SIEMENS

SIMATIC NET

Industrial Ethernet Security Setting up security

Getting Started

05/2016

C79000-G8976-C287-05

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-C287-05
℗ 03/2016 Subject to change

Table of contents

Preface

1

Getting results fast with Getting Started

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

Working through the Getting Started, you will be able to implement the basic functions of the security modules and the SOFTNET Security Client based on various security examples.

IP settings for the Examples

Note

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

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

This Getting Started applies to the following:

Configuration software:

- STEP 7 Classic V5.5 as of SP2 Hotfix 1
- Security Configuration Tool (SCT) as of V4.1

Products:

- SCALANCE S602, article number: 6GK5 602-0BA10-2AA3
- SCALANCE S612, article number: 6GK5 612-0BA10-2AA3
- SCALANCE S623, article number: 6GK5 623-0BA10-2AA3
- SCALANCE S627-2M, article number: 6GK5 627-2BA10-2AA3
- SOFTNET Security Client as of V5.0, article number: 6GK1 704-1VW05-0AA0
- CP 343-1 Advanced GX31 as of V3.0, article number: 6GK7 343-1GX31-0XE0
- CP 443-1 Advanced GX30 as of V3.0, article number: 6GK7 443-1GX30-0XE0
- CP 1628, article number: 6GK1162-8AA00
- SCALANCE M875, article number: 6GK5 875-0AA10-1AA2

General terminology "security module"

In this documentation, the following products are grouped together under the term "security module":
CP 343-1 Advanced GX31, CP 443-1 Advanced GX30, CP 1628, SCALANCE S602 V4 / SCALANCE S612 V4 / SCALANCE S623 V 4 / SCALANCE S627-2M V4.

The CPs 343-1 Advanced GX31 and 443-1 Advanced GX30 are simply called "CP x43-1 Adv.".

SCALANCE M875 is called "SCALANCE M".

Use of the terms "interface" and "port"

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

- "External interface": The external port of the SCALANCE S602 / S612 / S623 or an external port of the SCALANCE S627-2M
- "Internal interface": The internal port of the SCALANCE S602 / S612 / S623 or an internal port of the SCALANCE S627-2M
- "DMZ interface": The DMZ port of the SCALANCE S623 / S627-2M

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

IP addresses of the security modules in the configuration examples

When downloading a configuration to a security module, the IP address via which the interface can currently be reached must always be specified. In the configuration examples in this manual, it is assumed that the IP addresses of the configuration are identical to the current IP addresses of the security module.

If you want to know more

You will find further information on the topic of "Industrial Ethernet Security" in the configuration manual "SIMATIC NET Industrial Ethernet Security - Basics and Application". This explains the entire functionality and the Security Configuration Tool configuration software in greater detail.

You will find a current release on the Internet under the following entry ID: 61630777 (http://support.automation.siemens.com/WW/view/en/66644895)

You will find hardware descriptions and installation instructions in the documents relating to the individual modules.

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

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

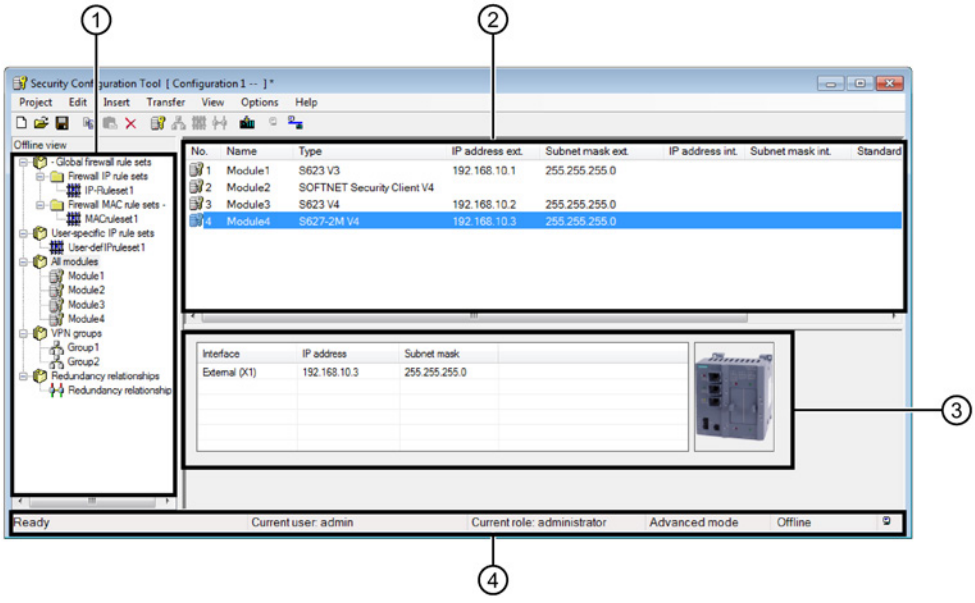
For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit https://support.industry.siemens.com.

User interface and menu commands

2

Structure of the user interface in advanced mode



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 S≥V3.0
- 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.

Symbol	Meaning / remarks
	Create new redundancy relationship. The symbol is only active if you are located in the navigation panel in the "Redundancy relationships" folder.
	 Download the configuration to the selected security modules or create configuration data for SOFTNET Security Client / SCALANCE M / VPN device / NCP VPN client (Android).
	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.	
	New...	Create a new project. For CPs: Projects are created as a result of STEP 7 configuration.	
	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
	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.	
	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.	
	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.	

Menu command		Meaning / remarks	Keyboard shortcut
Insert ▸…		Menu commands only in offline mode	
	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 ▸…			
	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.	
	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.	
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 + D

Menu command		Meaning / remarks	Keyboard shortcut
	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.	
	Network adapter...	The SCALANCE S is assigned an IP address via the selected network adapter.	
	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.	

Configuring IP addresses for SCALANCE S623

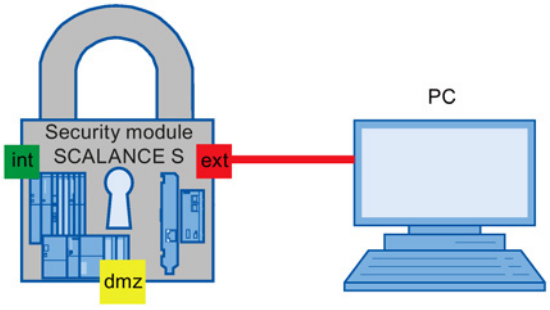
3

3.1 Overview

Overview

In this example, the Security Configuration Tool is used to configure IP addresses for a SCALANCE S623 module which still has the factory settings. The configuration is then downloaded to the security module via the external interface.

Setting up the test network



Required devices/components:

Use the following components to set up the network:

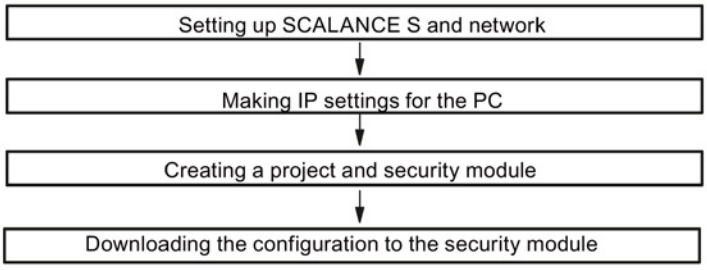
- 1 x SCALANCE S623 module, (additional option: a suitably installed DIN rail with fittings)
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC on which the "Security Configuration Tool" is installed
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

Requirement

To be able to work through this example, the following requirements must be met:

- The security module has the factory-settings. These settings can be restored by pressing the Reset button on the security module and holding it down for at least 5 seconds. For more detailed information on the Reset button of the security module, refer to section "4.3 Reset button - resetting the configuration to the factory defaults" in the manual "SIMATIC NET Industrial Ethernet Security - SCALANCE S V4".

Overview of the next steps:



3.2 Set up SCALANCE S and the network

Follow the steps outlined below:

1. First unpack the SCALANCE S623 and check that it is undamaged.
2. Connect the power supply to the SCALANCE S623.

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

WARNING

Use safety extra-low voltage only

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

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

1. Now establish the physical network connection by connecting the external interface of the security module to the PC.
2. Now, turn on the PC.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;
- Interface X3 - DMZ port (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.

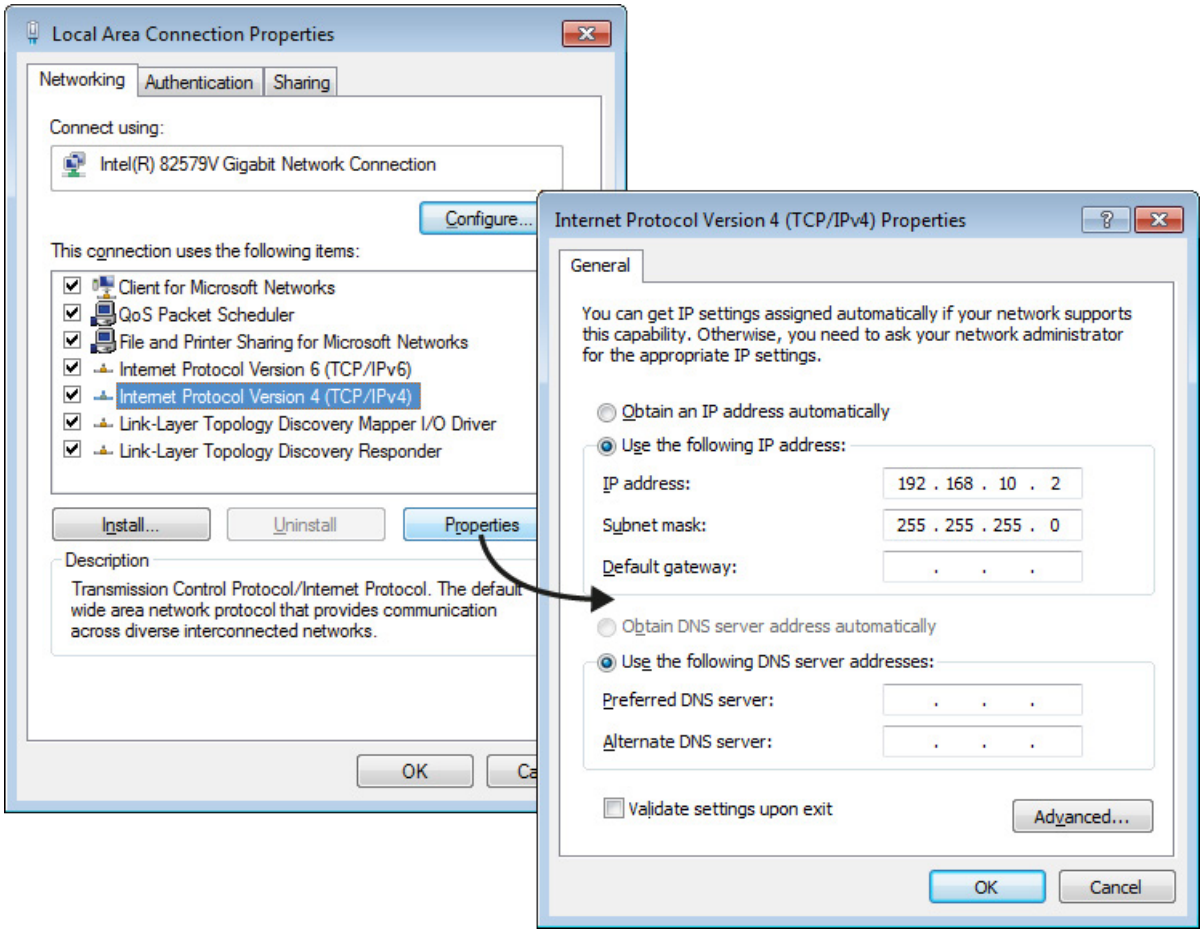
3.3 Making IP settings for the PC

The following IP address settings are made for the PC.

PC	IP address	Subnet mask
PC	192.168.10.2	255.255.255.0

Follow the steps outlined below:

1. On the PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.
5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.



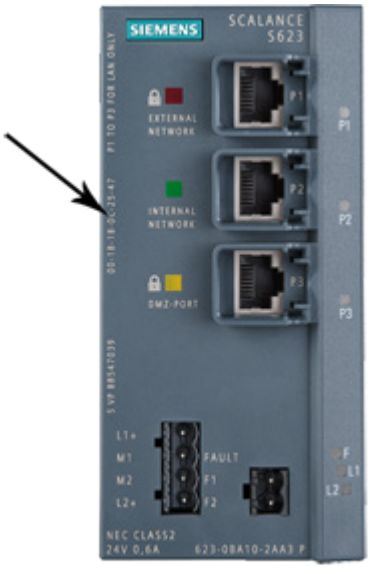
6. Enter the values assigned to the PC from the table "Making IP settings for the PC" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

3.4 Creating a project and security module

Follow the steps below:

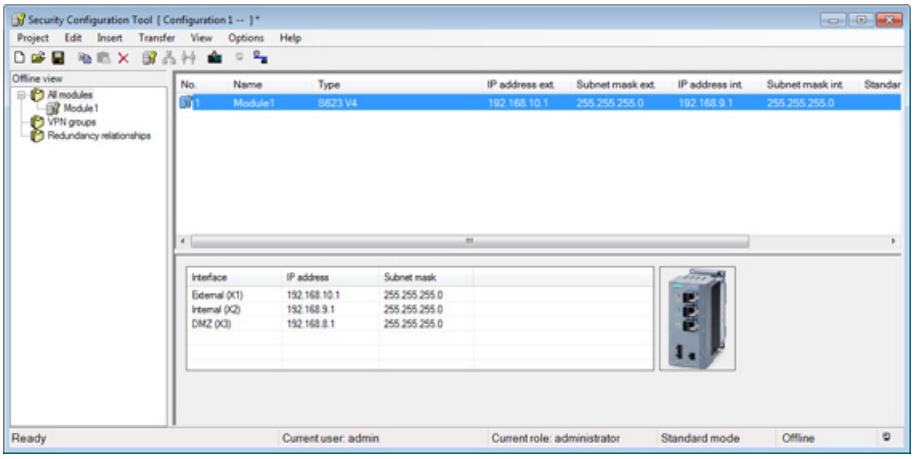
1. Install the Security Configuration Tool on the PC.
2. Start the configuration software.
3. Select the "Project" > "New..." menu command.
4. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
5. Confirm your entries with "OK".

   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.
6. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module: S623
   - Firmware release: V4
7. In the "Configuration" area, enter the MAC address in the required format. The MAC address is printed on the front of the SCALANCE S module (see figure).



8. In the "Configuration" area, enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0).

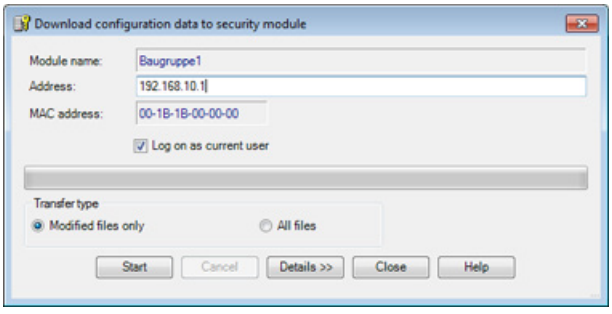
9. From the drop-down list "Interface routing external/internal", select the "Routing mode".
10. Enter the internal IP address (192.168.9.1) and the internal subnet mask (255.255.255.0) and confirm the dialog with "OK".
11. Select the security module you have created and select the "Edit" > "Properties" menu command, "Interfaces" tab.
12. Select the "Activate interface" check box in the "DMZ port (X3)" area and enter the IP address (192.168.8.1) and the subnet mask (255.255.255.0) for the DMZ interface.
13. Confirm with "OK".



3.5 Downloading the configuration to the security module

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Select the security module in the content area.
3. Select the "Transfer" > "To module(s)..." menu command.



4. Start the download with the "Start" button.

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

Result: SCALANCE S in productive operation

The SCALANCE S is now in productive operation. This mode is indicated by the Fault display being lit green. You can now download configurations via all interfaces and modify the configured IP addresses, if required.

Firewall in standard mode

4

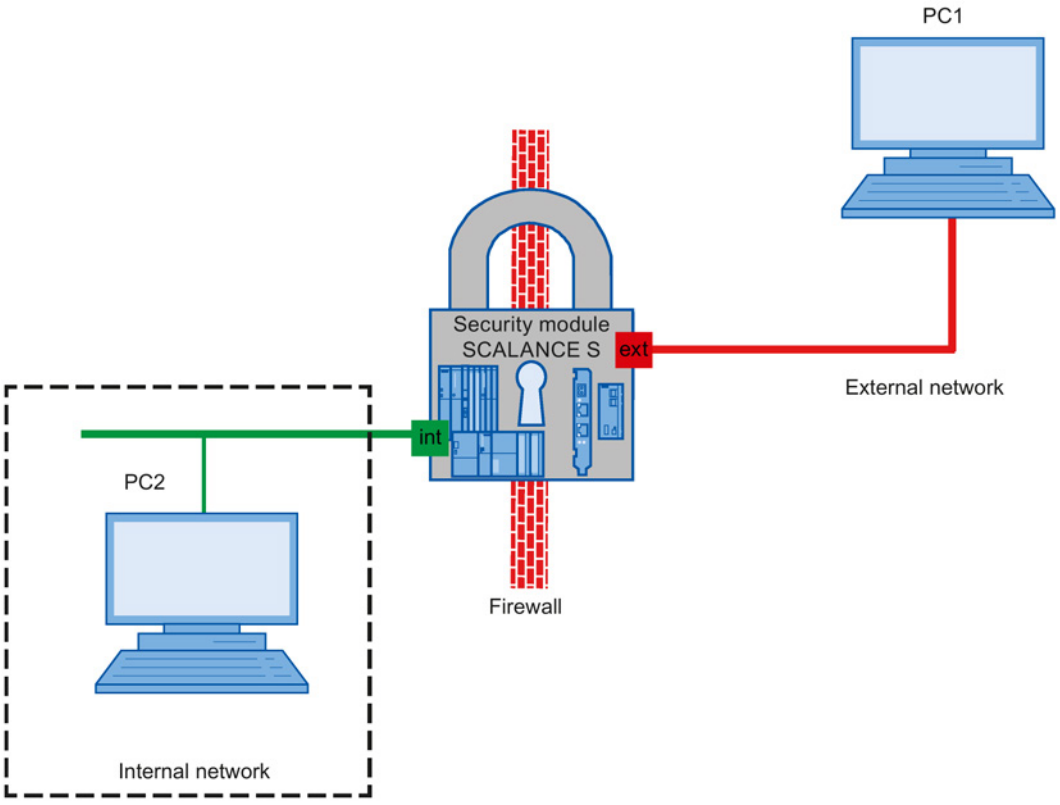
4.1 Example with a SCALANCE S

4.1.1 Overview

In this example, you configure the firewall in the "standard mode" project engineering view. The standard mode includes predefined rules for data traffic.

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

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the security module.

  – PC2: Represents a node in the internal network

- Security module: SCALANCE S module for protection of the internal network
- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

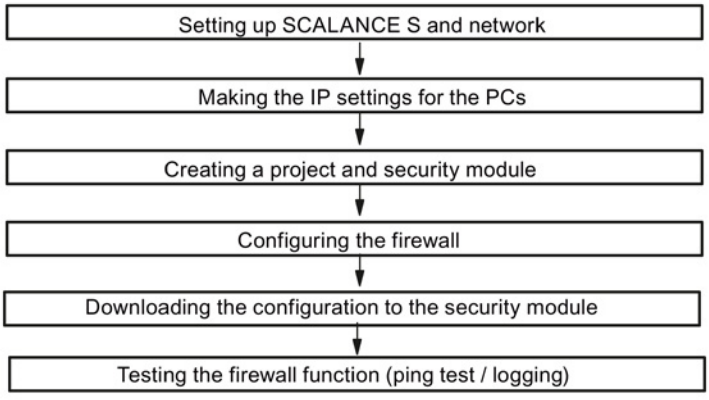
  – PC1: PC with the Security Configuration Tool

Required devices/components:

Use the following components to set up the network:

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

Overview of the next steps:



4.1.2 Set up SCALANCE S and the network

Follow the steps below:

1. First unpack the SCALANCE S and check that it is undamaged.
2. Connect the power supply to the SCALANCE S.

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

⚠ WARNING

Use safety extra-low voltage only

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

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

1. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   - Connect PC2 to the internal interface of the security module.
   - Connect PC1 to the external interface of the security module.
2. Now turn on the PCs.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;

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

4.1.3 Making the IP settings for the PCs

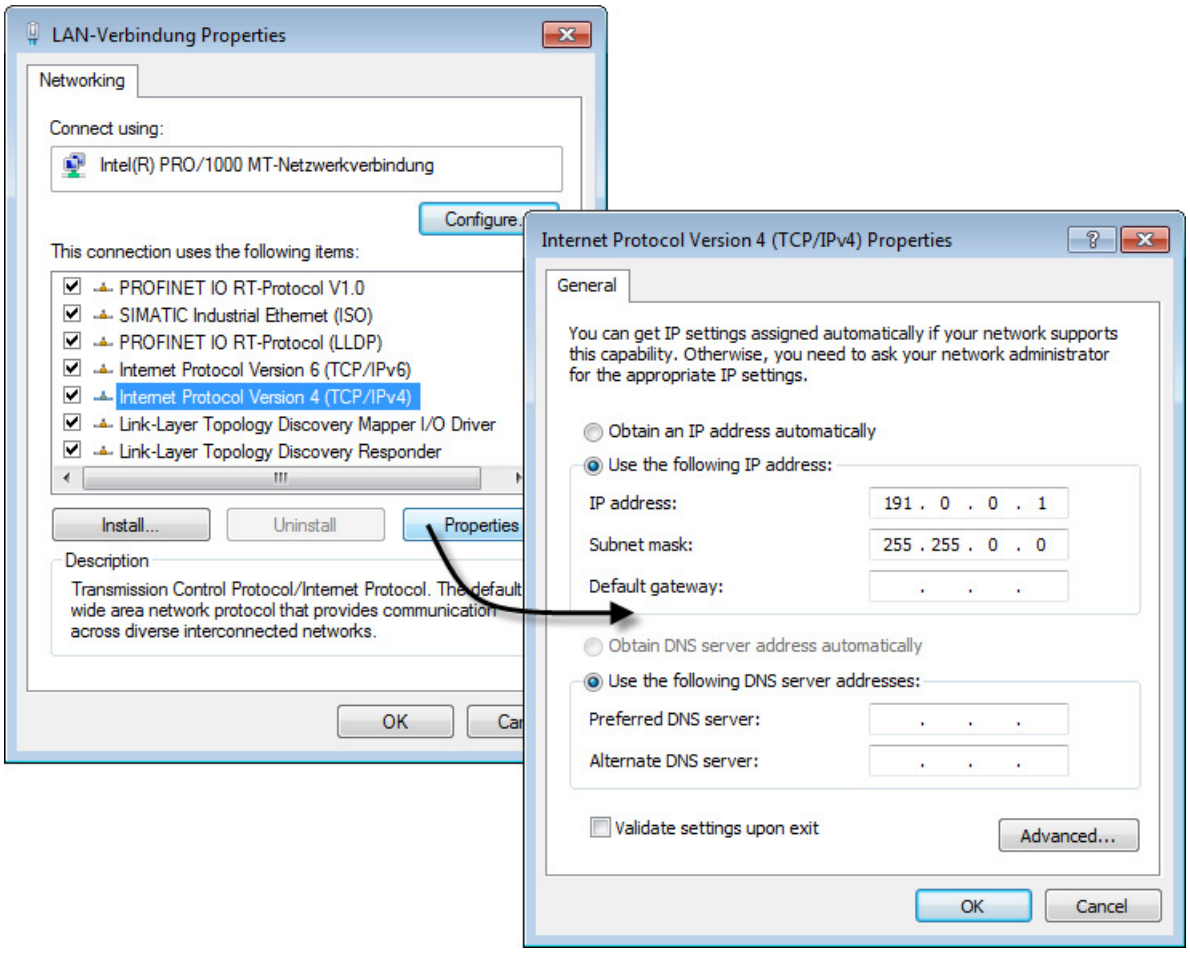
For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask
PC1	191.0.0.1	255.255.0.0
PC2	191.0.0.2	255.255.0.0

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button.
6. Now enter the values assigned to the PC from the table "Making the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

4.1.4 Creating a project and security module

Follow the steps below:

1. Install and start the Security Configuration Tool on PC1.
2. Select the "Project" > "New..." menu command.
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.

