Instructions"

- **Documentation from the STEP 7 installation**

  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" > "All Programs" > "Siemens Automation" > "Documentation").

See also

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

/1/

SIMATIC NET
S7 CPs for Industrial Ethernet
Configuring and Commissioning
Manual Part A - General Applications
Configuration Manual
Siemens AG
30374198 (http://support.automation.siemens.com/WW/view/en/30374198)

/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

/3/

SIMATIC NET
NCM S7 for Industrial Ethernet
Primer
Siemens AG
(part of the online documentation in STEP 7)

/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)

/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

/6/

SIMATIC S7
Siemens AG

- S7-300 automation system
  - CPU 31xC and 31x Installation: Operating Instructions
    Link: 13008499 (http://support.automation.siemens.com/WW/view/en/13008499)
  - Module Data: Reference Manual
    Link: 8859629 (http://support.automation.siemens.com/WW/view/en/8859629)
- Automation system S7-400, M7-400
  - Installation: Installation Manual
    Link: 1117849 (http://support.automation.siemens.com/WW/view/en/1117849)
  - Module Data: Reference Manual
    Link: 1117740 (http://support.automation.siemens.com/WW/view/en/1117740)

B.5 On setting up and operating an Industrial Ethernet network

/7/

SIMATIC NET
Twisted-Pair and Fiber-Optic Networks Manual
Siemens AG
(SIMATIC NET Manual Collection)

B.6 SIMATIC and STEP 7 basics

/8/

SIMATIC
Communication with SIMATIC
system manual
Siemens AG
Entry ID:
25074283 (http://support.automation.siemens.com/WW/view/en/25074283)

/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

/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

/11/

SIMATIC NET
Commissioning PC Stations - Manual and Quick Start
Configuration Manual
Siemens AG
13542666 (http://support.automation.siemens.com/WW/view/en/13542666)

B.9 On configuration of PC CPs

/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

/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)

/14/

SIMATIC NET Industrial Remote Communication
SCALANCE M-800

Configuration Manual
Siemens AG

(SIMATIC NET Manual Collection)

On the Internet under the following entry ID: 78389151

See also

78389151 (http://support.automation.siemens.com/WW/view/en/78389151)

/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

*

*.cer, 236, 257
*.dat, 257
*.p12, 89, 236, 257

3

3DES, 221

A

Access protection, 44
Active nodes, 229
Address of the gateway, 288
Address parameters, 94
Address range, 161
Administrator, 73
Advanced Encryption Standard (AES), 221
Advanced mode, 46
  DHCP server, 193
  Firewall rules, 136
  Global firewall rules, 137
  Local logging, 276, 278
  Logging, 284
  Network Syslog, 276
  User-specific firewall rules, 149
AES, 202, 221
Aggressive mode, 221
Applet, 77
ARP, 211
ARP proxy, 203
Audit events, 277
Authentication, 71
Authentication method, 212, 219
Autocrossover, 102
Automatic firewall rules, 152
Autonegotiation, 102

B

Bandwidth, 156, 166
Bridge mode, 99
Broadcast, 176
Buffer, 277

C

CA certificate, 85, 89
CA group certificate, 89
Certificate, 86, 212
  Exporting, 85
  Importing, 85
  Renewing, 88
  Replace, 89
  Replacing, 89
Certificate manager, 86
Certification authority, 85, 86
CHAP, 103
Configurable properties, 259
Configuration data
  Load, 260
Configuration rights, 76
Configuring time-of-day synchronization, 199
Connection rules, 152
Consistency check, 69, 110, 196
  local, 67
  project-wide, 67
Content area, 94
CP 1628
  Purpose, 41
CP x43-1 Adv.
  Purpose, 38
C-PLUG, 44, 66
Creating a route, 174

D

Data Encryption Standard (DES), 222
Data espionage, 30
DCP (Primary Setup Tool), 170
Dead peer detection (DPD), 230
Default firewall setting
  CP 1628, 123
  CP x43 Adv., 117
Default initialization values, 66
Dependencies of rights, 78
DES, 202, 222
Detect members, 262
Device rights, 76

DHCP
- Server configuration, 193
- Symbolic names, 68

DHCP server, 194
Diagnostics, 273
Diagnostics user, 73
Diffie-Hellman key agreement, 221
DNS conformity, 287

E

Enabling the firewall
- CP 1628, 117
- CP x43-1 Adv., 117
- SCALANCE S V3, 133

Enabling tunneled communication
- CP x43-1 Adv., 117
- SCALANCE S V3, 133

Encryption, 47, 66
ESP protocol, 118, 124, 222
Ethernet non IP frames, 115
Exporting an NTP server, 201
External network nodes
- CP x43-1 Adv., 40
- SCALANCE 602, 29
- SCALANCE S612 / S623 / S627-2M, 32

F

Facility, 282
Firewall, 31
- Advanced mode, 136
- Firewall rules, 115
- Symbolic names, 68

Firewall rule sets
- Global, 62
- User-defined, 149

Firmware version, 3
Flat network, 99
FTP, 77
FTP/FTPS, 59
FTPS certificates, 85
Full duplex, 99

G

Ghost mode, 100
Global firewall rule sets, 164
Global firewall rules, 137
- Assigning, 139

Global packet filter rules, 139
Glossary, 9
Group assignments, 62
Group name, 162, 168

H

Half duplex, 99

I

ICMP, 154
ICMP services, 163
IEEE 802.3, 31, 115
IKE, 118, 124
IKE settings, 219
Installation
- SCALANCE S, 47

Interface routing, 92, 99
Interfaces, 173
Internal network nodes
- Configuring, 242
- CP x43-1 Adv., 40
- SCALANCE 602, 29
- SCALANCE S612 / S623 / S627-2M, 32