4. Confirm your entries with "OK".

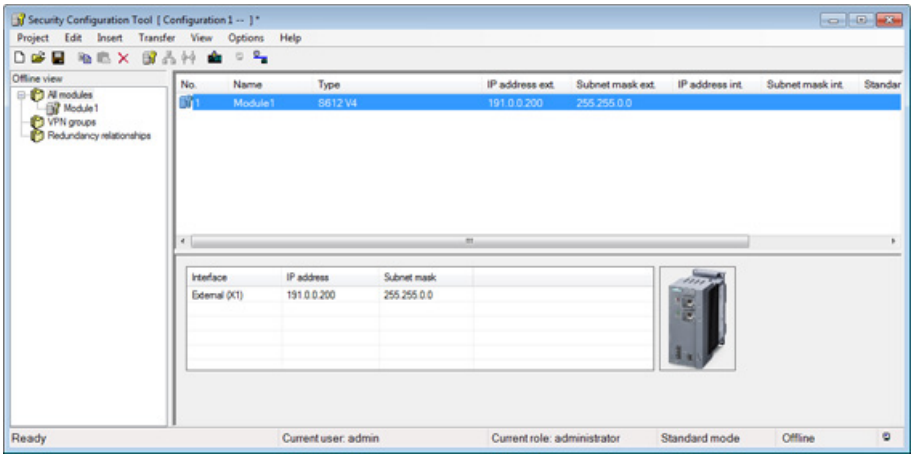
   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.

5. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module: S612
   - Firmware release: V4

6. In the "Configuration" area, enter the MAC address in the required format.

   The MAC address is printed on the front of the SCALANCE S module.

7. In the "Configuration" area, enter the external IP address (191.0.0.200) and the external subnet mask (255.255.0.0) in the required format and confirm the dialog with "OK".



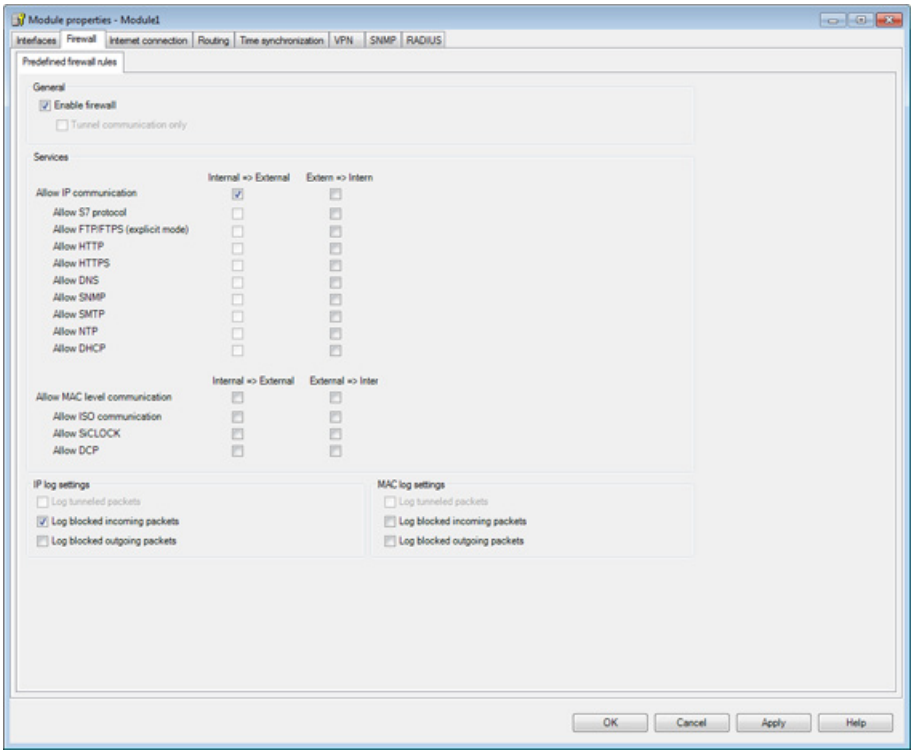
4.1.5 Configure the firewall

In standard mode, the firewall can be set simply with predefined rules. You can activate these rules by clicking on them.

Follow the steps below:

1. Select the security module in the content area.
2. Select the "Edit" > "Properties..." menu command.
3. Select the "Firewall" tab in the displayed dialog.

4. Activate the settings shown below:



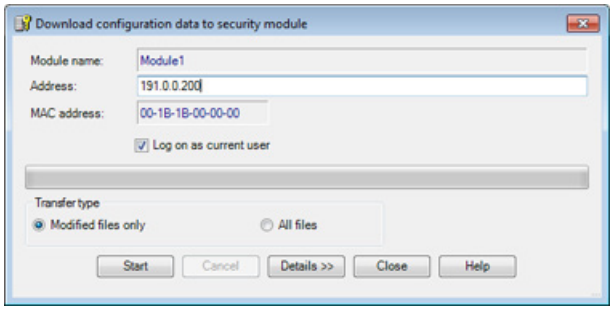
   Result: IP traffic is only initiated from the internal network; only the response is permitted from the external network.

5. You should also select the Logging option to record data traffic.
6. Close the dialog with "OK".
7. Save the project with the "Project" > "Save" menu command.

4.1.6 Downloading the configuration to the security module

Follow the steps below:

1. Select the security module in the content area.
2. Select the "Transfer" > "To module(s)..." menu command.



3. Start the download with the "Start" button.

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

Result: SCALANCE S in productive operation

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

Commissioning the configuration is now complete and the SCALANCE S is now protecting the internal network (PC2) with the firewall.

4.1.7 Test the firewall function (ping test)

How can you test the configured function?

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

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

Note

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

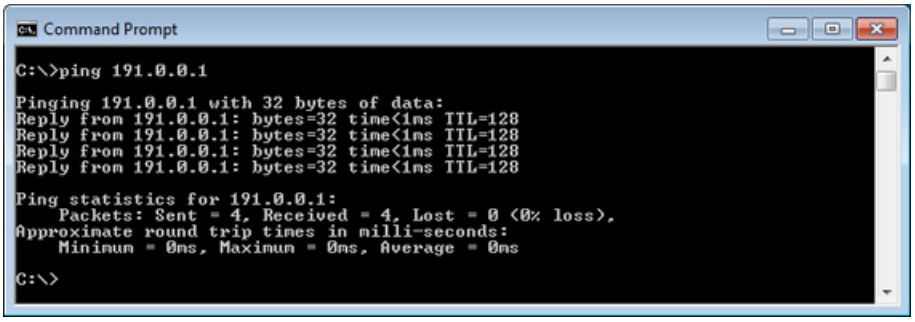
Test phase 1

Now test the function of the firewall configuration, first with allowed IP data traffic initiated in the internal network as follows:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the Ping command from PC2 to PC1 (IP address 191.0.0.1)

   In the command line of the "Command Prompt" window, enter the command "ping 191.0.0.1" at the cursor position.

   You will then receive the following message (positive reply from PC1):



Result

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

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

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

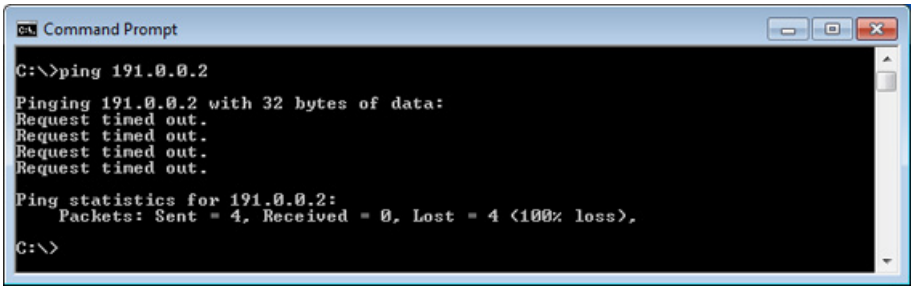
Test phase 2

Now test the function of the firewall configuration, for the blocked IP data traffic initiated in the external network as follows:

1. On PC1, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the Ping command from PC1 to PC2 (IP address 191.0.0.2)

   In the command line of the "Command Prompt" window, enter the command "ping 191.0.0.2" at the cursor position.

   You will then receive the following message (no reply from PC2):



Result

The IP packets from PC1 cannot reach PC2 since the data traffic from the "external network" (PC1) to the "internal network" (PC2) is not allowed.

This is shown in the "Ping statistics" for 191.0.0.2 as follows:

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

4.1.8 Log firewall data traffic

On the security modules, the local logging of system and audit events is enabled as default.

While working through this example, you also activated the logging option for the relevant data traffic when configuring the firewall.

You can display the recorded events in online mode.

Follow the steps below:

1. On PC1, change to online mode in the Security Configuration Tool with the "View" > "Online" menu command.
2. Select the "Edit" > "Online diagnostics ..." menu command.
3. Select the "Packet filter log" tab.

4. Click the "Start reading" button.
5. Acknowledge the displayed dialog with "OK".

   Result: The log entries are read from the security module and displayed here.

4.2 Example with a CP x43-1 Advanced

4.2.1 Overview

In this example, you configure the firewall in the "standard mode" project engineering view. The standard mode includes predefined rules for data traffic.

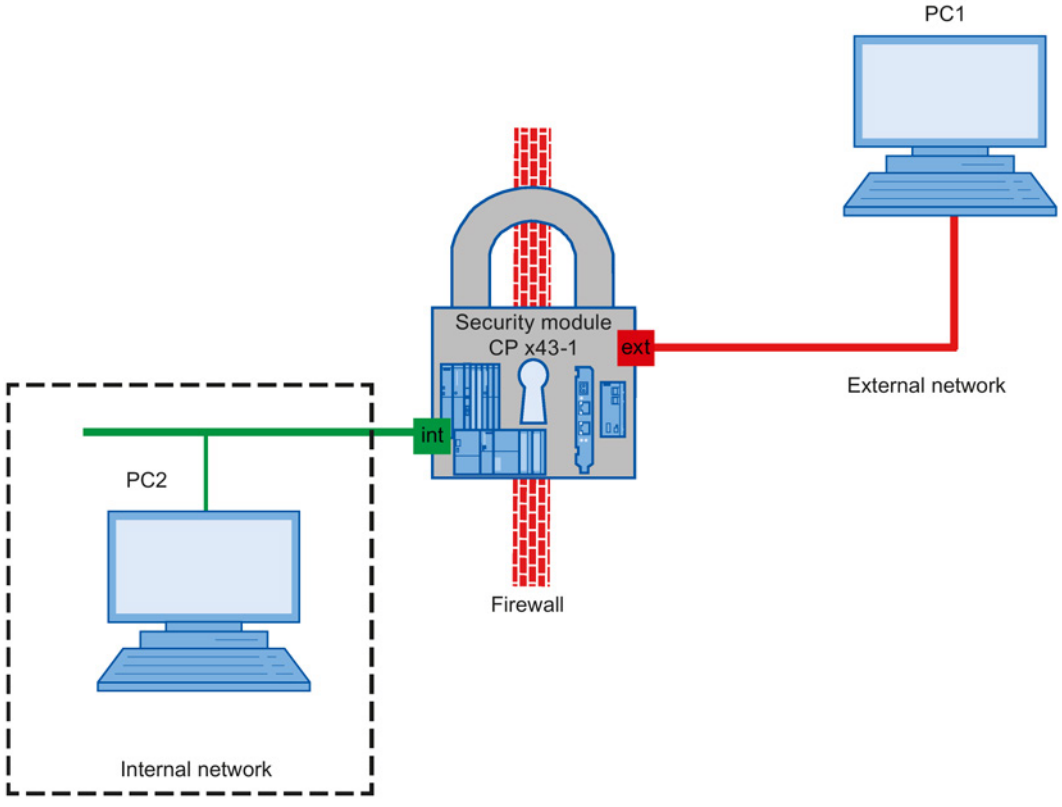
With this configuration, IP traffic can only be initiated from the internal network and from the station; only the response is permitted from the external network.

Note

Please remember that after loading the configuration, your station can only be reached if the S7 protocol (TCP port 102) is allowed from "External => Station" in the firewall. Unencrypted communication from the external network should be avoided following commissioning. If you do not use secure connection establishment from the external network via VPN, you should run STEP 7 diagnostics and reconfigure only from within the internal network.

For this reason, in the following example the port for S7 communication is not open in the firewall.

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the security module.

  – PC2: Represents a node in the internal network
- Security module: CP x43-1 Adv. to protect the internal network
- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

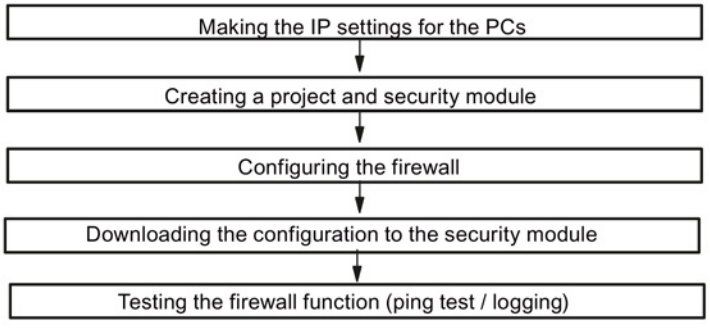
  – PC1: PC with the Security Configuration Tool and STEP 7

Requirement:

To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software is installed on PC1.
- STEP 7 is installed on PC1 and a STEP 7 project with the security module has already been created.
- The IP address of PC1 must be in the same subnet as the gigabit address of the security module.
- CP x43-1 Adv. has the following settings in STEP 7:
  – Gigabit IP address: 140.0.0.1, subnet mask: 255.255.0.0
  – PROFINET IP address: 192.0.0.1, subnet mask: 255.255.255.0

Overview of the next steps:



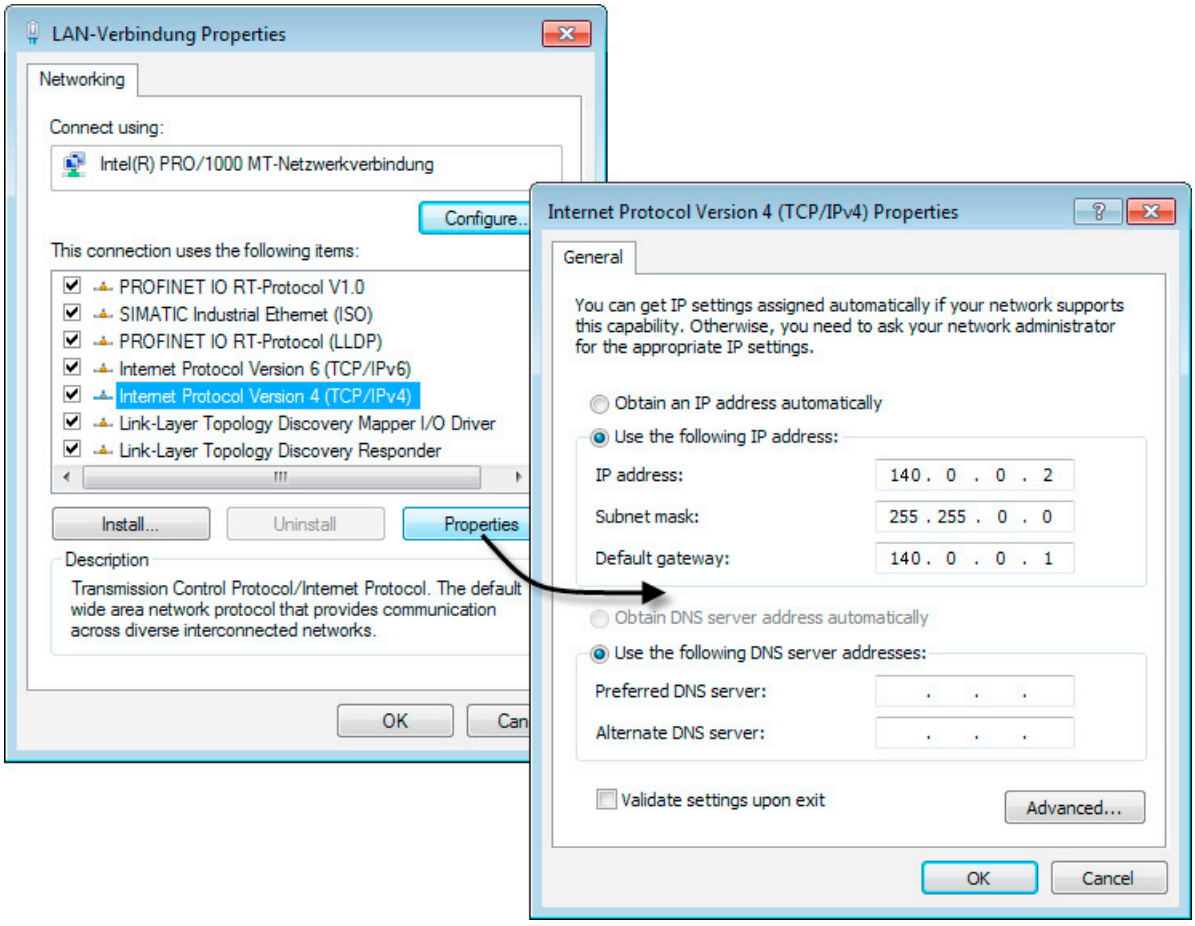
4.2.2 Make the IP settings for the PCs

For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask	Default gateway
PC1	140.0.0.2	255.255.0.0	140.0.0.1
PC2	192.0.0.2	255.255.255.0	192.0.0.1

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Now enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

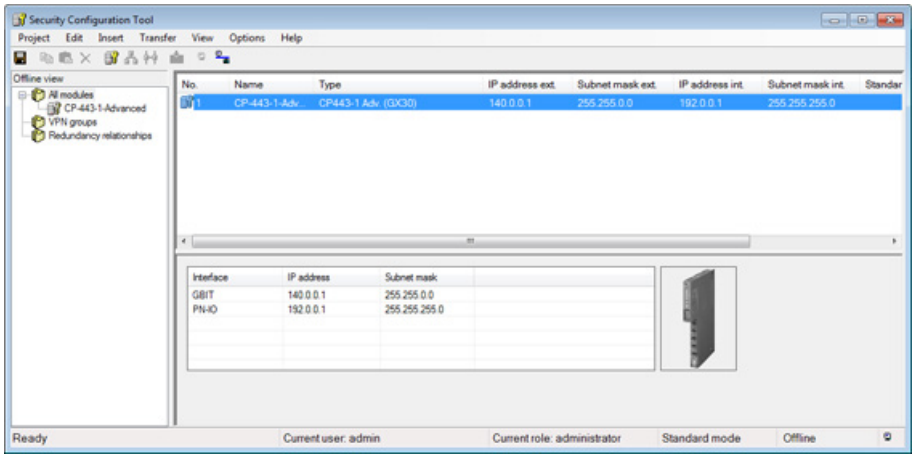
4.2.3 Creating a project and security module

Follow the steps below:

1. In the "Security" tab of the object properties, enable the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new security project is created.
3. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.

Result: The security module will then be displayed in the list of configured modules.



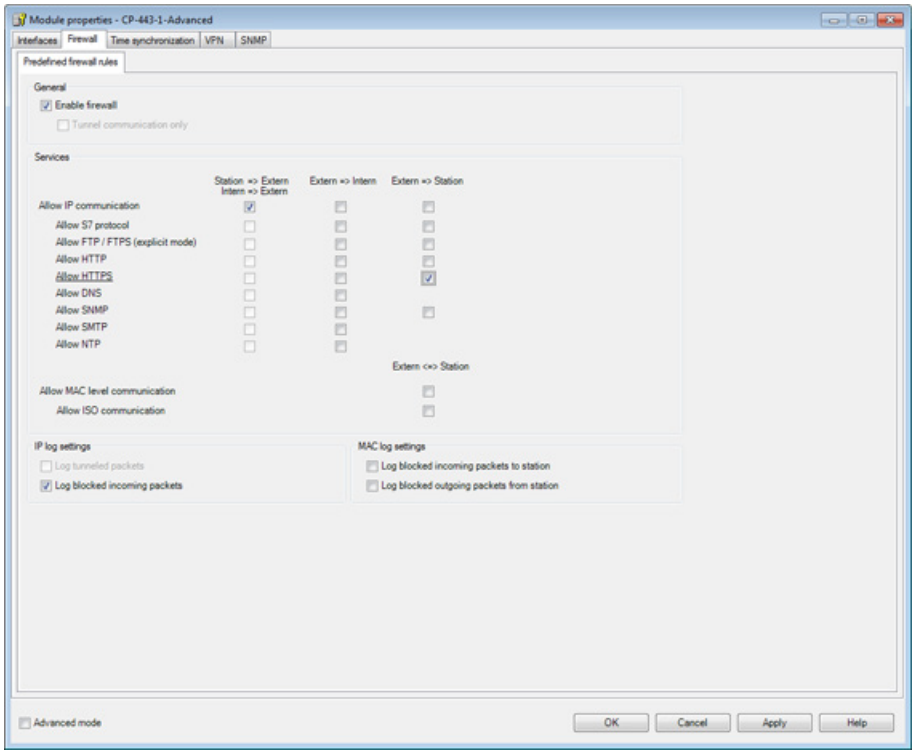
4.2.4 Configure the firewall

In standard mode, the firewall can be set simply with predefined rules. You can activate these rules by clicking on them.

Follow the steps below:

1. Select the security module in the content area.
2. Select the "Edit" > "Properties..." menu command.
3. Select the "Firewall" tab in the displayed dialog.
4. Select the "Enable firewall" check box.

5. Activate the settings shown below:



   Result: IP traffic can only be initiated from the internal network and from the station; only the response is permitted from the external network. Access using HTTPS for online diagnostics from PC1 to the security module is allowed.

6. You should also select the Logging option to record the relevant data traffic.
7. Close the dialog with "OK".

4.2.5 Downloading the configuration to the security module

Follow the steps below:

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu.
3. Download the new configuration to the security module using the "PLC" > "Download to Module ..." menu.

If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.

Result: Security module in productive mode

The commissioning of the configuration is complete. The security module protects the internal network (PC2). Outgoing IP traffic from the internal to the external network is allowed.

4.2.6 Test the firewall function (ping test)

How can you test the configured function?

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

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

Note

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

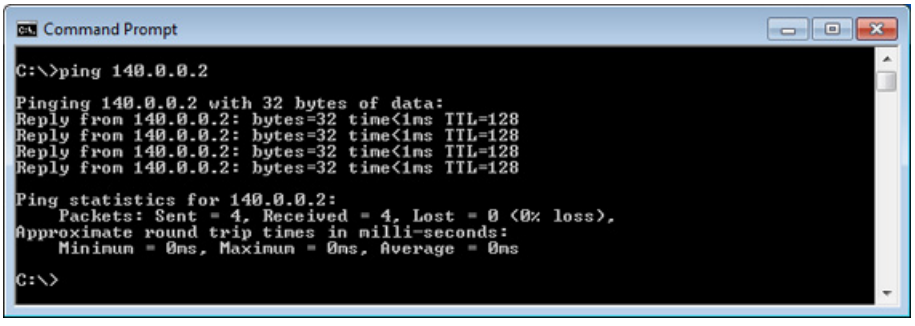
Test phase 1

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

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the Ping command from PC2 to PC1 (IP address 140.0.0.2)

   In the command line of the "Command Prompt" window, enter the command "ping 140.0.0.2" at the cursor position.

   You will then receive the following message (positive reply from PC1):



Result

If the IP packets have reached PC1, the "Ping statistics for 140.0.0.2" display the following:

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

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

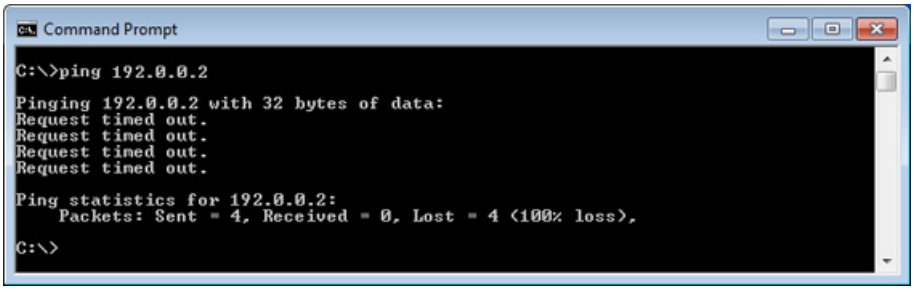
Test phase 2

Now test the function of the firewall configuration, for the blocked IP data traffic initiated in the external network as follows:

1. On PC1, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the Ping command from PC1 to PC2 (IP address 192.0.0.2)

   In the command line of the "Command Prompt" window, enter the command "ping 192.0.0.2" at the cursor position.

   You will then receive the following message (no reply from PC2):



Result

The IP packets from PC1 cannot reach PC2 since the data traffic from the "external network" (PC1) and from the station to the "internal network" (PC2) is not allowed.

This is shown in the "Ping statistics" for 192.0.0.2 as follows:

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

4.2.7 Log firewall data traffic

On the security modules, the local logging of system, audit and packet filter events is enabled as default.

While working through this example, you also activated the logging option for the relevant data traffic when configuring the firewall.

You can display the recorded events in online mode.

Follow the steps below:

1. On PC1, change to online mode in the Security Configuration Tool with the "View" > "Online" menu command.
2. Select the "Edit" > "Online diagnostics ..." menu command.
3. Select the "Packet Filter Log" tab.
4. Click the "Start reading" button.
5. Acknowledge the displayed dialog with "OK".

   Result: The log entries are read from the security module and displayed here.

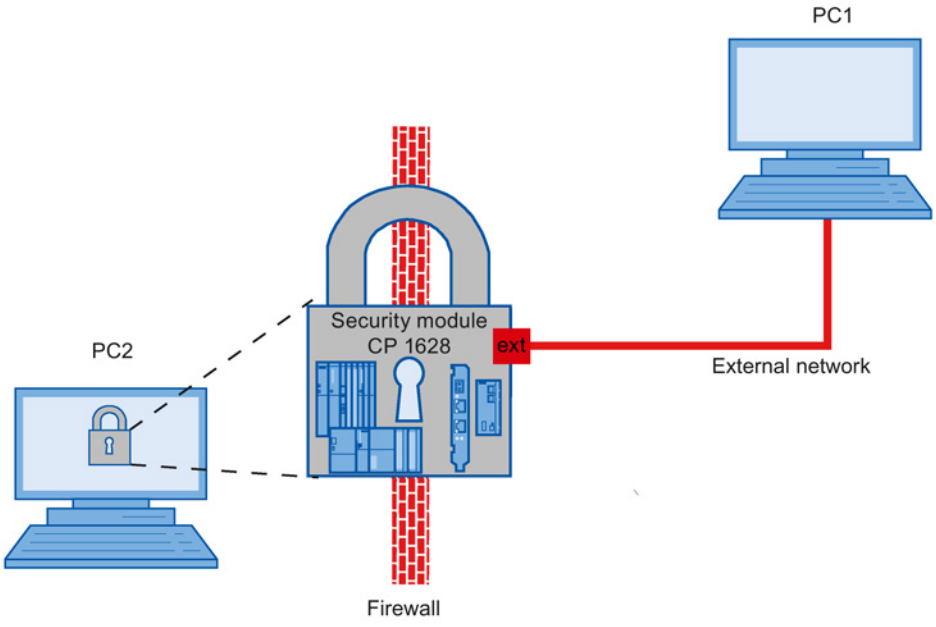
4.3 Example with a CP 1628

4.3.1 Overview

In this example, you configure the firewall in the "standard mode" project engineering view. The standard mode includes predefined rules for data traffic.

With this configuration, IP traffic can only be initiated from PC2; only the response is permitted from the external network.

Setting up the test network



- PC1: PC with the Security Configuration Tool and STEP 7
- PC2 and security module: PC with CP 1628

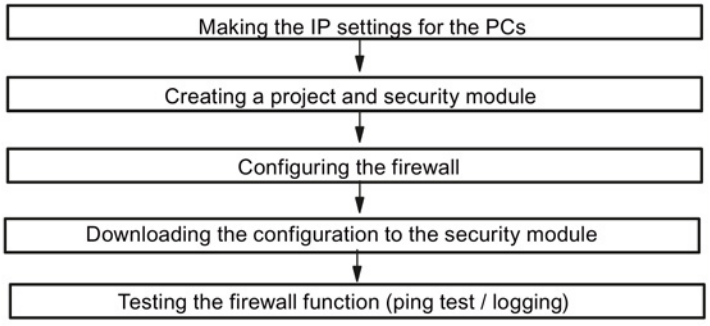
Requirement:

To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software is installed on PC1.
- STEP 7 is installed on PC1 and a STEP 7 project with the security module has already been created.
- PC2 with the CP 1628 has the following settings in STEP 7:
  - IP address Industrial Ethernet: 192.168.0.5, subnet mask: 255.255.255.0

    The NDIS IP address is set up in the IP settings of the PC.

Overview of the next steps:



4.3.2 Make the IP settings for the PCs

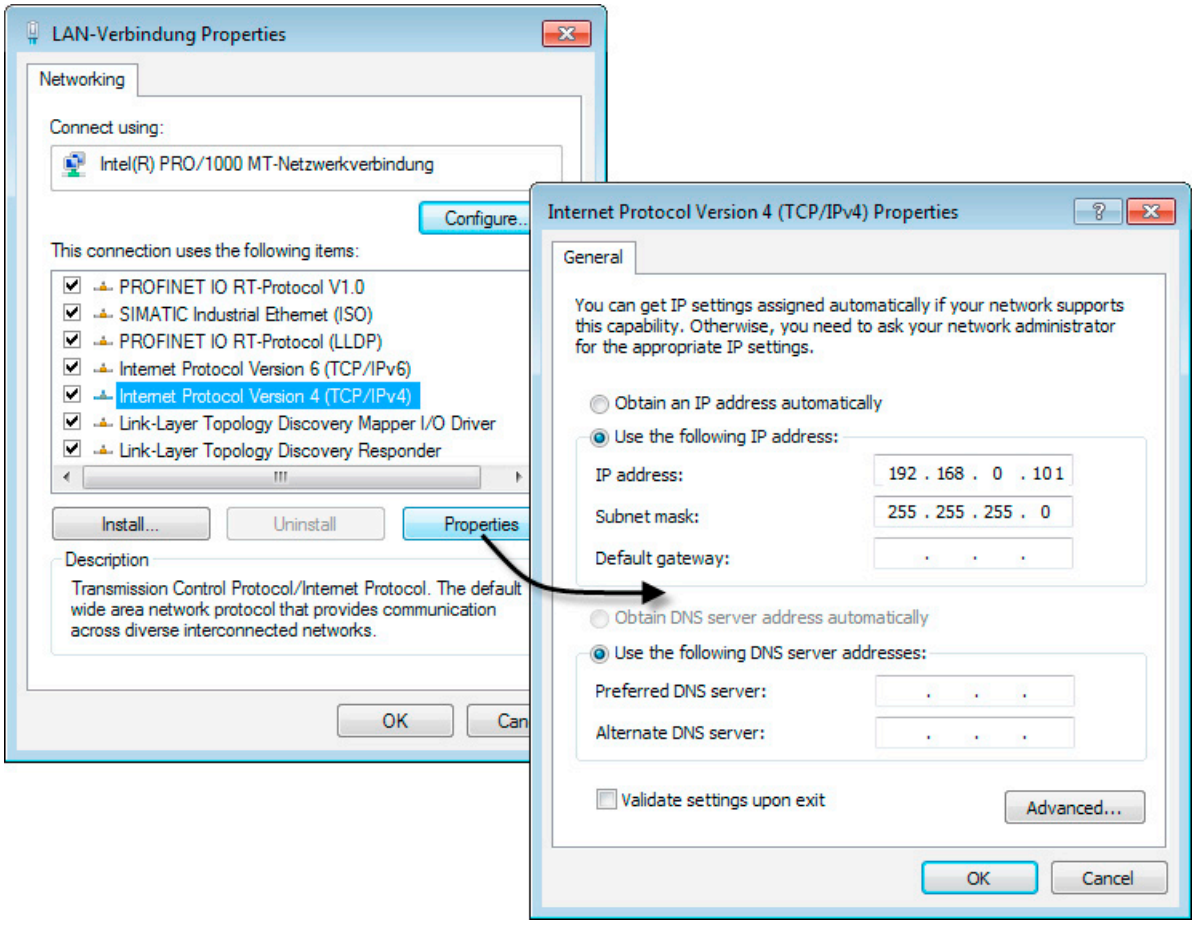
For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask
PC1	192.168.0.101	255.255.255.0
PC2	NDIS: 192.168.0.105	255.255.255.0

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Now enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

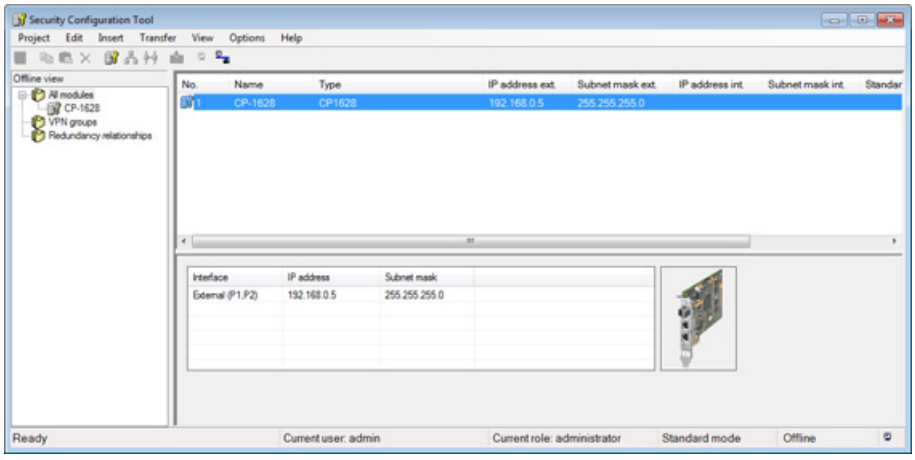
4.3.3 Creating a project and security module

Follow the steps below:

1. In the "Security" tab of the object properties, enable the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new security project is created.
3. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.

Result: The security module will then be displayed in the list of configured modules.



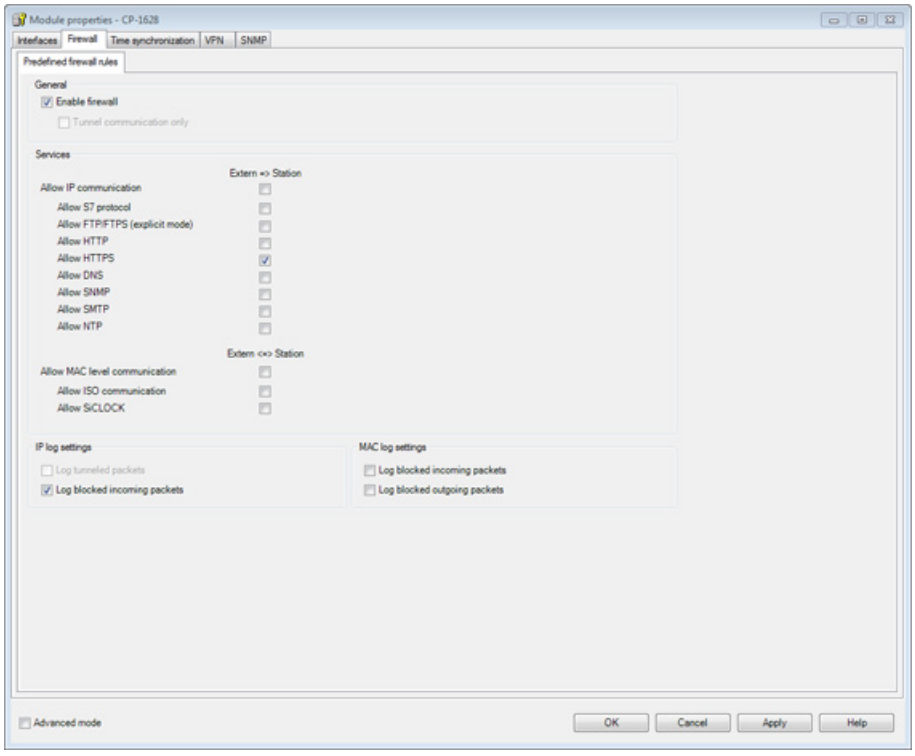
4.3.4 Configure the firewall

In standard mode, the firewall can be set simply with predefined rules. You can activate these rules by clicking on them.

Follow the steps below:

1. Select the security module in the content area.
2. Select the "Edit" > "Properties..." menu command.
3. Select the "Firewall" tab in the displayed dialog.

4. Activate the settings shown below:



   Result: The IP traffic can now be initiated by PC2; only the reply from PC1 is allowed. Access using HTTPS for online diagnostics from PC1 to the security module is allowed.

5. You should also select the Logging option to record data traffic.
6. Close the dialog with "OK".

4.3.5 Downloading the configuration to the security module

Follow the steps below:

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu.
3. Download the new configuration to the security module using the "PLC" > "Download to Module..." menu.

If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.

Result: Security module in productive mode

The commissioning of the configuration is complete. The security module protects PC2. Outgoing IP traffic from PC2 to the external network (PC1) is allowed.

4.3.6 Test the firewall function (ping test)

How can you test the configured function?

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

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

Note

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

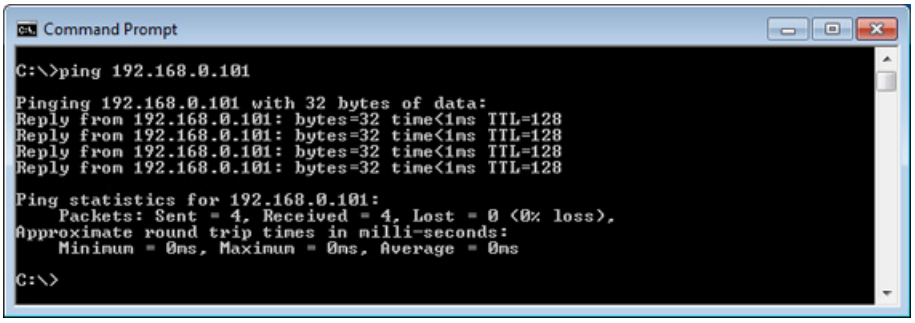
Testing

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

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to PC1 (IP address 192.168.0.101)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.0.101" at the cursor position.

   You will then receive the following message (positive reply from PC1):



Result

If the IP packets have reached PC1, the "Ping statistics" for 192.168.0.101 display the following:

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

Due to the configuration, the ping packets from PC2 can reach PC1. PC1 has replied to the ping frames. Due to the "stateful inspection" function of the firewall, the reply packets arriving from PC1 are automatically allowed to PC2.

4.3.7 Log firewall data traffic

On the security modules, the local logging of system, audit and packet filter events is enabled as default.

While working through this example, you also activated the logging option for the relevant data traffic when configuring the firewall.

You can display the recorded events in online mode.

Follow the steps below:

1. On PC1, change to online mode in the Security Configuration Tool with the "View" > "Online" menu command.
2. Select the "Edit" > "Online diagnostics ..." menu command.
3. Select the "Packet filter log" tab.
4. Click the "Start reading" button.
5. Acknowledge the displayed dialog with "OK".

   Result: The log entries are read from the security module and displayed here.

Firewall in advanced mode

5

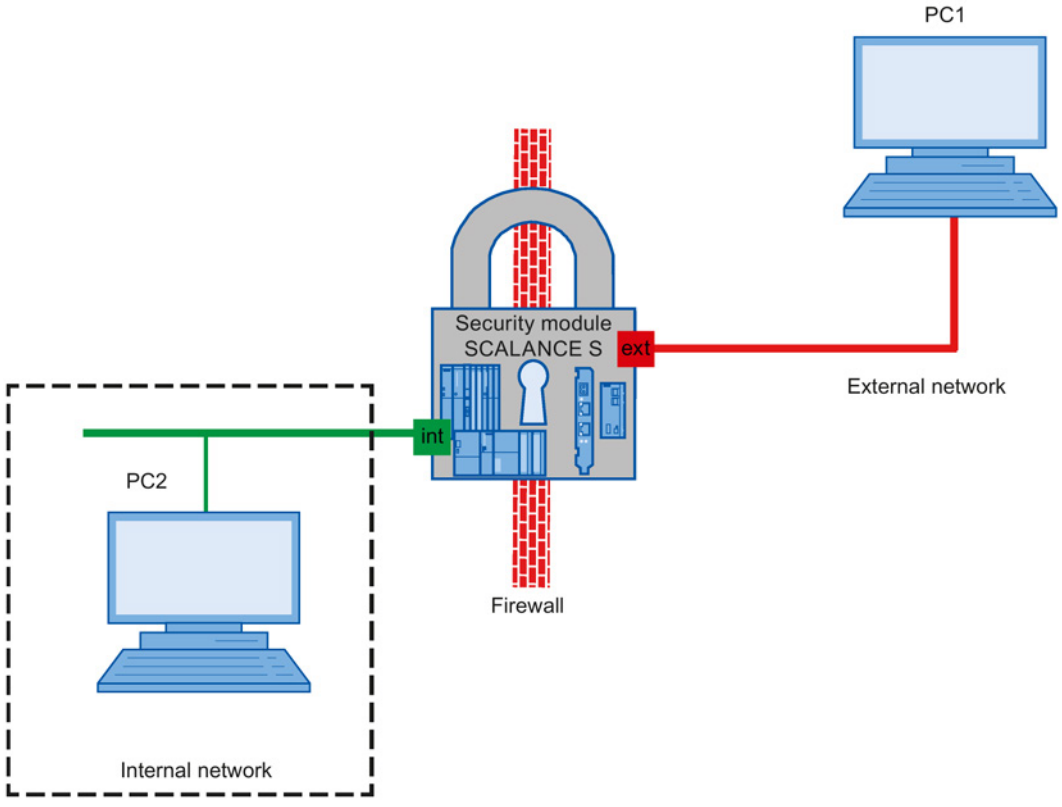
5.1 SCALANCE S as firewall and NAT router

5.1.1 Overview

In this example, you configure the NAT router mode. You configure in the "advanced mode" configuration view.

With this configuration, you have the situation that all the packets sent from the internal subnet to the PC1 node in the external network are allowed to pass the firewall. The packets are forwarded to the outside with an IP address translated to the IP address of the security module and with a dynamically assigned port number. Only the replies to these packets is allowed to pass from the external network.

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the security module.

  – PC2: Represents a node in the internal network
- Security module: SCALANCE S module for protection of the internal network
- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

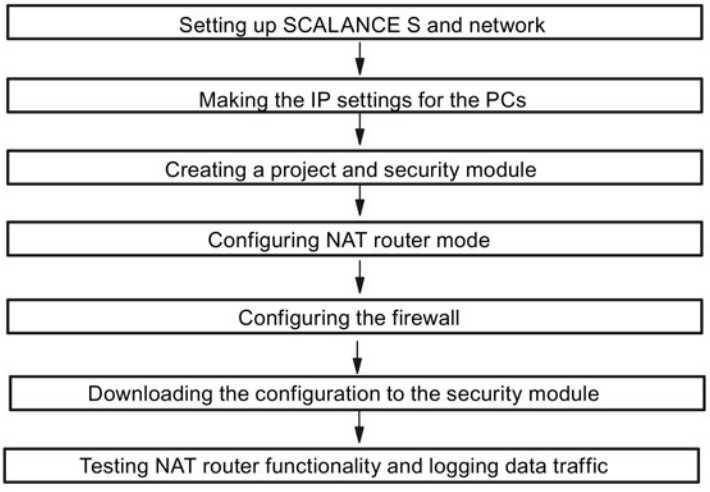
  PC1: PC with the Security Configuration Tool

Required devices/components:

Use the following components to set up the network:

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

Overview of the next steps:



5.1.2 Set up SCALANCE S and the network

Follow the steps below:

1. First unpack the SCALANCE S and check that it is undamaged.
2. Connect the power supply to the SCALANCE S.

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

⚠ WARNING

Use safety extra-low voltage only

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

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

1. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   - Connect PC2 to the internal interface of the security module.
   - Connect PC1 to the external interface of the security module.
2. Now turn on the PCs.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;

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

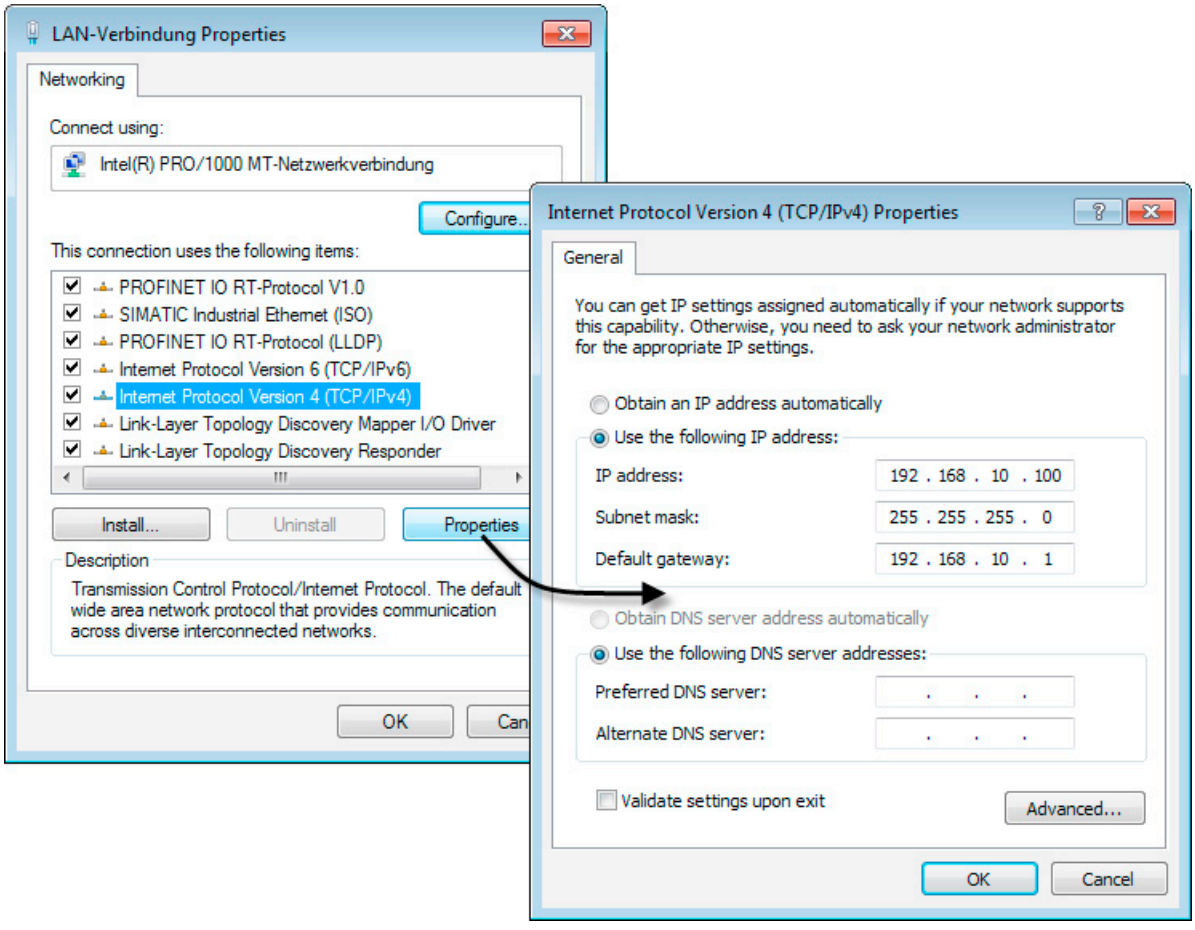
5.1.3 Make the IP settings for the PCs

For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask	Default gateway
PC1	192.168.10.100	255.255.255.0	192.168.10.1
PC2	172.10.10.100	255.255.255.0	172.10.10.1

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.

6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

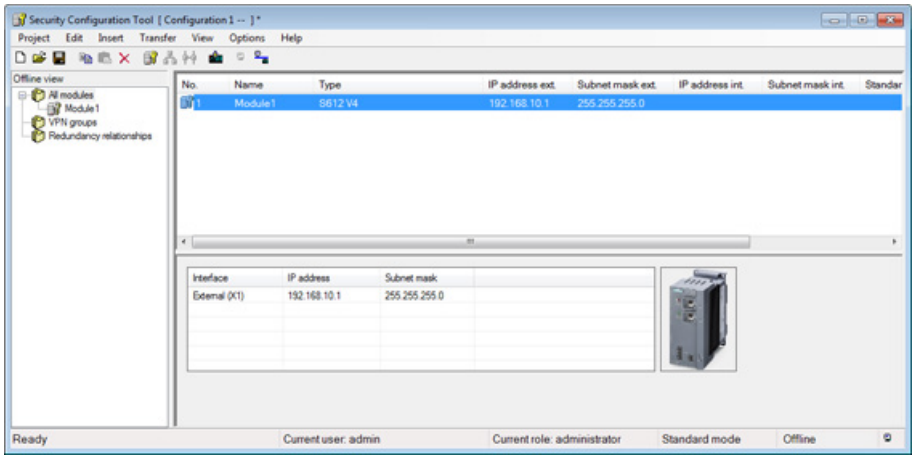
5.1.4 Creating a project and security module

Follow the steps below:

1. Install and start the Security Configuration Tool on PC1.
2. Select the "Project" > "New..." menu command.
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
4. Confirm your entries with "OK".