Internet Key Exchange (IKE), 221
IP access control list, 77
IP access protection, 59
IP address, 160, 287
IP blacklist, 275
IP packet filter
- local, 154

IP packet filter rules, 155
- CP 1628, 157
- CP x43-1 Adv., 157
- SCALANCE S, 157

IP protocol, 136
IP rule sets, 137
- User-specific, 149

IP services, 162
IPsec settings, 219
IPsec tunnel, 209
ISAKMP, 231
ISO protocol, 245
ISP account, 103

L

Layer 2, 115, 136, 211
Layer 3, 115, 136
Layer 4, 115
Learning mode, 244

Life of certificates, 217
Line Diagnostics, 277, 280, 283
LLDP, 77, 77
Local firewall rules, 116, 137
Local logging, 273, 276, 279
  Audit events, 279
  Packet filter events, 279
  System events, 279
Logging, 116, 273
  CP x43-1 Adv., 117
  Event classes, 282
  SCALANCE S V3, 133

M

M-800, 237
MAC address, 288
MAC packet filter rules, 163, 166
MAC protocol, 136
MAC rule sets, 137
MAC services, 168
Main dialog, 259
Main mode, 221
Maximum time of the session, 72, 75
MD5, 202, 222
Meaning of the symbols, 7
MIB, 77, 77
Module properties, 91
Multicast, 176

N

NAT/NAPT
  Routing, 175
NAT/NAPT router
  Symbolic names, 68
NCP VPN client, 92
  CA group certificate, 241
  Creating a configuration file, 237, 240
  Group certificate, 241
Network cards, 262
Network device, 262
Network ID, 174
Network Syslog, 273, 276
No repercussions, 32
Non IP packets, 211
Non privileged users, 265
NTP
  Symbolic names, 68, 68
NTP (secure), 199
NTP server, 199

O

Offline configuration view, 46
One-shot buffer, 277
Online diagnostics, 276
Online diagnostics view, 46
Overview of the functions
  Module types, 20

P

Packet filter events, 277
PAP, 103
Password, 261
Perfect Forward Secrecy, 222
PING command, 262
Port
  123 (NTP), 176
  443 (HTTPS), 176, 176
  4500 (IPsec), 176
  500 (IPsec), 176
  500 (ISAKMP), 231
  514 (Syslog), 176
Predefined firewall rules
  CP x43-1 Adv., 117, 117
  SCALANCE S V3, 133
Pre-shared keys, 212
Privileged users, 265
Product from other manufacturer, 92
PROFINET, 245
Project
  Initialization values, 66
  Specifying properties, 66
Protocol, 162

R

Range of values for IP address, 287
Remote access user, 73
Renewing the CA group certificate, 229
Ring buffer, 277
Role name, 75
Roles, 73
  System-defined, 73
  User-defined, 74
Root certification authorities, 87
Router IP address, 174
Routing mode, 99, 173
  Enable, 173

S

SA lifetime, 222
SCALANCE M
- Certification authority, 236
- Creating a configuration file, 235
- Group certificate, 236

SCALANCE M875, 237
SCALANCE S
- Creating a module, 91
- Operating systems supported, 47

SCALANCE S product DVD, 48
SCALANCE S602
- Purpose, 27

SCALANCE S612
- Purpose, 30

SCALANCE S623
- Purpose, 30

SCALANCE S627-2M
- Purpose, 30

Security Configuration Tool, 44, 45, 46
- in STEP 7, 46, 56
- Installation, 48
- Installation of CP x34-1 Adv., 48
- Installation of the CP 1628, 48
- Operating modes, 46
- Standalone, 46, 55

Security settings, 255
Service group, 170
Settings
- Project wide, 62

Severity, 282
SHA1, 202, 222
SiClock, 170
SIMATIC NET glossary, 9
SNMP, 77, 77
SNMPv1, 202
SNMPv3, 202
SOFTNET Security Client
- Configuring in the project, 256
- Creating a configuration file, 256
- Database, 257
- Operating systems supported, 255
- Purpose, 26
- Startup behavior, 256
- Uninstalling, 256

Specified connections, 57, 115
Standard mode, 46
- Firewall, 116
- Local logging, 276
- Logging, 283

Standard router, 94, 174
Standard user, 73
Stateful packet inspection, 115
Status information, 263
STEP 7, 56
- Migrated data, 57
- Object properties, 57
- User migration, 70

Subnet mask, 94, 287
Supported operating systems
- SCALANCE S, 47
- SOFTNET Security Client, 255

Symbolic names, 67, 282
Symbols, 7
Syslog
- Audit events, 282
- Packet filter events, 282
- Symbolic names, 68
- Syslog server, 64, 273, 280
- System events, 283

System events, 277
System-defined role
- Administrator, 73
- diagnostics, 73
- Remote access, 73
- standard, 73

T

TCP, 154, 162
Time-of-day synchronization, 199
Tunnel, 209, 260
- Configure, 261
- Tunnel connections, 260

Tunnel functionality, 209

U

UDP, 154, 162
Unspecified connections, 58
Update firmware, 79
User
- Assigning roles, 76
- Creating roles, 73
- Non-privileged, 265
- Privileged, 265
- Setting up, 72

User management, 62, 70
User name, 72
User permissions, 76
User-defined roles, 74

User-specific firewall rules, 149
- Remote access user, 73
- Timeout parameters, 151

User-specific IP rule sets, 150

V

VLAN operation, 212
VLAN tagging, 212
VPN, 26, 209
- Module-specific properties, 230
- SOFTNET Security Client, 253

VPN device, 92
- Module certificate, 239

VPN group, 216

W

WAN IP address
- Specifying, 231