   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.
5. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module S612
   - Firmware release: V4
6. In the "Configuration" area, enter the MAC address in the required format.

   The MAC address is printed on the front of the SCALANCE S module.
7. In the "Configuration" area, enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0) in the required format and confirm the dialog with "OK".

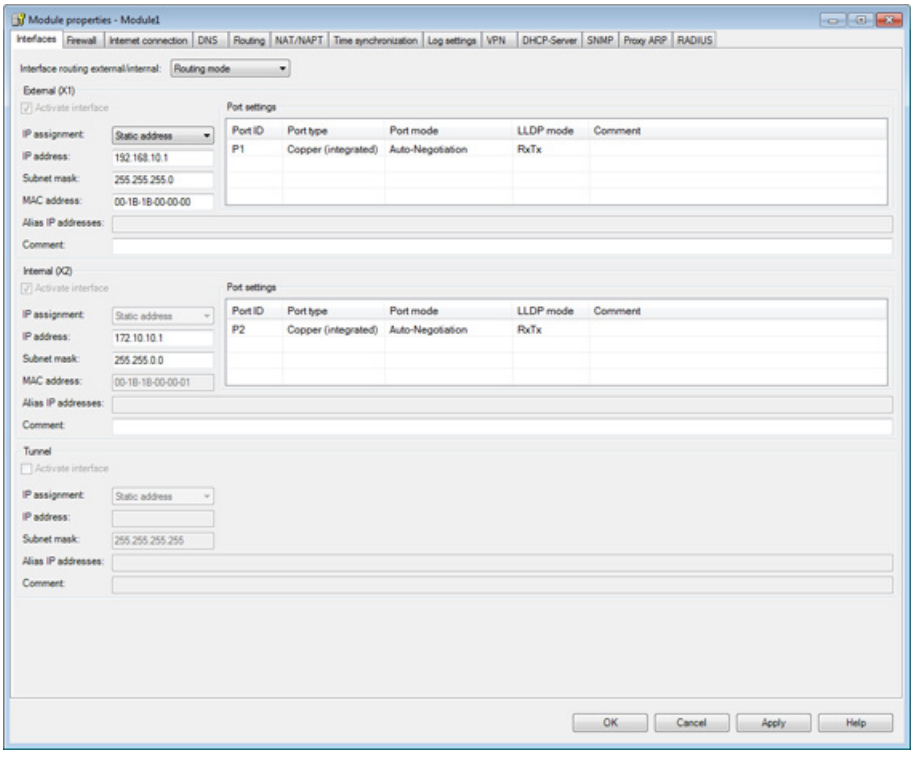


5.1.5 Configuring the NAT router mode

Activating router mode

1. Change the configuration view to advanced mode with the menu command "View" > "Advanced mode".
2. Select the security module in the content area.
3. Select the "Edit" > "Properties..." menu command.

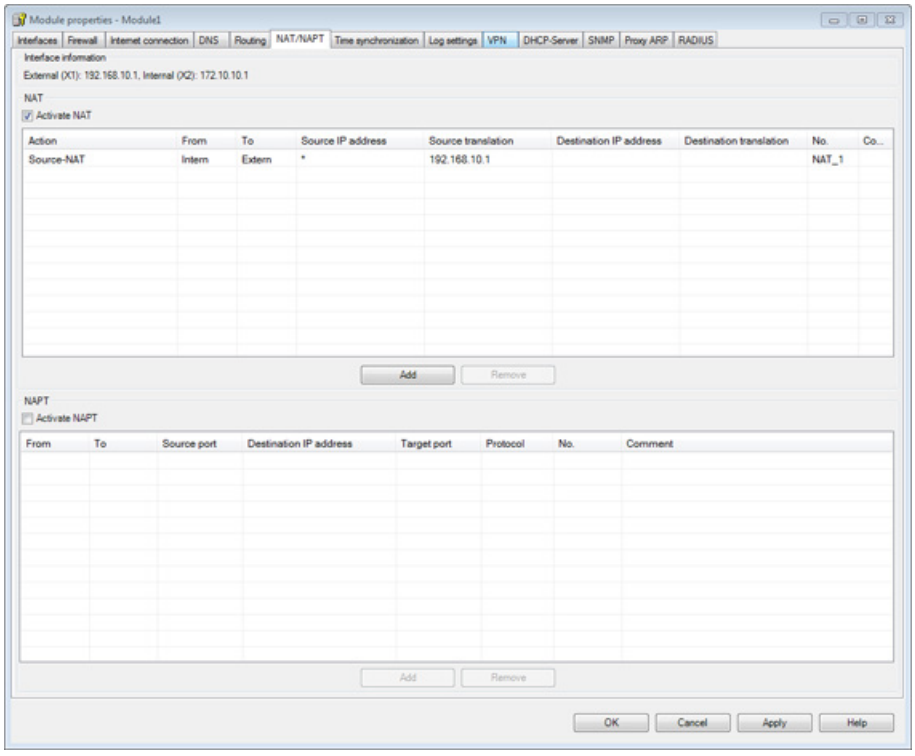
   Result: The "Interfaces" tab is opened.
4. From the drop-down list "Interface routing external/internal", select the "Routing mode".
5. In the "Internal (X2)" input area, you add the address information for the internal interface of the SCALANCE S as follows:
   - IP address: 172.10.10.1
   - Subnet mask: 255.255.255.0
6. Confirm with "Apply".



Activating NAT router mode for internal nodes

1. Select the "NAT/NAPT" tab.
2. Select the "Activate NAT" check box.
3. Click the "Add" button in the "NAT" input area.

4. Configure the NAT rule with the following parameters:
   - Action: "Source NAT"
   - From: "Internal"
   - To: "External"
   - Source IP address: "*"
   - Source translation: "192.168.10.1"
5. Confirm with "Apply".



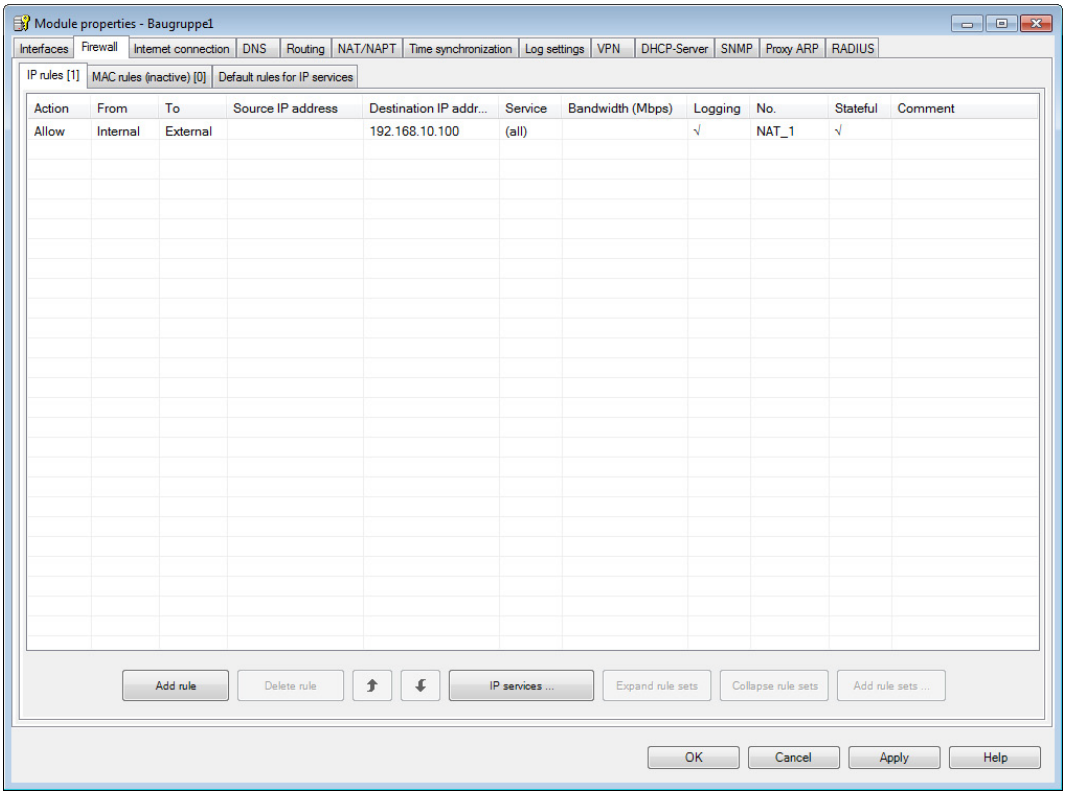
Result: SCT automatically generated a firewall rule that allows communication in the configured address translation direction. In the next step, specify this firewall rule by restricting the permitted destination IP addresses of frames to the IP address of PC1.

5.1.6 Configuring the firewall

Follow the steps below:

1. Select the "Firewall" tab.
2. Expand the firewall rule created by SCT by the following information:
   - Destination IP address: 192.168.10.100
3. In the row of the new rule set, select the "Logging" check box. As a result, packets to which the defined rule is applied are logged.

4. Confirm with "Apply".

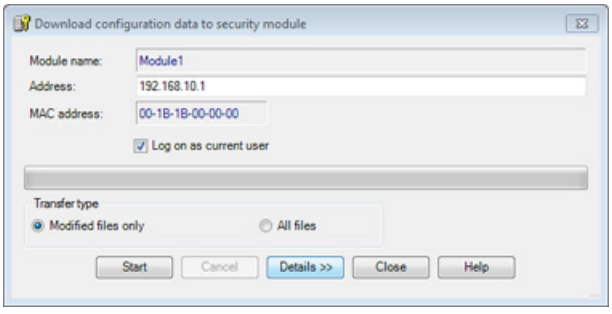


5. Close the dialog with "OK".

5.1.7 Downloading the configuration to the security module

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Select the security module in the content area.
3. Select the "Transfer" > "To module(s)..." menu command.



4. Start the download with the "Start" button.

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

Result: SCALANCE S in productive operation

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

5.1.8 Testing NAT router functionality and logging data traffic

How can you test the configured function?

The function can be tested as described below using a ping command. To be able to recognize the effects of the NAT router mode, use the packet filter logging.

Note on the ping command: As an alternative, you can also use other communication programs to test the configuration.

Note

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

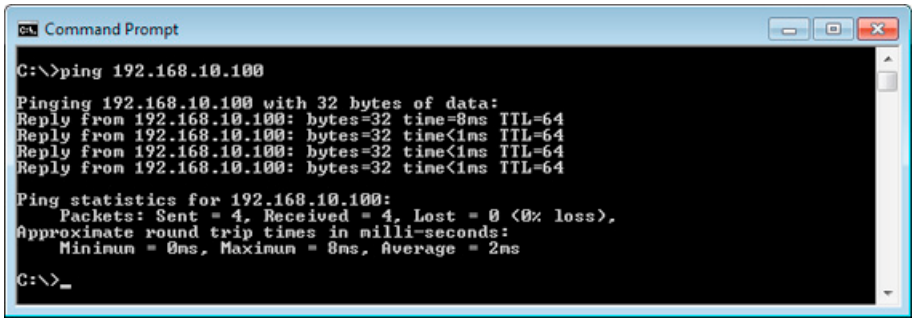
Test part 1 - sending the ping command

Now test the function of the NAT router mode in IP data traffic from internal to external as follows:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to PC1 (IP address 192.168.10.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.10.100" at the cursor position.

   You will then receive the following message (positive reply from PC1):



Result

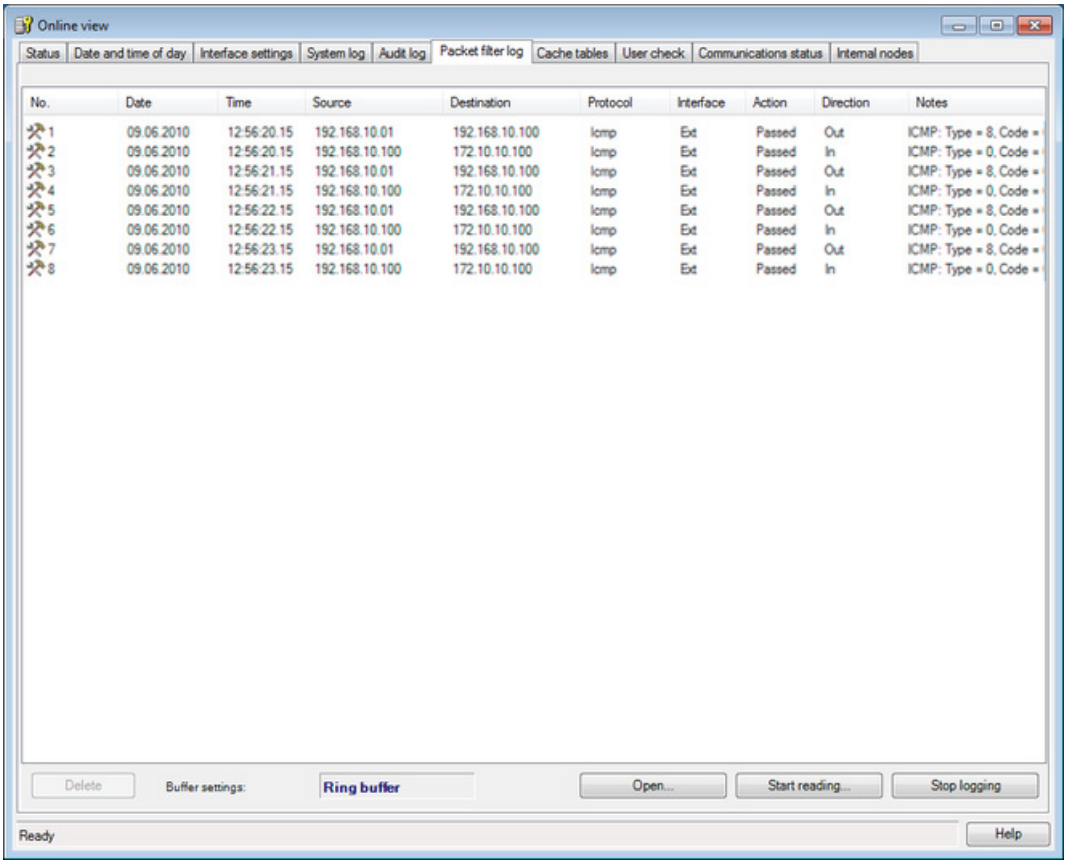
If the IP packets have reached PC1, the "Ping statistics" for 192.168.10.100 display the following:

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

Test part 2 - evaluating the result

1. Change to online mode in the Security Configuration Tool with the "View" > "Online" menu command.
2. Select the module you want to edit and then select the menu command "Edit" > "Online diagnostics" to open the online dialog.
3. Select the "Packet filter log" tab.
4. Click the "Start reading" button.
5. Acknowledge the displayed dialog with "OK".

   Result: The log entries are read from the security module and displayed here.



Result

You will see the following in the log output:

- Output row 1

  The IP addresses of the packets from PC2 to PC1 are displayed on the interface to the external network with the external IP address of the security module (192.168.10.1). This corresponds to the expected address translation (the additional port assignment is not visible here).

- Output row 2

  The reply packets are displayed with the destination address of the node in the internal subnet (PC2: 172.10.10.100).

- The following output rows accordingly

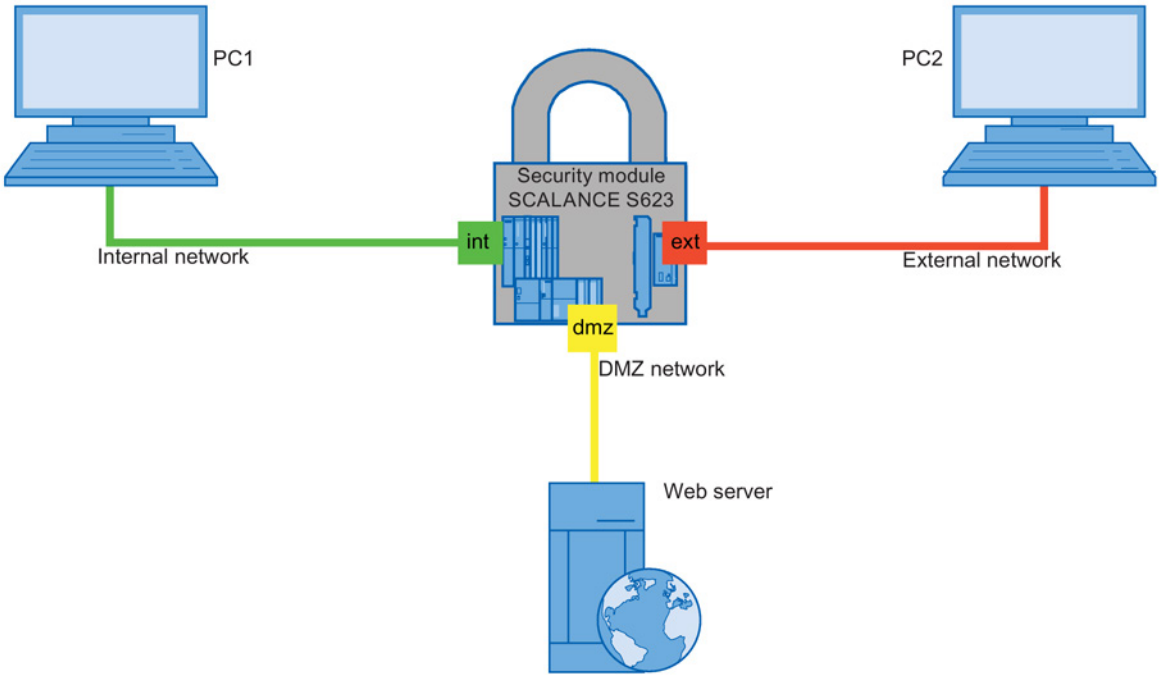
5.2 SCALANCE S as firewall between external network and DMZ

5.2.1 Overview

Overview

In this example, use the Software Configuration Tool to create a firewall rule permitting access from a PC from the external network to the Web server in the DMZ network. Access to the internal network remains blocked.

Setting up the test network



Required devices/components

Use the following components to set up the network:

- 1 x SCALANCE S623, (additional option: a suitably installed DIN rail with fittings);
- 1 x 24 V power supply with cable connector and terminal block plug;
- 1 x PC on which the "Security Configuration Tool" is installed;
- 1x Web server for configuration testing;

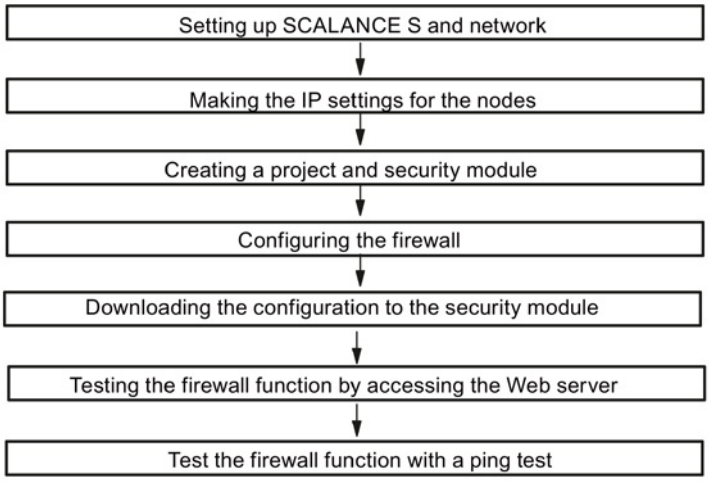
- 1x PC for testing the configuration;
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

Requirement:

To be able to work through the example, the following requirements must be met:

- You have defined an IP address, a subnet mask as well as a default gateway for the Web server. The IP address data used in this example can be obtained from the chapter " Configuring IP settings for network nodes".

Overview of the next steps:



5.2.2 Set up SCALANCE S and the network

Follow the steps outlined below:

1. First unpack the SCALANCE S623 and check that it is undamaged.
2. Connect the power supply to the SCALANCE S623.

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

⚠ WARNING

Use safety extra-low voltage only

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

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

1. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   - Connect PC1 to the internal interface of the security module.
   - Connect the Web server to the DMZ interface of the security module.
   - Connect PC2 to the external interface of the security module.
2. Now, turn on the PCs.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;
- Interface X3 - DMZ port (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.

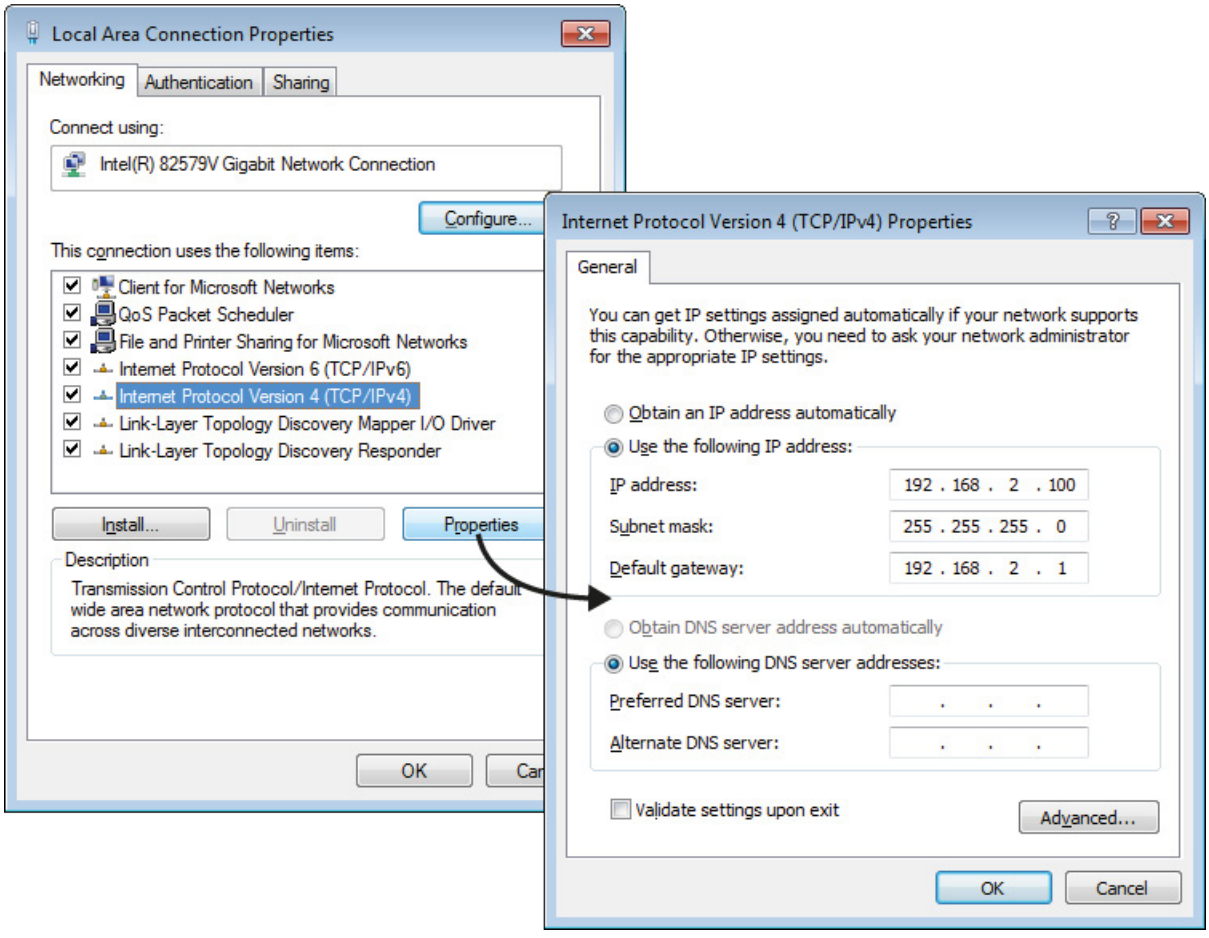
5.2.3 Configuring IP settings for the nodes

For the test, the nodes are given the following IP address settings:

Node	IP address	Subnet mask	Default gateway (SCALANCE S623)
PC1	192.168.2.100	255.255.255.0	192.168.2.1
Web server	192.168.3.100	255.255.255.0	192.168.3.1
PC2	192.168.1.100	255.255.255.0	192.168.1.1

Setting the IP addresses of the PCs

1. On PC1, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.



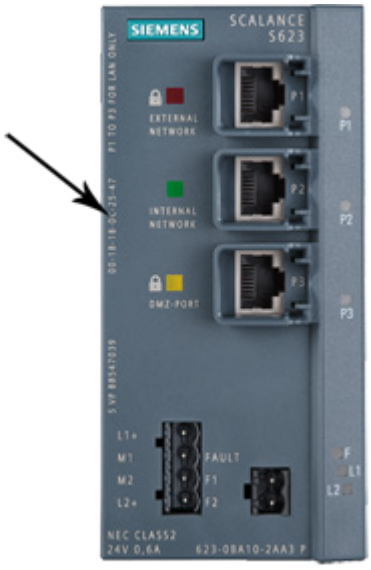
5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button.
6. Now enter the values assigned to the PC in the relevant boxes from the table "Making the IP settings for the nodes".
7. Close the dialogs with "OK" and close the Control Panel.
8. Repeat steps 1 to 7 for PC2.

5.2.4 Creating a project and security module

Follow the steps below:

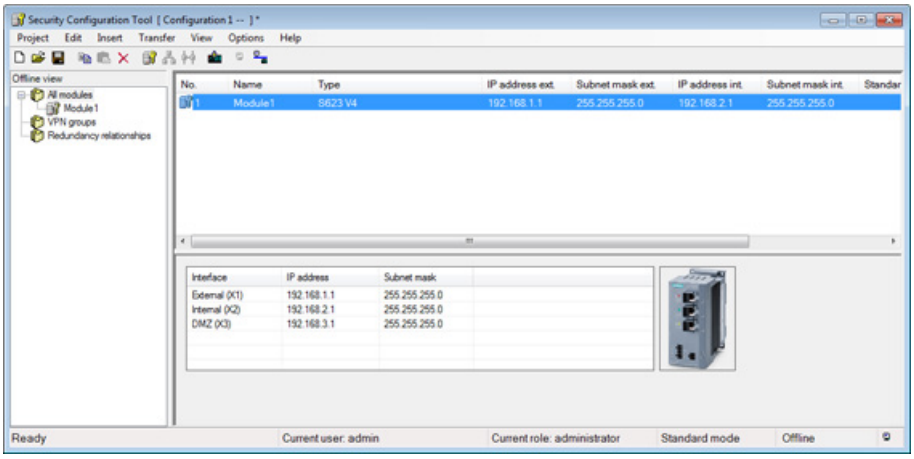
1. Install and start the Security Configuration Tool on PC2.
2. Select the "Project" > "New..." menu command.
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.
4. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module: S623
   - Firmware release: V4
5. In the "Configuration" area, enter the MAC address in the required format. The MAC address is printed on the front of the SCALANCE S module (see figure).



6. In the "Configuration" area, enter the external IP address (192.168.1.1) and the external subnet mask (255.255.255.0) in the required format.
7. From the drop-down list, select the "Routing mode" for "Interface routing external/internal".
8. Enter the internal IP address (192.168.2.1) and the internal subnet mask (255.255.255.0) in the required format and confirm the dialog with "OK".
9. Select the security module in the content area.
10. Select the "Edit" > "Properties..." menu command.

11. Select the "Activate interface" check box in the "DMZ port (X3)" area of the "Interfaces" tab and enter the IP address (192.168.3.1) and the subnet mask (255.255.255.0) for the DMZ interface.
12. Confirm the dialog with "OK".



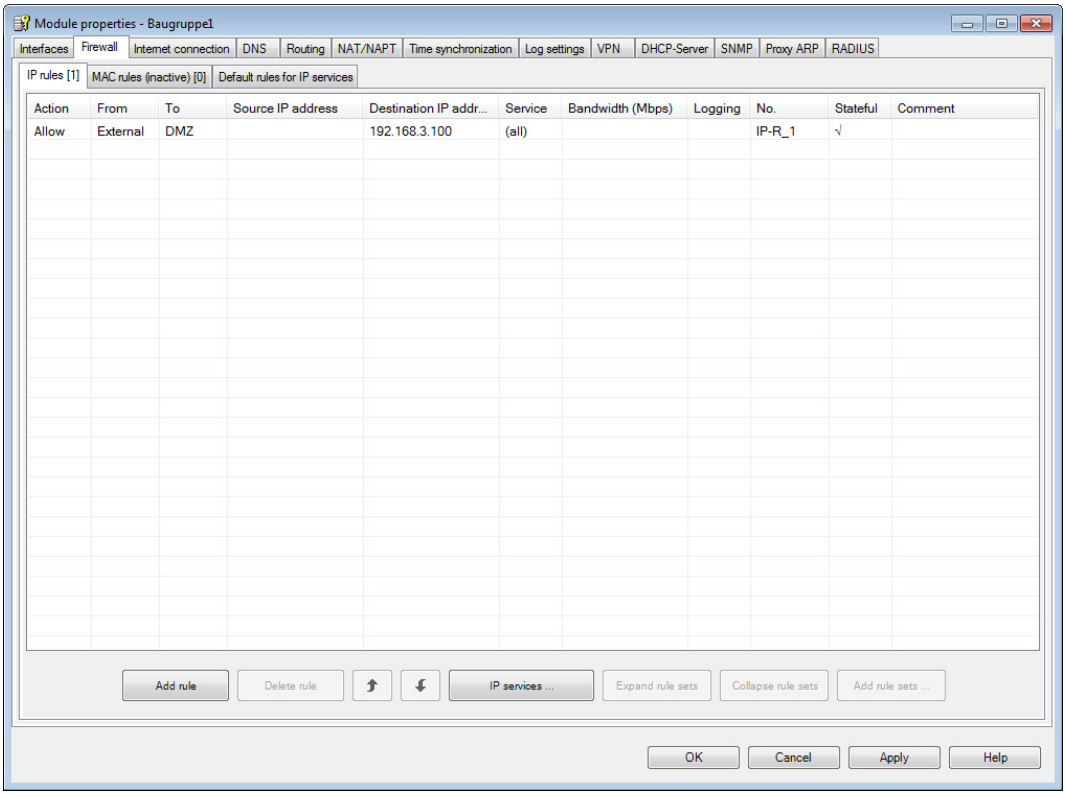
5.2.5 Configuring a firewall

In the next section, you define a firewall rule permitting access from PC2 in the external network to the Web server in the DMZ network.

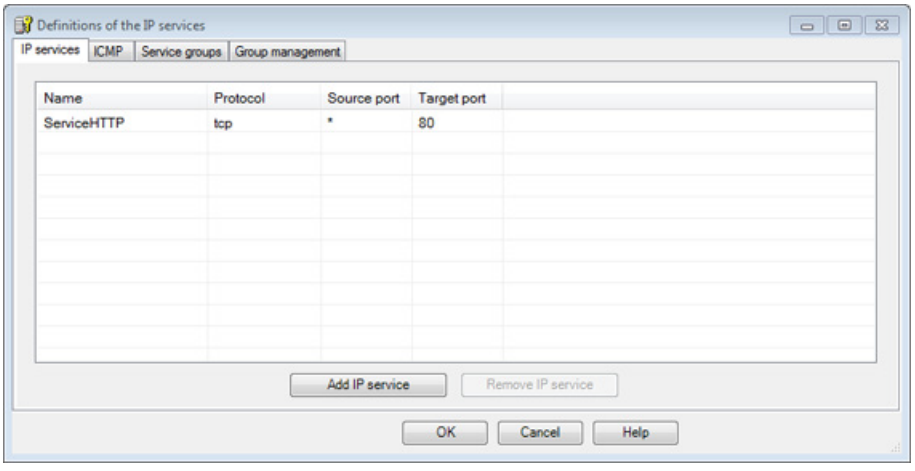
Configuring the firewall - Follow the steps below:

1. Change the configuration view to advanced mode with the menu command "View" > "Advanced mode".
2. Select the security module in the content area.
3. Select the "Edit" > "Properties..." menu command, "Firewall" tab.

4. Click the "Add rule" button to add a new rule as follows:



5. Click the "Apply" button and then the "IP services..." button.
6. In the "Definitions of the IP services" dialog, click the "Add IP service" button and enter an IP service as shown below. The name of the IP service has no effect on its function.

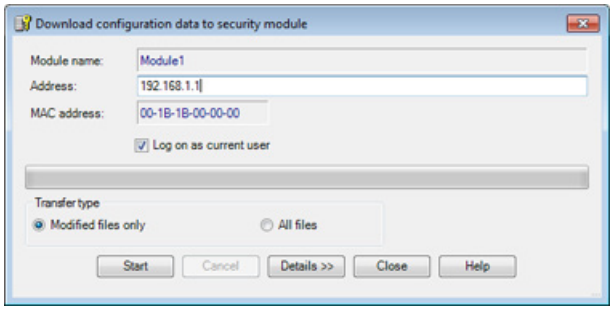


7. Close the "Definitions of the IP services" dialog with "OK".
8. For the firewall rule, select the IP service you have just defined from the drop-down list in the "Service" column.
9. Close the dialog with "OK".

5.2.6 Downloading the configuration to the security module

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Select the security module in the content area.
3. Select the "Transfer" > "To module(s)..." menu command.



4. Start the download with the "Start" button.

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

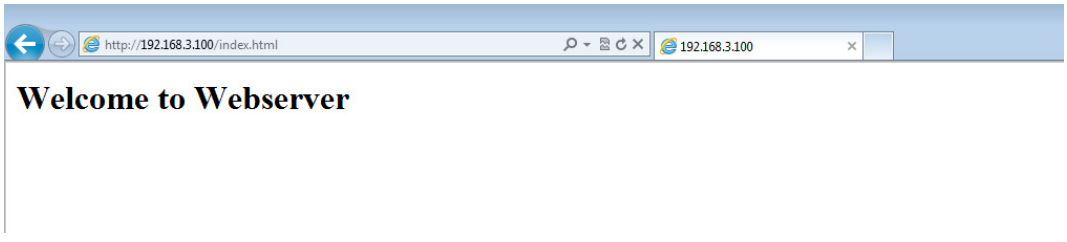
Result: SCALANCE S in productive operation

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

5.2.7 Testing the firewall function by accessing the Web server

Follow the steps below:

1. Start a Web browser on PC2.
2. Test the reachability of the Web server by entering the IP address of the Web server (192.168.3.100) in the address line of the Web browser. In the situation here, for example, an HTML document is called up that is located on the Web server.



Result

Based on the configured firewall rule, access from PC2 in the external network to the Web server in the DMZ network was successful.

5.2.8 Test the firewall function with a ping test

How can you test the configured function?

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

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

Note

Firewall in Windows

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

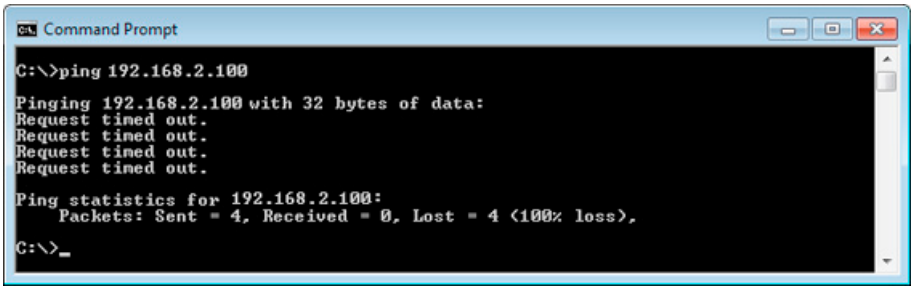
Testing

Now test the function of the firewall configuration with blocked data traffic from the external network to the internal network as follows:

1. Call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt" on PC2.
2. Enter the ping command from PC2 to PC1 (IP address 192.168.2.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.2.100" at the cursor position.

   You will then receive the following message (no reply from PC1):



Result

The IP packets from PC2 cannot reach PC1 because the data traffic from the external network to the internal network is not allowed.

This is shown in the "Ping statistics" for 192.168.2.100 as follows:

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

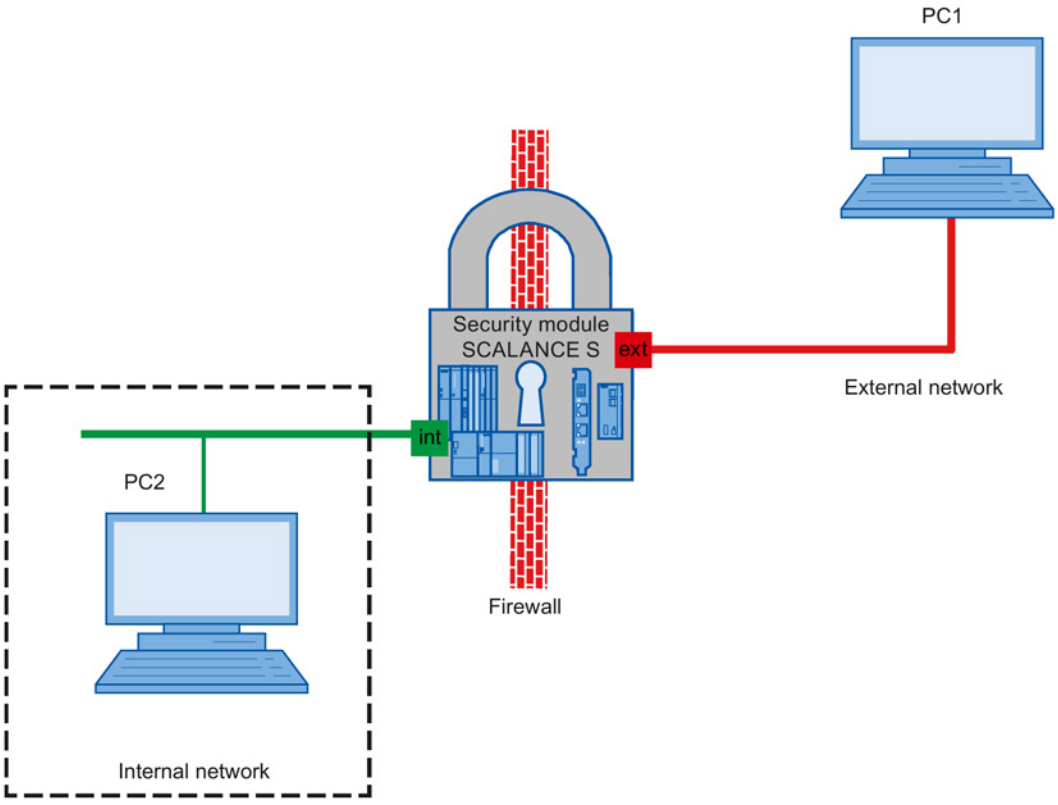
5.3 SCALANCE S as user-specific firewall between external network and internal network

5.3.1 Overview

Overview

In this example, you create a user-specific IP rule set and assign it to a user. You configure in the "advanced mode" configuration view.

The created user is allowed to access PC2 in the internal network from PC1 in the external network. For other users, access remains blocked.



Setting up the test network

- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the security module.

  – PC2: Represents a node in the internal network

- Security module: SCALANCE S module for protection of the internal network

- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

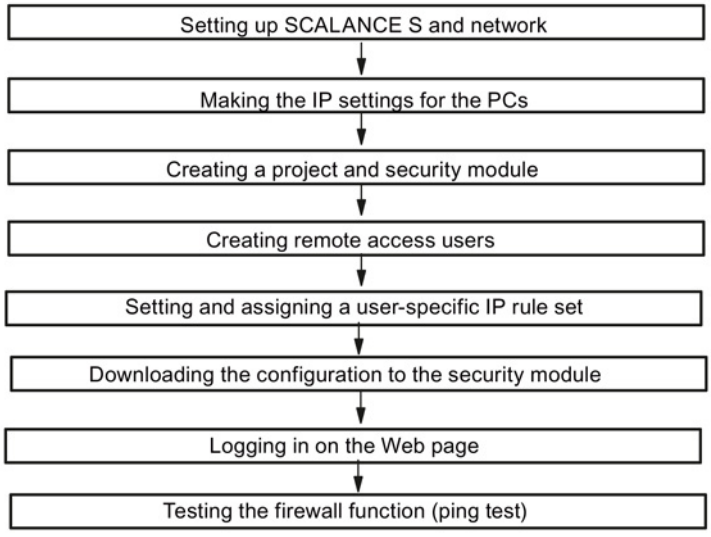
  PC1: PC with the Security Configuration Tool

Required devices/components:

Use the following components to set up the network:

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

Overview of the next steps:



5.3.2 Set up SCALANCE S and the network

Follow the steps below:

1. First unpack the SCALANCE S and check that it is undamaged.
2. Connect the power supply to the SCALANCE S.

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

⚠ WARNING

Use safety extra-low voltage only

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

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

1. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   – Connect PC2 to the internal interface of the security module.
   – Connect PC1 to the external interface of the security module.
2. Now turn on the PCs.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;

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

5.3.3 Make the IP settings for the PCs

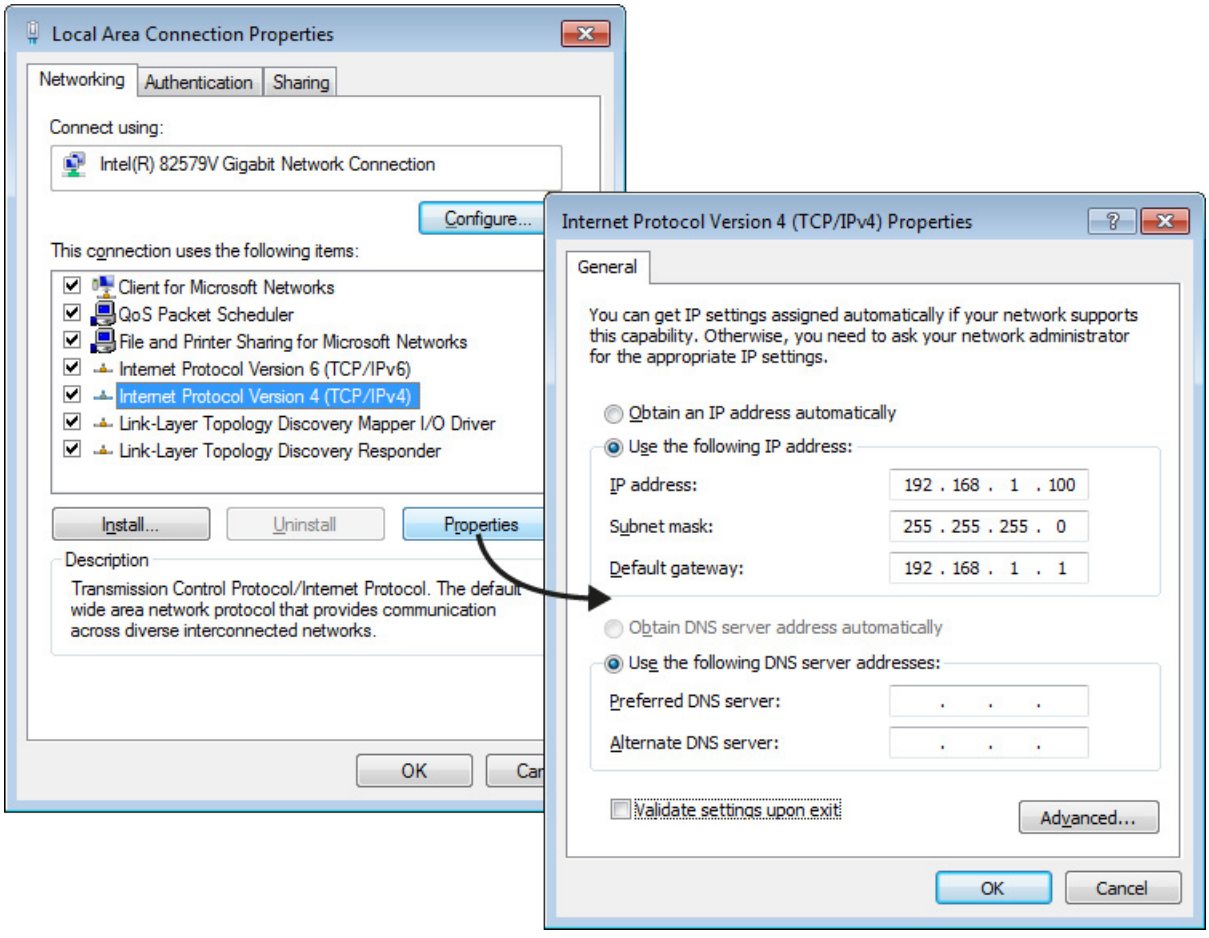
For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask	Default gateway
PC1	192.168.1.100	255.255.255.0	192.168.1.1
PC2	192.168.2.100	255.255.255.0	192.168.2.1

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button.
6. Now enter the values assigned to the PC from the table "Making the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

5.3.4 Creating a project and security module

Follow the steps below:

1. Install and start the Security Configuration Tool on PC1.
2. Select the "Project" > "New..." menu command.

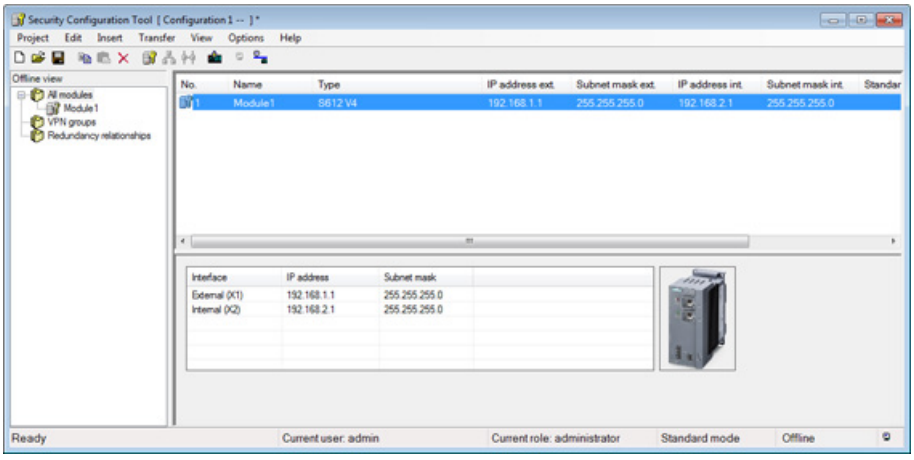
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.

4. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module: S612
   - Firmware release: V4
5. In the "Configuration" area, enter the MAC address in the required format.

   The MAC address is printed on the front of the SCALANCE S module.

6. In the "Configuration" area, enter the external IP address (192.168.1.1) and the external subnet mask (255.255.255.0) in the required format.
7. From the drop-down list, select the "Routing mode" for "Interface routing external/internal".
8. Enter the internal IP address (192.168.2.1) and the internal subnet mask (255.255.255.0) in the required format and confirm the dialog with "OK".

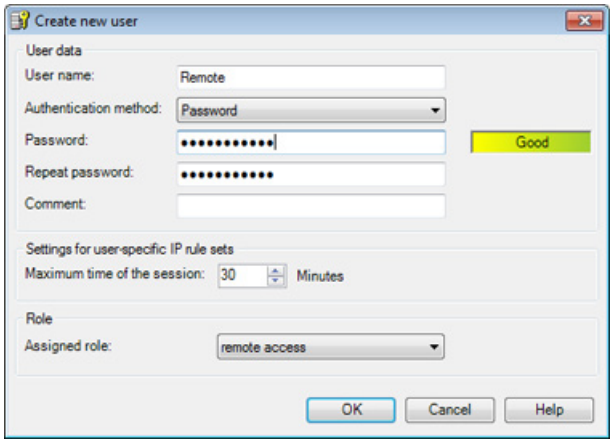


5.3.5 Creating remote access users

Creating a remote access user

1. Select the "Options" > "User management..." menu command.
2. Click the "Add..." button in the "User" tab.

3. Create a new user with the following settings:

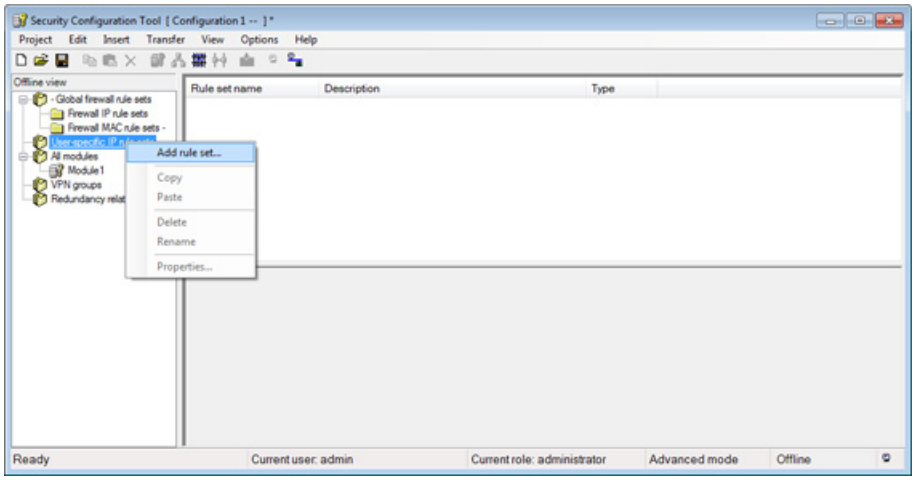


4. Close the dialog with "OK".
5. Close the user management with "OK".

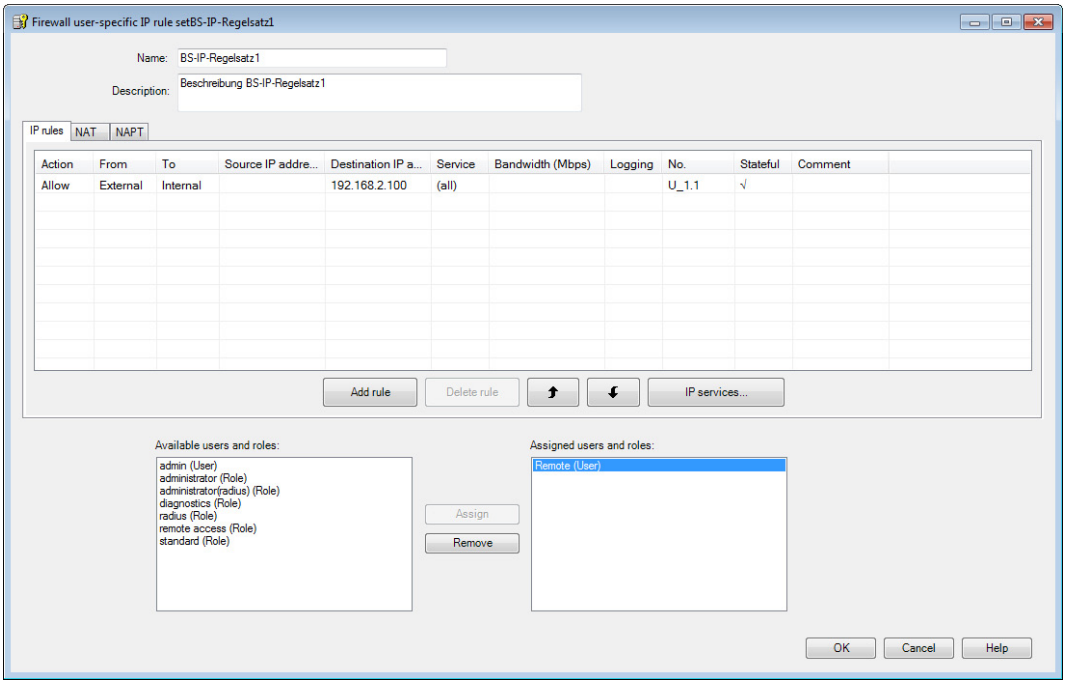
5.3.6 Setting and assigning a user-specific IP rule set

How to access this function

1. Change the configuration view to advanced mode with the menu command "View" > "Advanced mode".
2. Select the "User-specific IP rule sets" object in the navigation panel.
3. Select the "Insert rule set..." entry in the shortcut menu.



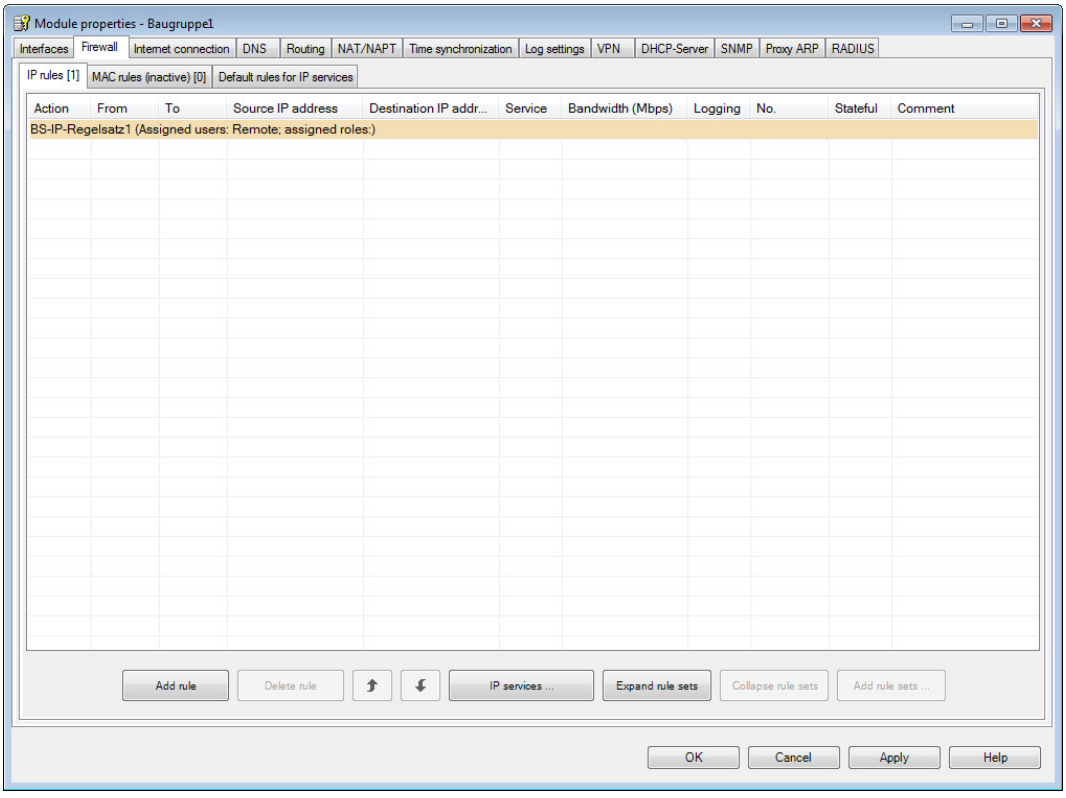
4. Enter a rule in the dialog as shown below:



5. From the "Available users and roles" list, select the "Remote (user)" entry and click the "Assign" button.
6. Close the dialog with "OK".

To assign a rule set, follow the steps below:

1. Select the security module in the navigation panel and holding down the left mouse button, drag it to the newly created user-specific IP rule set.
2. You can check the assignment by opening the dialog for setting the module properties and selecting the "Firewall" tab. The user-specific IP rule set was saved in the "IP rules" subtab.



3. If you click the "Expand rule sets" button, you can view the rule set in detail.

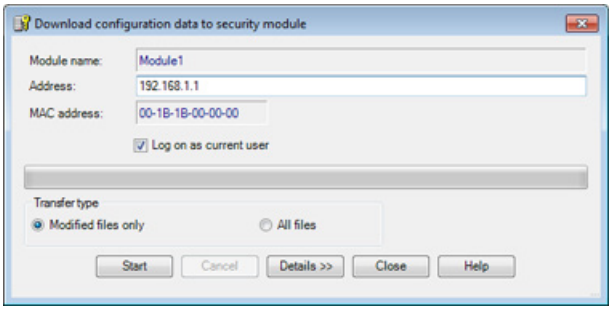
   Result: The offline configuration is complete.

5.3.7 Downloading the configuration to the security module

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Select the security module in the content area.

3. Select the "Transfer" > "To module(s)..." menu command.



4. Start the download with the "Start" button.

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

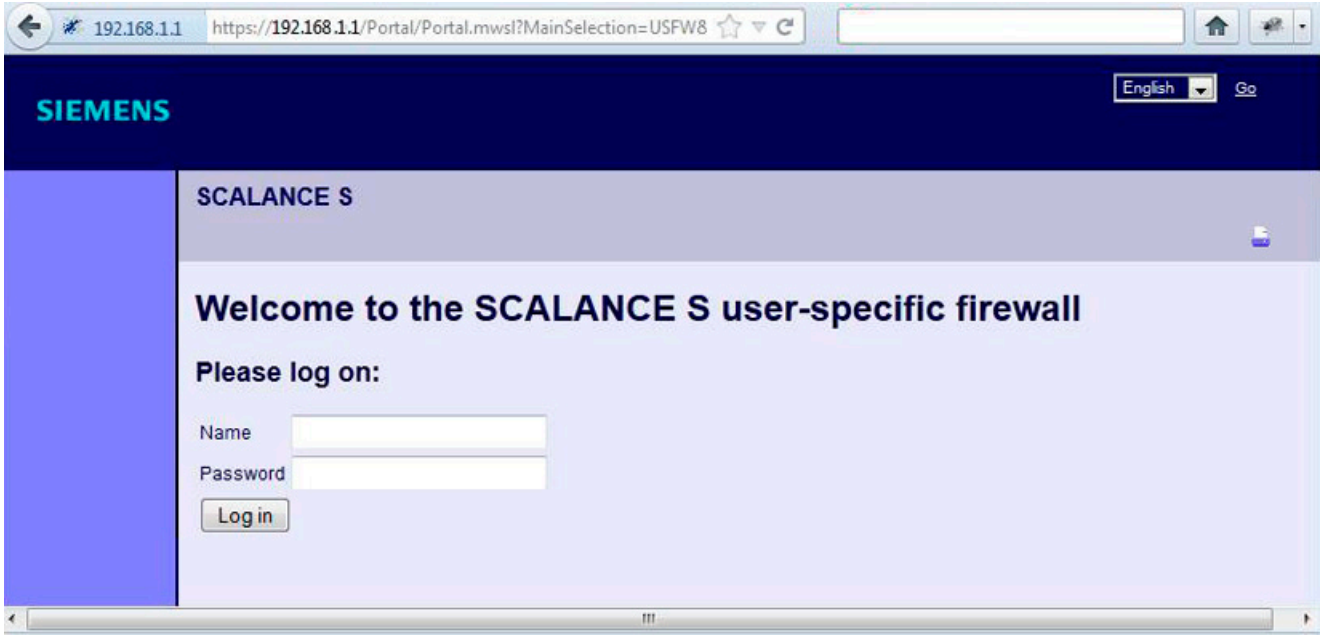
Result: SCALANCE S in productive operation

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

5.3.8 Logging in on the Web page

Logging on via Web page

1. In the Web browser of PC1, enter the address "https://192.168.1.1".
2. In the following window, enter the user name "Remote" and the corresponding password and click the "Log in" button.



3. The defined IP rule set is enabled for the "Remote" user. Access from PC1 in the external network to PC2 in the internal network is allowed.

5.3.9 Test the firewall function (ping test)

How can you test the configured function?

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

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

Note

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

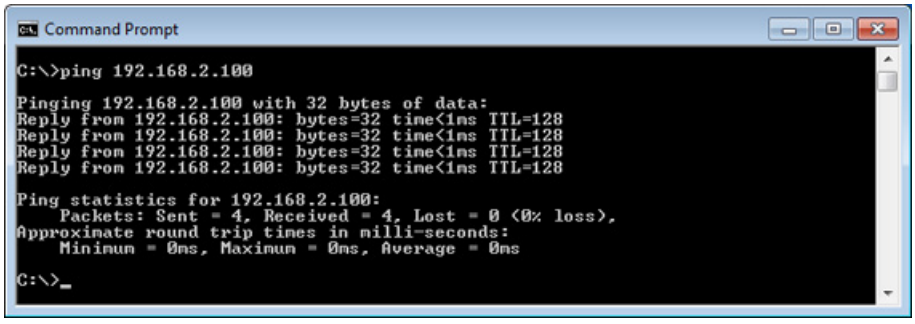
Testing

Now test the function of the firewall configuration as follows:

1. On PC1, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC1 to PC2 (IP address 192.168.2.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.2.100" at the cursor position:

   You will then receive the following message (positive reply from PC2):



Result

When the IP packets have reached PC2, the "Ping statistics" for 192.168.2.100 display the following:

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

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

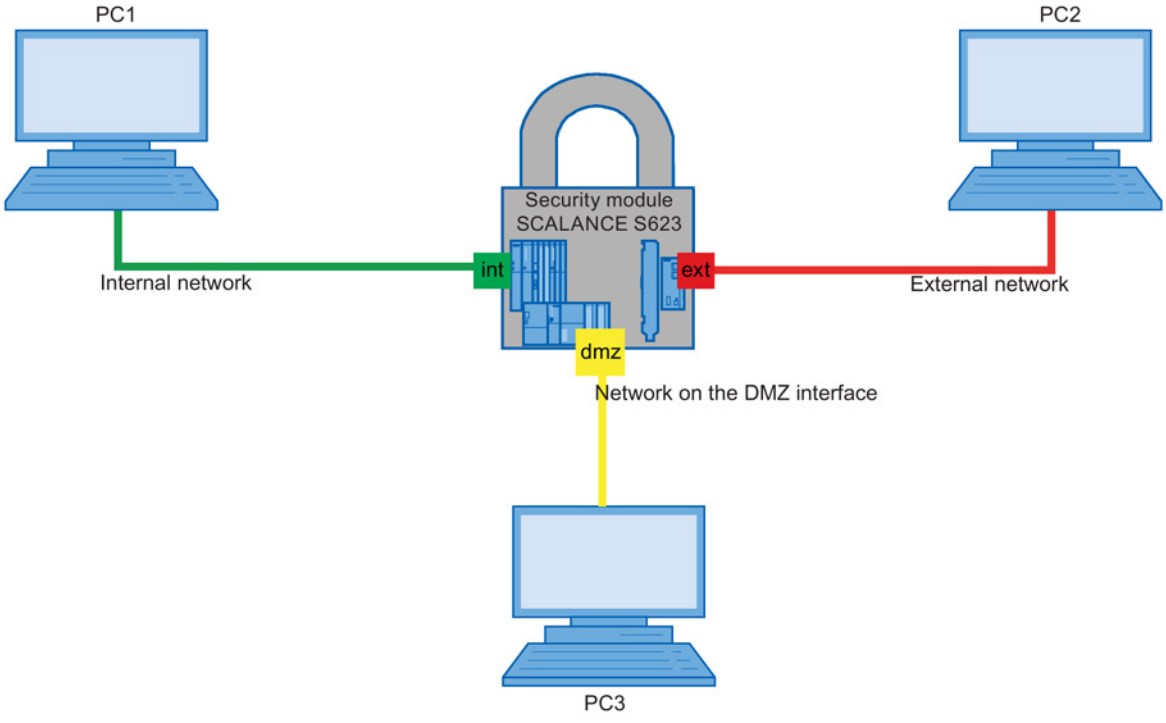
5.4 SCALANCE S as user-specific firewall between network on DMZ interface and internal network

5.4.1 Overview

Overview

In this example, you create a user-specific IP rule set and assign it to a user. You configure in the "advanced mode" configuration view.

The created user is permitted to access PC1 in the internal network from PC3 in the network connected to the DMZ interface. For other users, access remains blocked.



Setting up the test network

- Internal network - attachment to the internal interface of the security module

  In the internal network, there is a PC connected to the internal security of the security module.

- Network on the DMZ interface - attachment to the DMZ interface of the security module

  In the network on the DMZ interface, there is a PC that is attached to the DMZ interface of the security module. The Security Configuration Tool software is installed on the PC.

- External network - attachment to the external interface of the security module

  The PC connected to the external interface represents a node of the external network.

Required devices/components

Use the following components to set up the network:

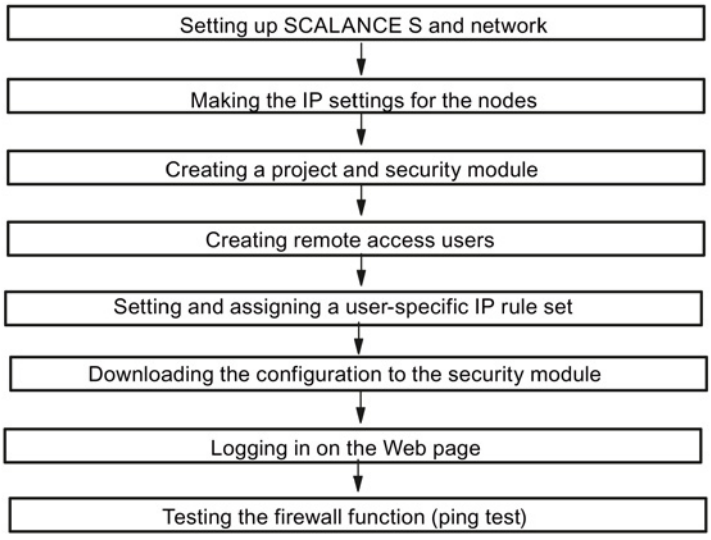
- 1 x SCALANCE S623 module, (additional option: a suitably installed DIN rail with fittings);
- 1 x 24 V power supply with cable connector and terminal block plug;
- 1 x PC in the network on the DMZ interface on which the Security Configuration Tool is installed;
- 2 x PC in the internal network or in the external network for testing the configuration;
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

Requirement:

To be able to work through the example, the following requirements must be met:

- You have configured IP addresses for the interfaces of the SCALANCE S623 module in the Security Configuration Tool and the configuration has been downloaded to the security module via the external or the internal interface. How you create such a configuration and download this to the security module via the external port is described in the following section:
  - Configuring IP addresses for SCALANCE S623 (Page 17)

Overview of the next steps



5.4.2 Setting up SCALANCE S and network

Follow the steps below:

1. First unpack the SCALANCE S623 and check that it is undamaged.
2. Connect the power supply to the SCALANCE S623.

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

⚠ WARNING

Use safety extra-low voltage only

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

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

3. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   - Connect PC1 to the internal interface of the security module.
   - Connect PC2 to the external interface of the security module.
   - Connect PC3 to the DMZ interface of the security module.
4. Now, turn on the PCs.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;
- Interface X3 - DMZ port (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.

5.4.3 Configuring IP settings for the nodes

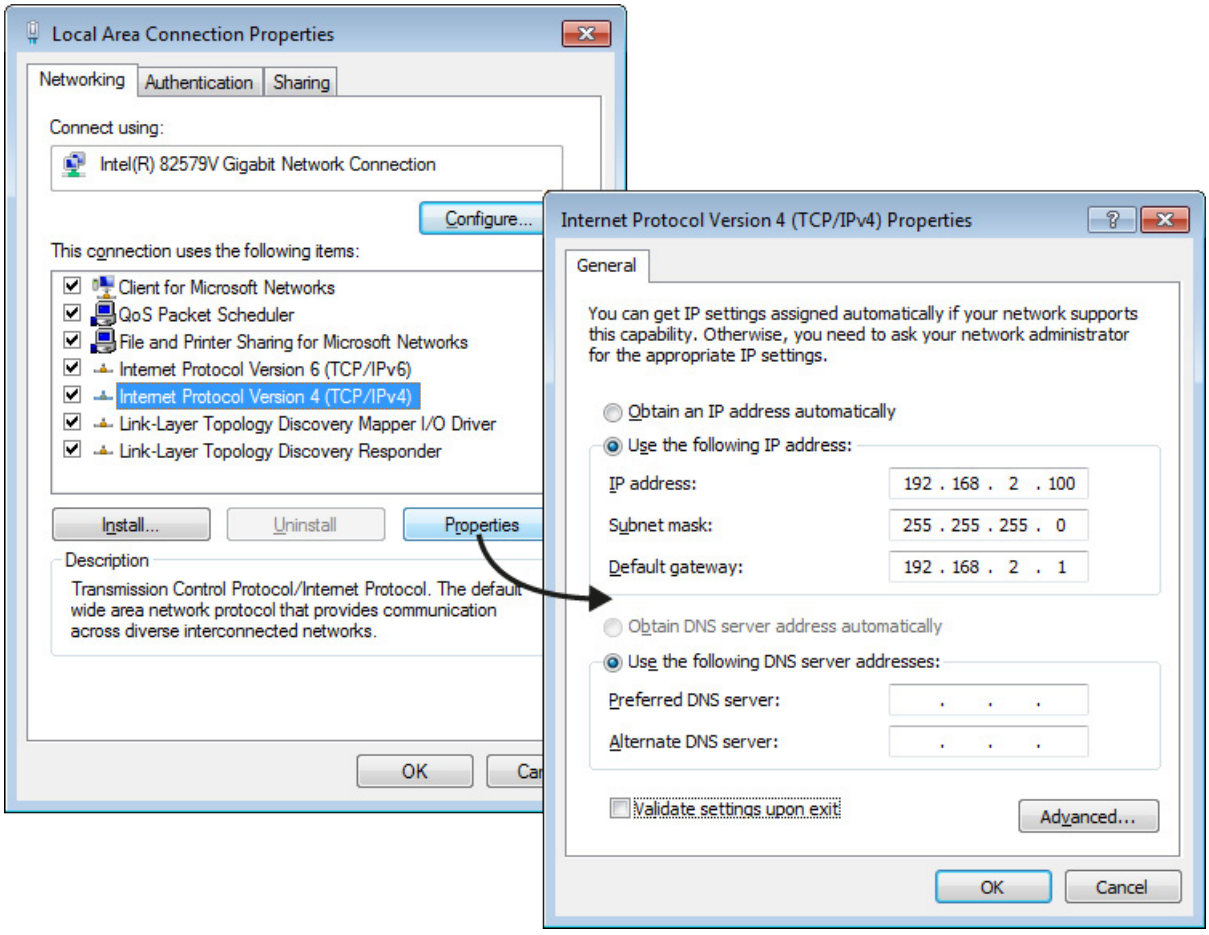
For the test, the nodes are given the following IP address settings:

Node	IP address	Subnet mask	Default gateway (SCALANCE S623)
PC1	192.168.2.100	255.255.255.0	192.168.2.1
PC2	192.168.3.100	255.255.255.0	192.168.3.1
PC3	192.168.1.100	255.255.255.0	192.168.1.1

Setting the IP addresses of the PCs

1. On PC1, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.

5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.



6. Now enter the values assigned to the PC in the relevant boxes from the table "Making the IP settings for the nodes".
7. Close the dialogs with "OK" and close the Control Panel.
8. Repeat steps 1 to 7 on PC2 and PC3.

5.4.4 Creating a project and security module

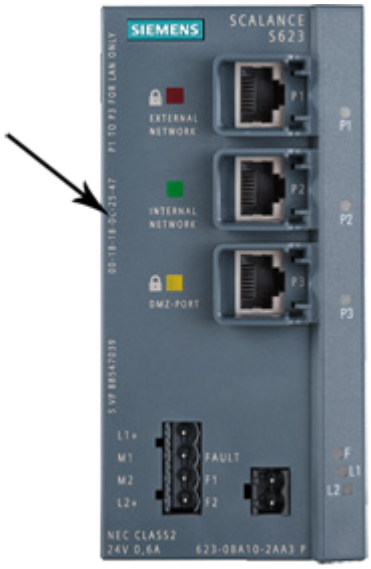
Follow the steps below:

1. Install and start the Security Configuration Tool on PC3.
2. Select the "Project" > "New..." menu command.

3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

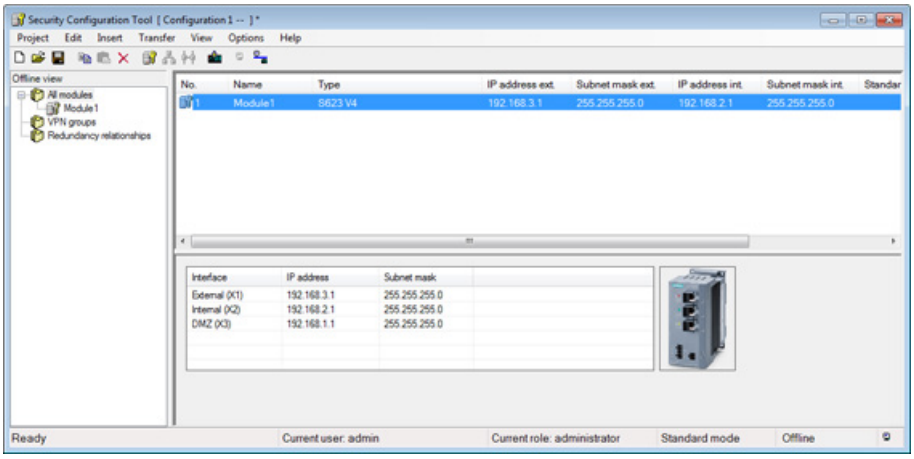
   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.

4. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module: S623
   - Firmware release: V4
5. In the "Configuration" area, enter the MAC address in the required format. The MAC address is printed on the front of the SCALANCE S module (see figure).



6. In the "Configuration" area, enter the external IP address (192.168.3.1) and the external subnet mask (255.255.255.0) in the required format.
7. From the drop-down list, select the "Routing mode" for "Interface routing external/internal".
8. Enter the internal IP address (192.168.2.1) and the internal subnet mask (255.255.255.0) in the required format and confirm the dialog with "OK".
9. Select the security module in the content area.
10. Select the "Edit" > "Properties..." menu command.

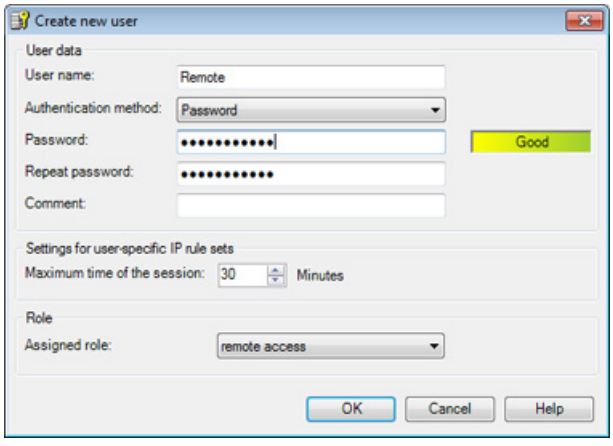
11. Select the "Activate interface" check box in the "DMZ port (X3)" area of the "Interfaces" tab and enter the IP address (192.168.1.1) and the subnet mask (255.255.255.0) for the DMZ interface.
12. Confirm the dialog with "OK".



5.4.5 Creating remote access users

Creating a remote access user

1. Select the "Options" > "User management..." menu command.
2. Click the "Add..." button in the "User" tab.
3. Create a new user with the following settings:

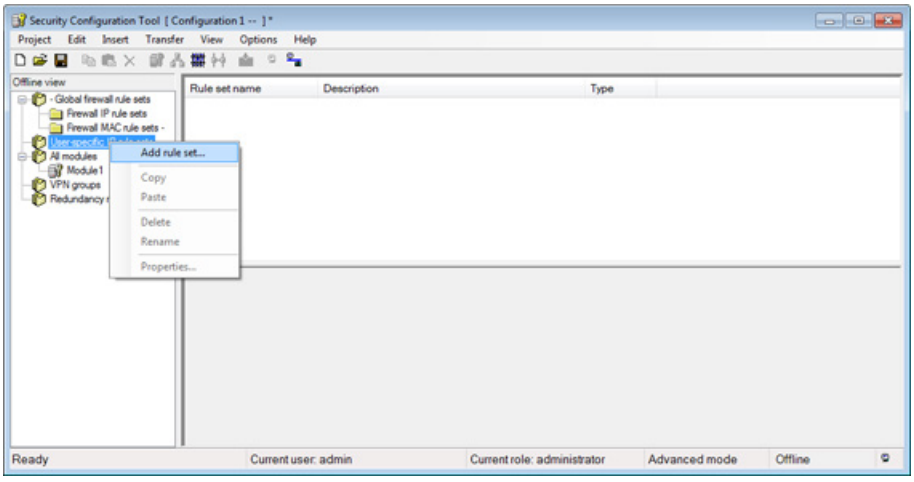


4. Close the dialog with "OK".
5. Close the user management with "OK".

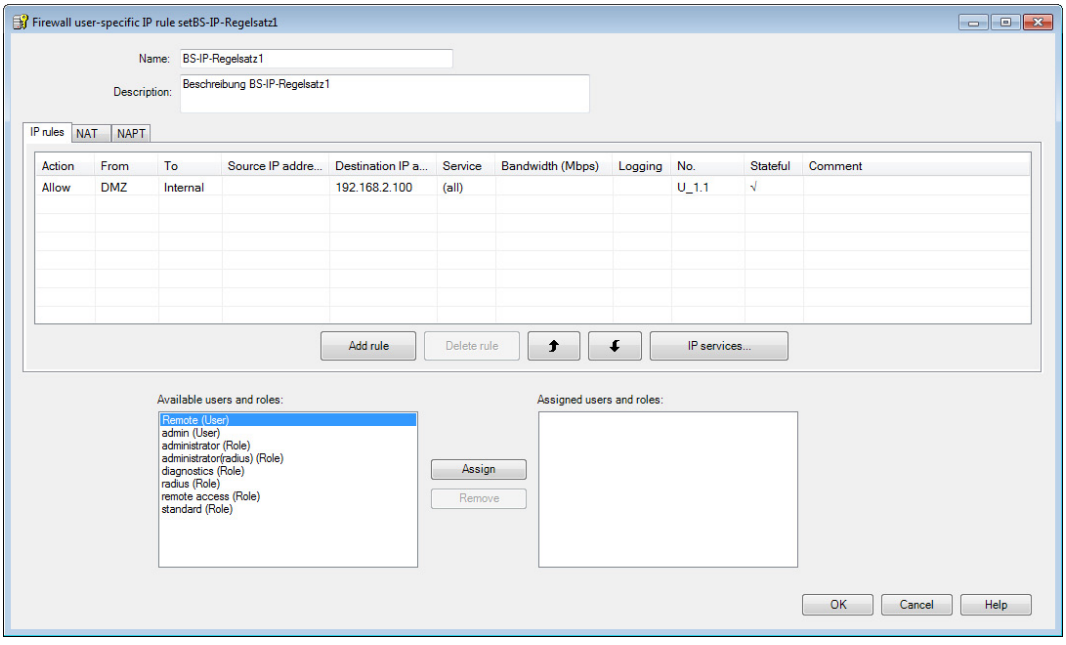
5.4.6 Setting and assigning a user-specific IP rule set

Setting a user-specific IP rule set

1. Change the configuration view to advanced mode with the menu command "View" > "Advanced mode".
2. Select the "User-specific IP rule sets" object in the navigation panel.
3. Select the "Insert rule set..." entry in the shortcut menu.



4. Click the "Add rule" button in the dialog that opens to add a new rule.
5. Enter a rule as shown below:



Note: This example describes full access to the network node with IP address "192.168.2.100" in the internal network without filtering at the port level. An example of

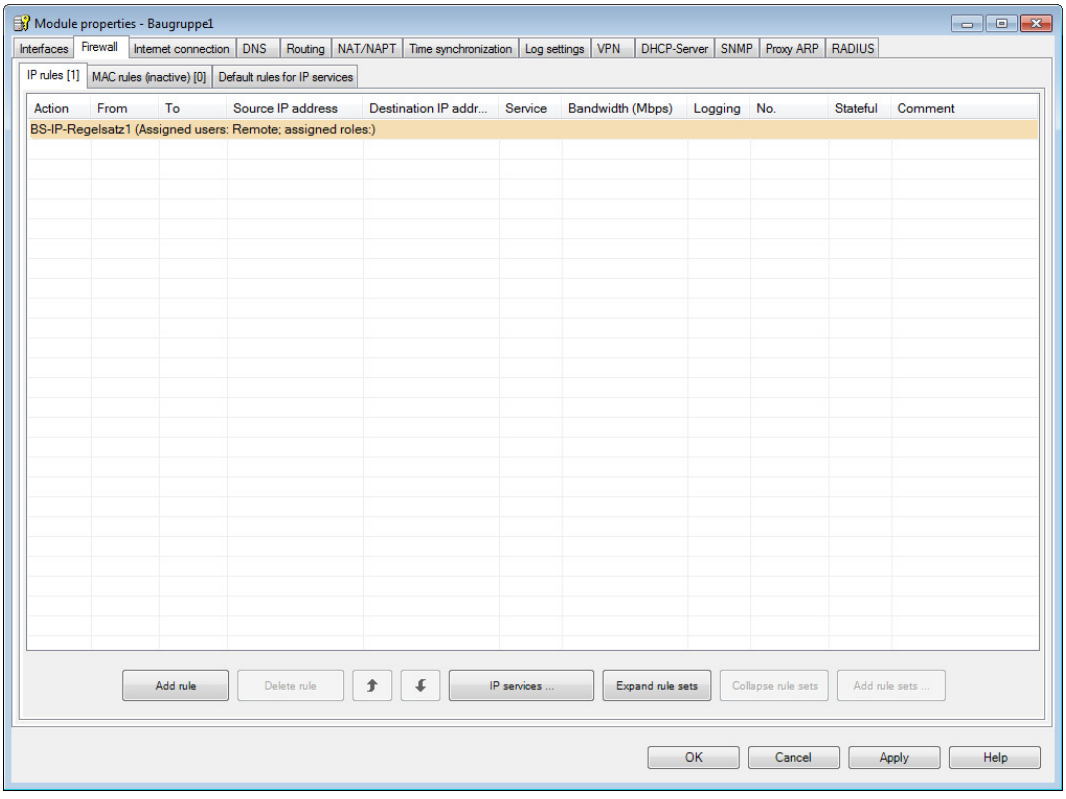
creating highly specific firewall rules can be found in the following section:
Configuring a firewall (Page 67)

For more detailed information, refer to the configuration manual "SIMATIC NET Industrial Ethernet Security - Basics and Application".

6. From the "Available users and roles" list, select the "Remote (user)" entry and click the "Assign" button.
7. Confirm the dialog with "OK".

Assigning a user-specific IP rule set

1. Select the security module in the navigation panel and holding down the left mouse button, drag it to the newly created user-specific IP rule set.
2. You can check the assignment by opening the dialog for setting the module properties and selecting the "Firewall" tab. The user-specific IP rule set was saved in the "IP rules" subtab.



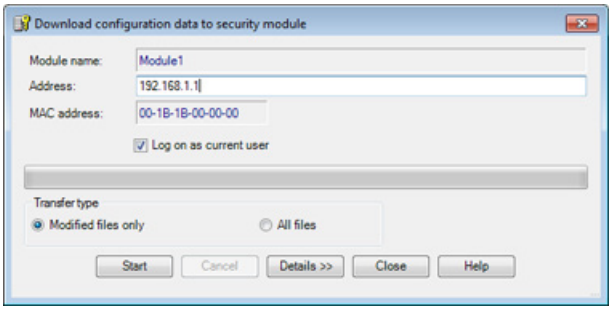
3. If you click the "Expand rule sets" button, you can view the IP rule set in detail.

   Result: The offline configuration is complete.

5.4.7 Downloading the configuration to the security module

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Select the security module in the content area.
3. Select the "Transfer" > "To module(s)..." menu command.



4. Start the download with the "Start" button.

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

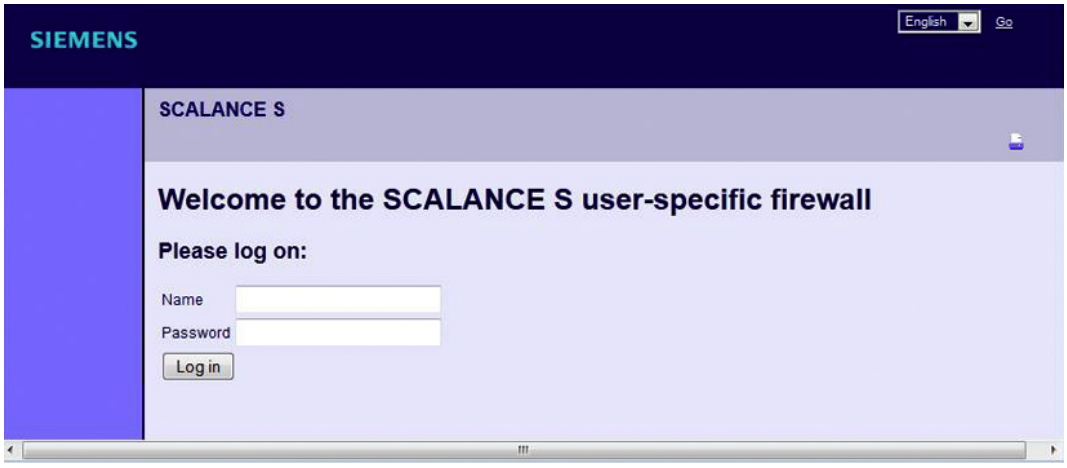
Result: SCALANCE S in productive operation

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

5.4.8 Logging in on the Web page

Logging on via Web page

1. In the Web browser of PC3, enter the address "https://192.168.1.1".
2. In the following window, enter the user name "Remote" and the corresponding password and click the "Log in" button.



3. The defined IP rule set is enabled for the "Remote" user. Access from PC3 in the network on the DMZ interface to PC1 in the internal network is allowed.

5.4.9 Test the firewall function (ping test)

How can you test the configured function?

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

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

Note

Firewall in Windows

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

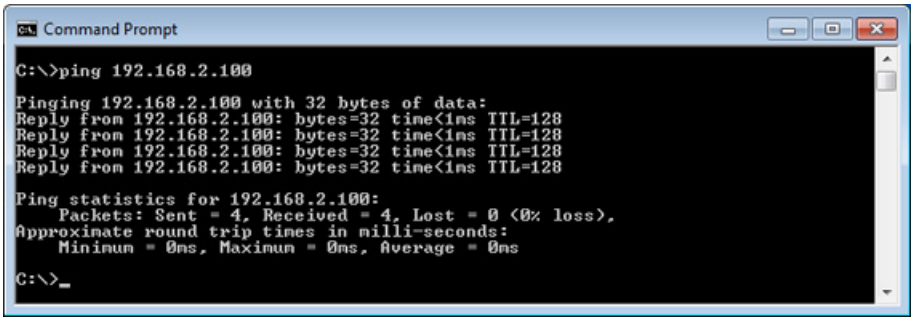
Test phase 1

Now test the function of the firewall configuration as follows:

1. On PC3, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC3 to PC1 (IP address 192.168.2.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.2.100" at the cursor position.

   You will then receive the following message (positive reply from PC1):



Result

If the IP packets have reached PC1, the "Ping statistics" for 192.168.2.100 display the following:

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

Due to the configuration, the ping packets can pass from the network on the DMZ interface to the internal network. PC1 in the internal network has replied to the ping packets. Due to the "stateful inspection" function of the firewall, the reply packets arriving from the internal network are automatically allowed into the network on the DMZ interface.

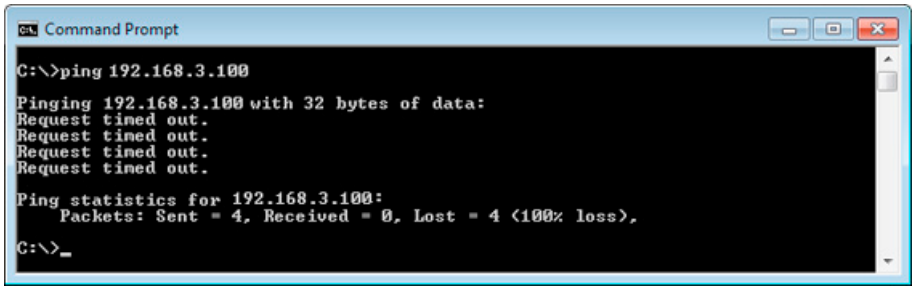
Test phase 2

Now test the function of the firewall configuration with blocked data traffic from the network on the DMZ interface to the external network as follows:

1. On PC3, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt" again.
2. Enter the ping command from PC3 to PC2 (IP address 192.168.3.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.3.100" at the cursor position.

   You will then receive the following message (no reply from PC2):



Result

The IP packets from PC3 cannot reach PC2 because the data traffic from the network on the DMZ interface to the external network is not allowed.

This is shown in the "Ping statistics" for 192.168.3.100 as follows:

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

5.5 CP x43-1 Advanced as firewall and NAT router

5.5.1 Overview

In this example, you configure the NAT router mode. You configure in the "advanced mode" configuration view.

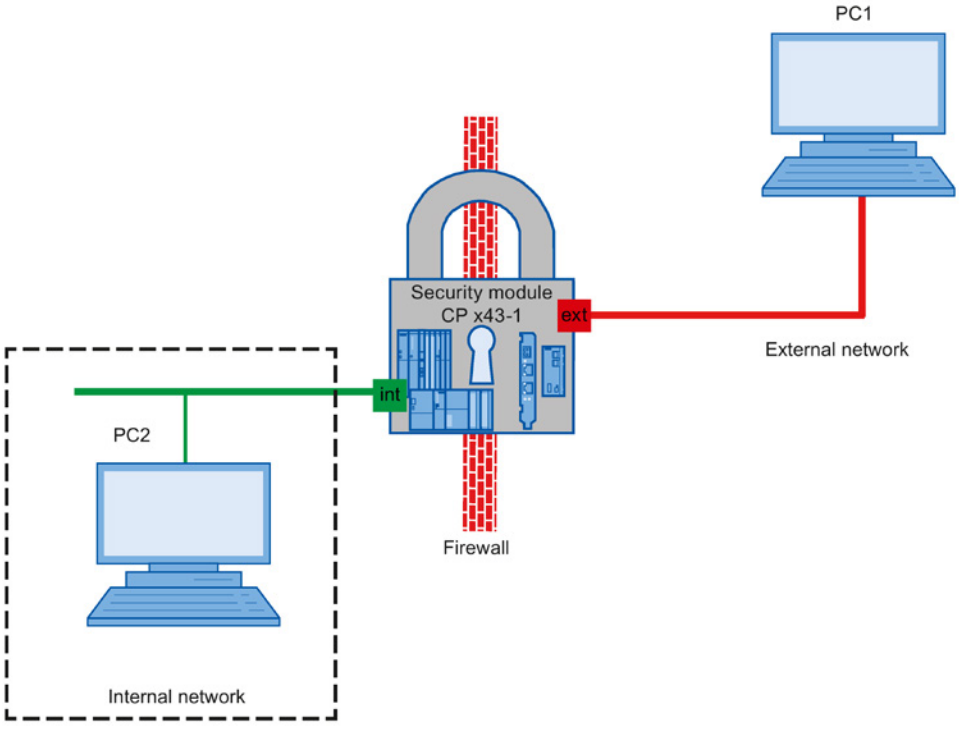
With this configuration, you have the situation that all the packets sent from the internal subnet to the PC1 node in the external network are allowed to pass the firewall. The packets are forwarded to the outside with an IP address translated to the IP address of the security module and with a dynamically assigned port number. Only the replies to these packets is allowed to pass from the external network.

Note

Please remember that after loading the configuration, your station can only be reached if the S7 protocol (TCP port 102) is allowed from "External => Station" in the firewall. Unencrypted communication from the external network should be avoided following commissioning. If you do not use secure connection establishment from the external network via VPN, you should run STEP 7 diagnostics and reconfigure only from within the internal network.

For this reason, in the following example the port for S7 communication is not open in the firewall.

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the security module.

  – PC2: Represents a node in the internal network
- Security module: CP x43-1 Adv. to protect the internal network
- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

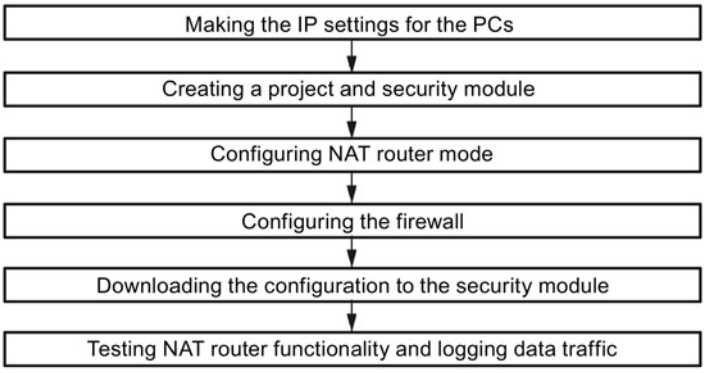
  – PC1: PC with the Security Configuration Tool and STEP 7

Requirement:

To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software is installed on PC1.
- STEP 7 is installed on PC1 and a STEP 7 project with the security module has already been created.
- The IP address of PC1 must be in the same subnet as the gigabit address of the security module.
- CP x43-1 Adv. has the following settings in STEP 7:
  – Gigabit IP address: 140.0.0.1, subnet mask: 255.255.0.0
  – PROFINET IP address: 192.0.0.1, subnet mask: 255.255.255.0

Overview of the next steps:



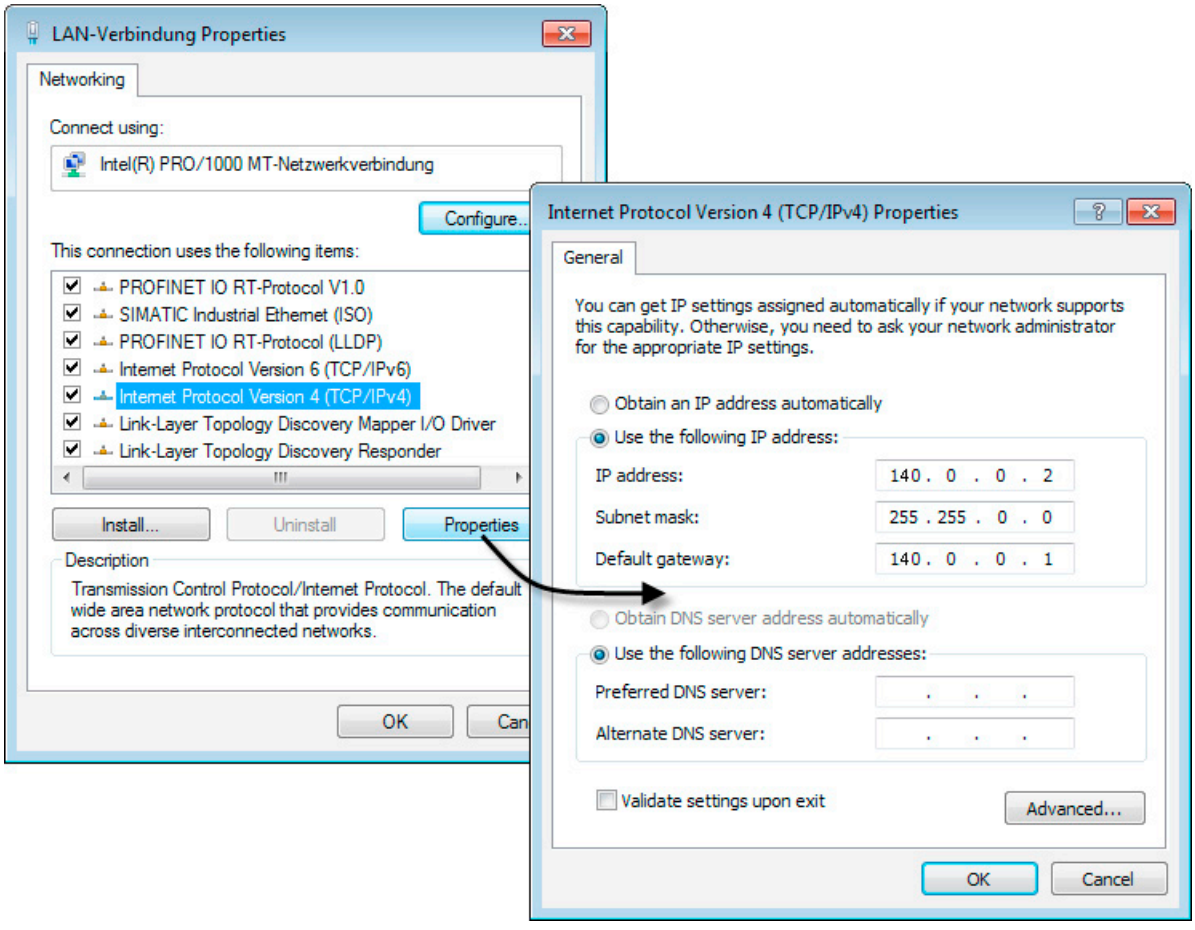
5.5.2 Make the IP settings for the PCs

For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask	Default gateway
PC1	140.0.0.2	255.255.0.0	140.0.0.1
PC2	192.0.0.2	255.255.255.0	192.0.0.1

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.

6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

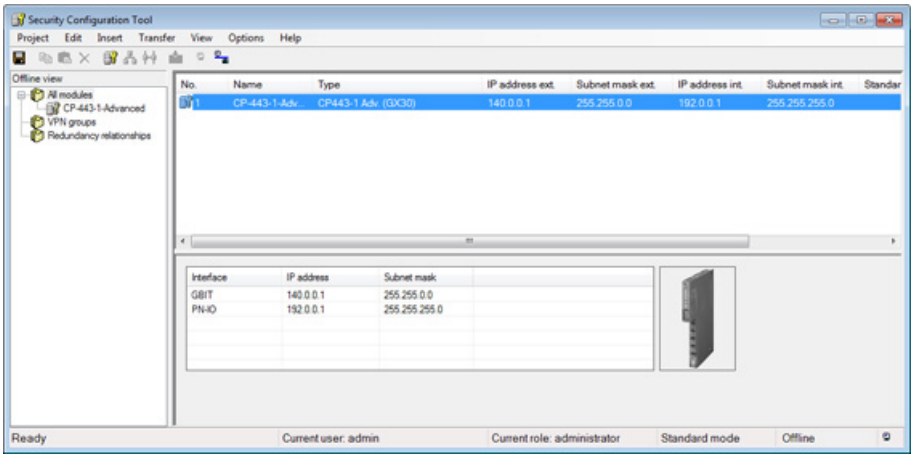
5.5.3 Creating a project and security module

Follow the steps below:

1. In the "Security" tab of the object properties, enable the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new security project is created.
3. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.

Result: The security module will then be displayed in the list of configured modules.



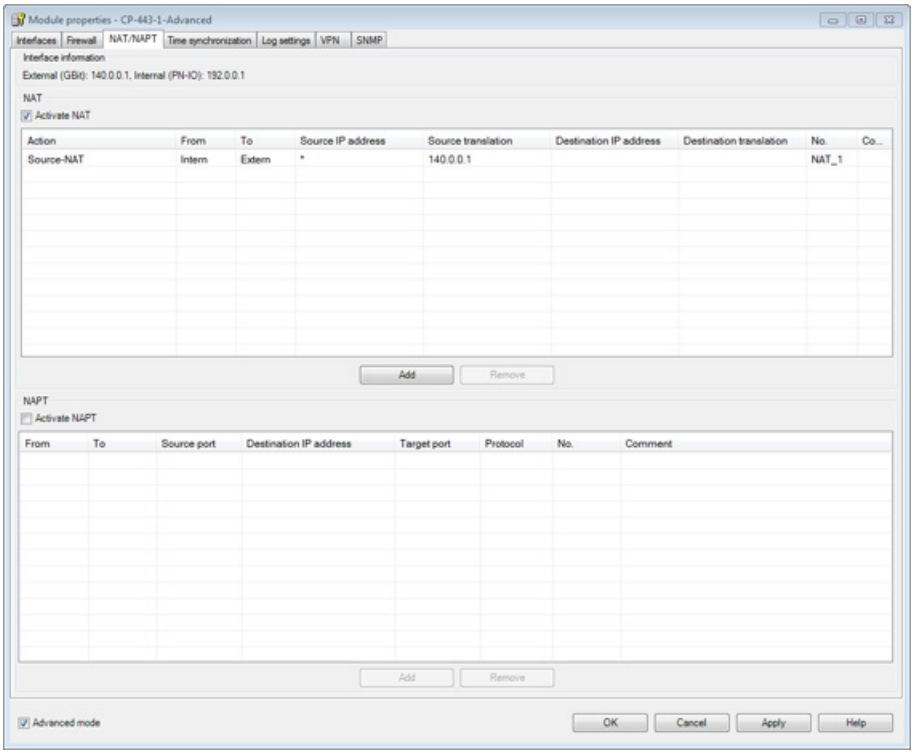
5.5.4 Configuring the NAT router mode

Activating NAT router mode

1. Change the configuration view to advanced mode with the menu command "View" > "Advanced mode".
2. Select the security module in the content area.
3. Select the "Edit" > "Properties..." menu command.

   Result: The "Interfaces" tab is opened.
4. Select the "NAT/NAPT" tab.

5. Select the "Activate NAT" check box.
6. Click the "Add" button in the "NAT" input area.
7. Configure the NAT rule with the following parameters:
   - Action: "Source NAT"
   - From: "Internal"
   - To: "External"
   - Source IP address: "*"
   - Source translation: "140.0.0.1"
8. Confirm with "Apply".



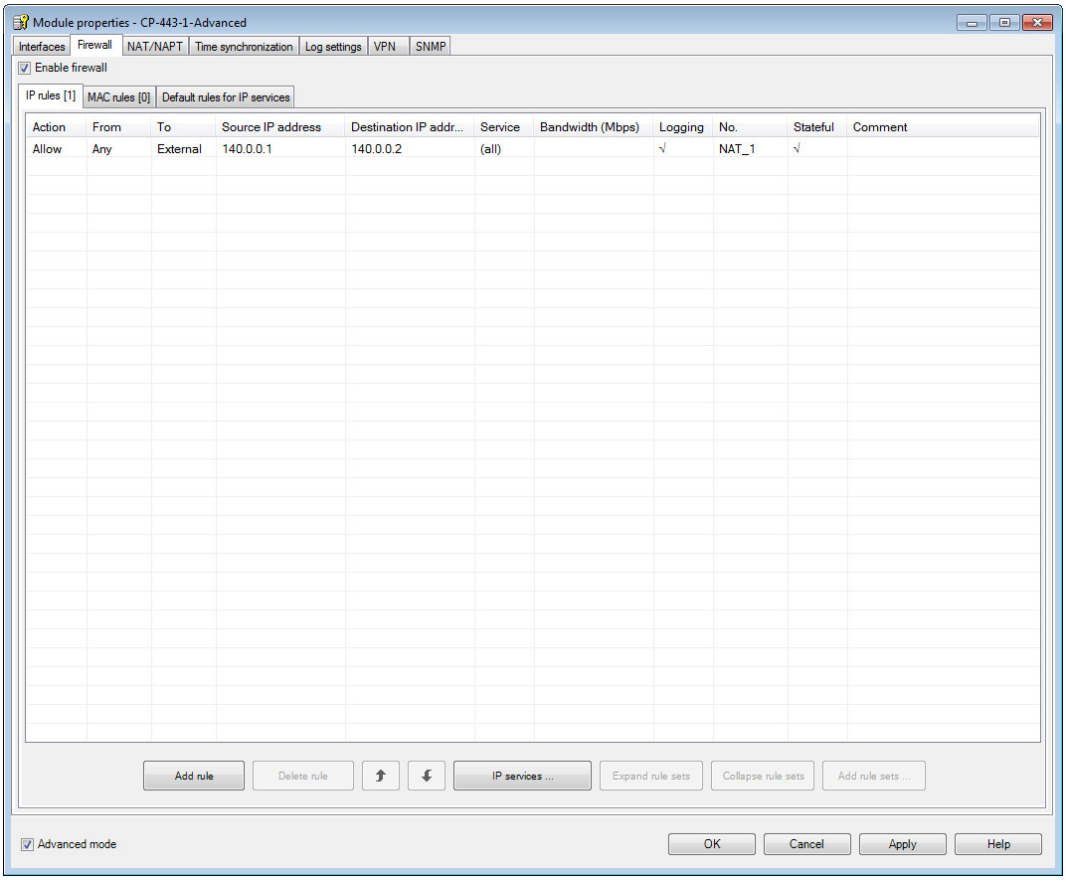
Result: SCT automatically generated a firewall rule that allows communication in the configured address translation direction. In the next step, specify this firewall rule by restricting the permitted destination IP addresses of frames to the IP address of PC1.

5.5.5 Configure the firewall

Follow the steps below:

1. Select the "Firewall" tab.
2. Select the "Enable firewall" check box.

3. Expand the firewall rule created by SCT by the following information:
   – Destination IP address: 140.0.0.2
4. In the row of the new rule set, select the "Logging" check box. As a result, packets to which the defined rule is applied are logged.
5. Confirm with "Apply".



6. Close the dialog with "OK".

5.5.6 Downloading the configuration to the security module

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Close the Security Configuration Tool.
3. In HW Config, select the "Station" > "Save and Compile" menu.
4. Download the new configuration to the security module using the "PLC" > "Download to Module ..." menu.

If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.

Result: Security module in productive mode

The commissioning of the configuration is complete. The security module protects the internal network (PC2). Outgoing IP traffic from the internal network to PC1 is allowed.

5.5.7 Testing NAT router functionality and logging data traffic

How can you test the configured function?

The function can be tested as described below using a ping command. To be able to recognize the effects of the NAT router mode, use the packet filter logging.

Note on the ping command: As an alternative, you can also use other communication programs to test the configuration.

Note

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

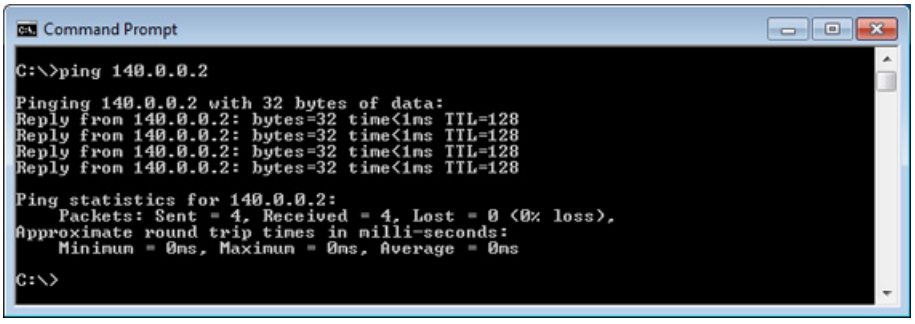
Test part 1 - sending the ping command

Now test the function of the NAT router mode in IP data traffic from the internal to the external network as follows:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the Ping command from PC2 to PC1 (IP address 140.0.0.2)

   In the command line of the "Command Prompt" window, enter the command "ping 140.0.0.2" at the cursor position.

   You will then receive the following message (positive reply from PC1):



Result

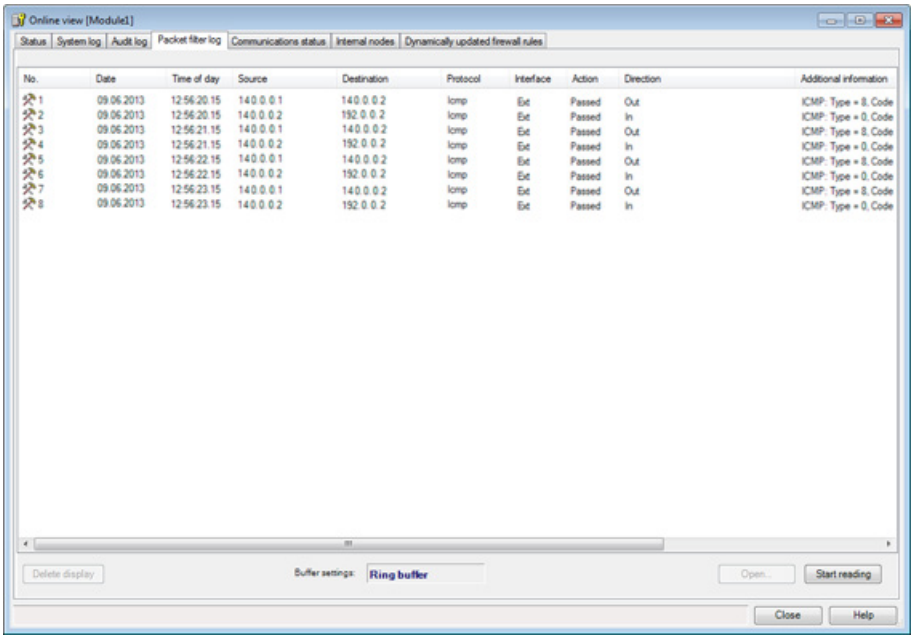
If the IP packets have reached PC1, the "Ping statistics for 140.0.0.2" display the following:

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

Test part 2 - evaluating the result

1. Change to online mode in the Security Configuration Tool with the "View" > "Online" menu command.
2. Select the security module you want to edit and then select the menu command "Edit" > "Online diagnostics" to open the online dialog.
3. Select the "Packet filter log" tab.
4. Click the "Start reading" button.
5. Acknowledge the displayed dialog with "OK".

   Result: The log entries are read from the security module and displayed here.



Result

You will see the following in the log output:

- Output row 1

  The IP addresses of the packets from PC2 to PC1 are displayed on the interface to the external network with the external IP address of the security module (140.0.0.1). This corresponds to the expected address translation (the additional port assignment is not visible here).

- Output row 2

  The reply packets are displayed with the destination address of the node in the internal subnet (PC2: 192.0.0.2).

- The following output rows accordingly

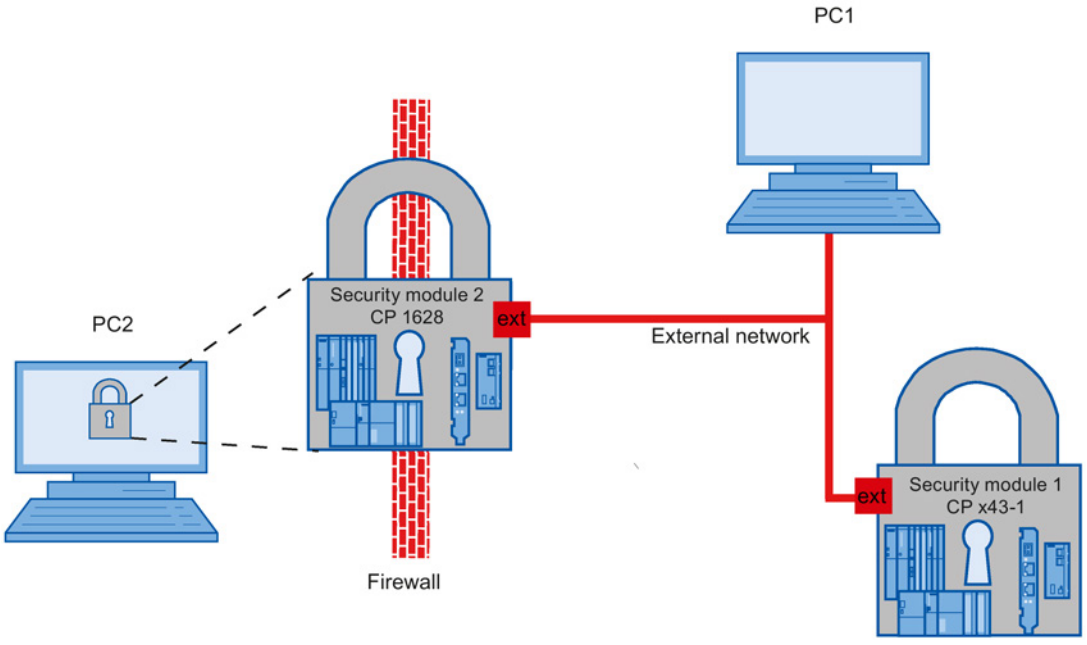
5.6 Example with a CP 1628 and CP x43-1 Adv.

5.6.1 Overview

In this example, configuration is in the "Advanced mode" configuration view.

With this configuration, you have the situation that all the frames sent by the PC2 node to security module 1 and vice versa are allowed to pass the firewall. In addition to this, PC1 is allowed to access PC2 and security module 1.

Setting up the test network



- Security module 1: CP x43-1 Advanced
- PC1: PC with the Security Configuration Tool and STEP 7
- PC2 with security module 2: PC with CP 1628

Requirement:

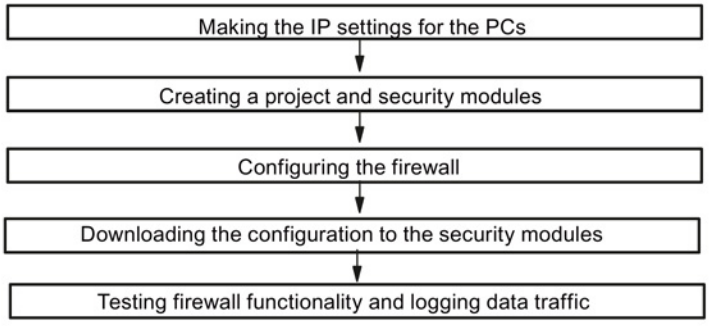
To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software is installed on PC1.
- STEP 7 is installed on PC1 and a STEP 7 project has already been created.
- In the STEP 7 project, a specified TCP/IP S7 connection between the CP 1628 (PC2) and CP x43-1 has been created. The CP 1628 is the active node.

- CP 1628 has the following settings in STEP 7:
  - IP address Industrial Ethernet: 192.168.0.5, subnet mask: 255.255.255.0

    The NDIS IP address is set up in the IP settings of the PC.
- CP x43-1 Adv. has the following settings in STEP 7:
  - Gigabit IP address: 192.168.0.11, subnet mask: 255.255.255.0
  - PROFINET IP address: 192.168.1.11, subnet mask: 255.255.255.0

Overview of the next steps:



5.6.2 Make the IP settings for the PCs

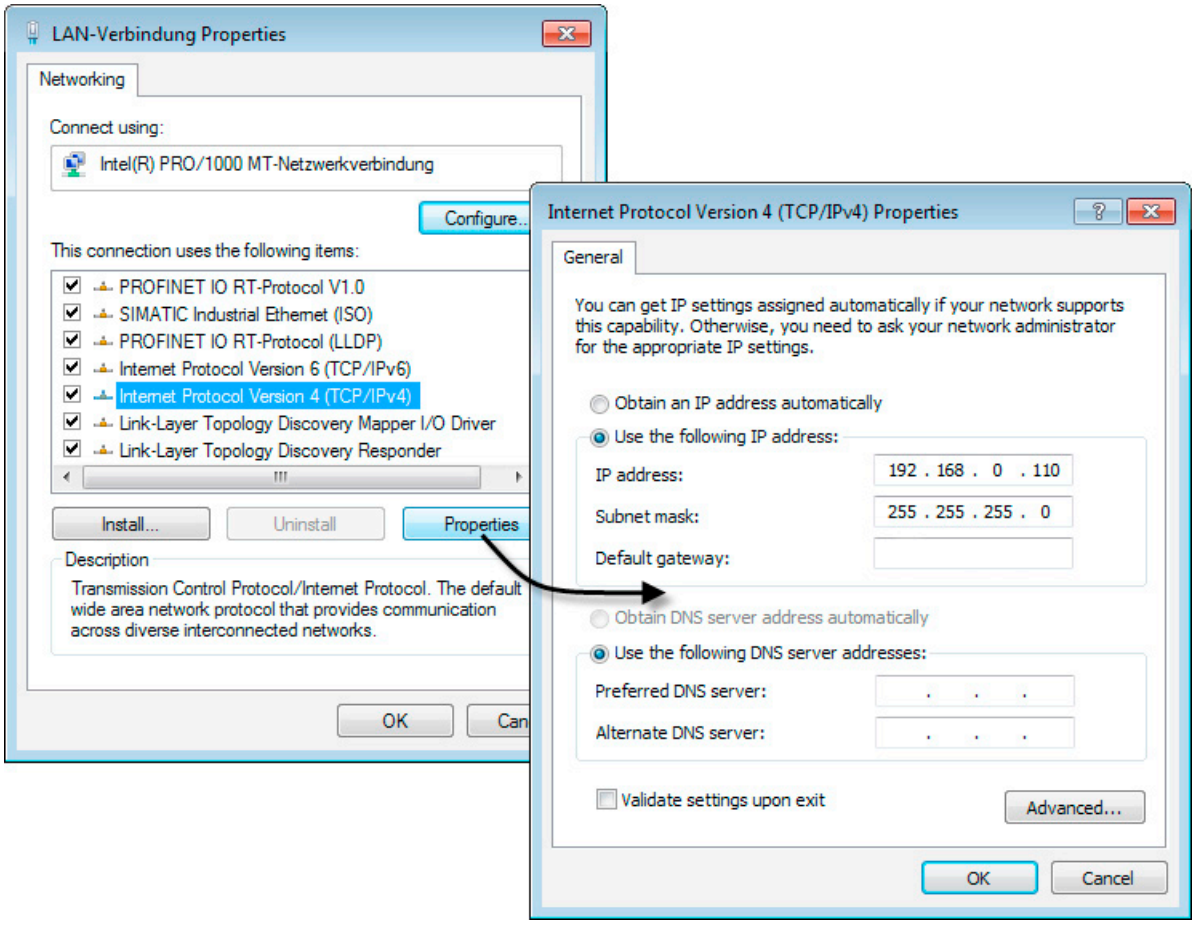
For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask
PC1	192.168.0.110	255.255.255.0
PC2	NDIS: 192.168.0.105	255.255.255.0

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

5.6.3 Creating a project and security modules

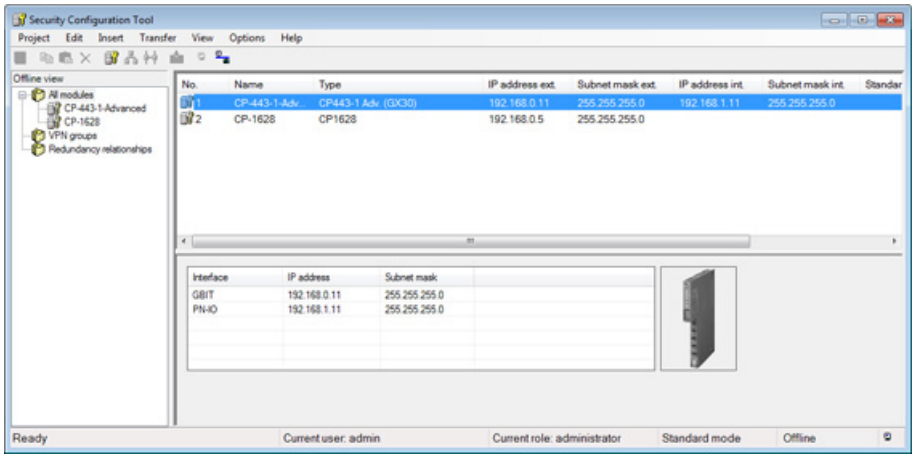
Follow the steps below:

1. In the "Security" tab of the object properties of the CP 1628, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new security project is created.

3. Change to the object properties of the CP x43-1 Adv. and select the "Enable security" check box on the "Security" tab.
4. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.

Result: The security modules will then be displayed in the list of configured modules.

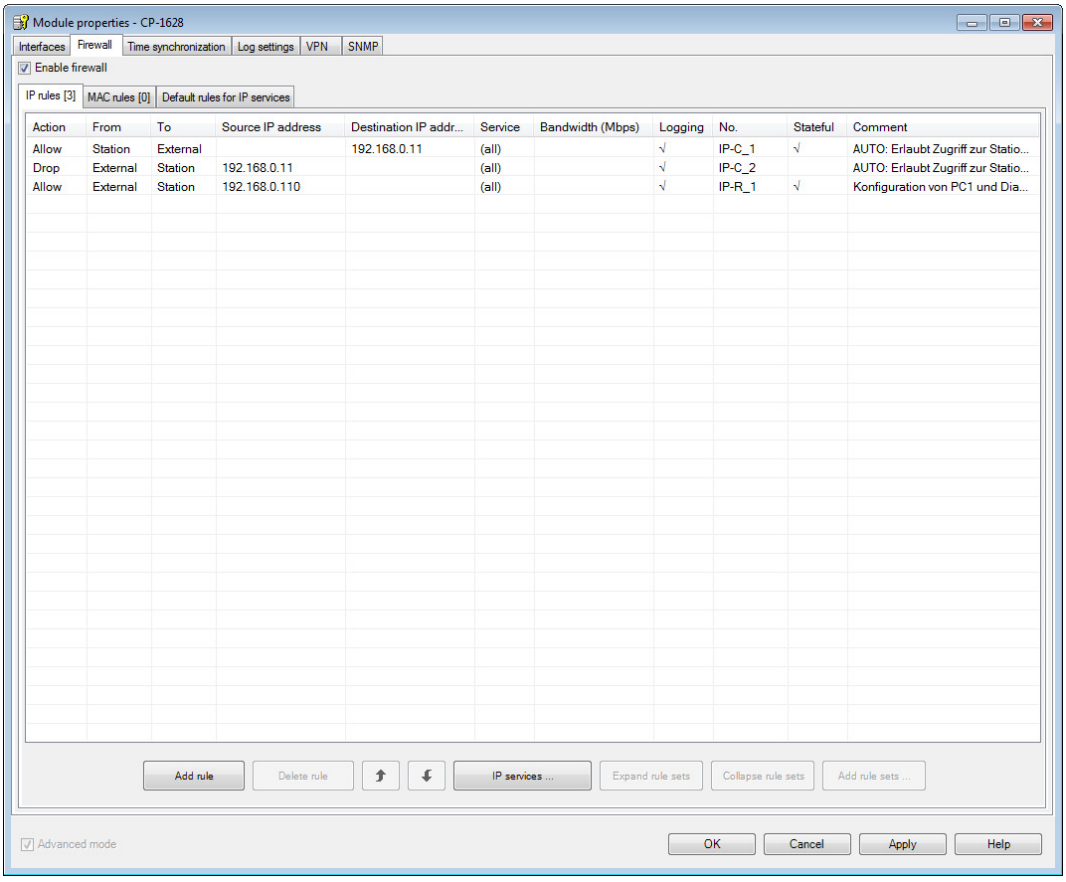


5.6.4 Configure the firewall

Defining a firewall rule for the CP 1628

1. Change the configuration view to advanced mode with the menu command "View" > "Advanced mode".
2. Select the security module of the type "CP 1628" in the content area.
3. Select the "Edit" > "Properties..." menu command.
4. Select the "Firewall" tab in the displayed dialog.
5. Select the "Enable firewall" check box.

6. Click the "Add rule" button and enter the firewall rule in the third row as shown below. The first two rules are created automatically for the configured connection.

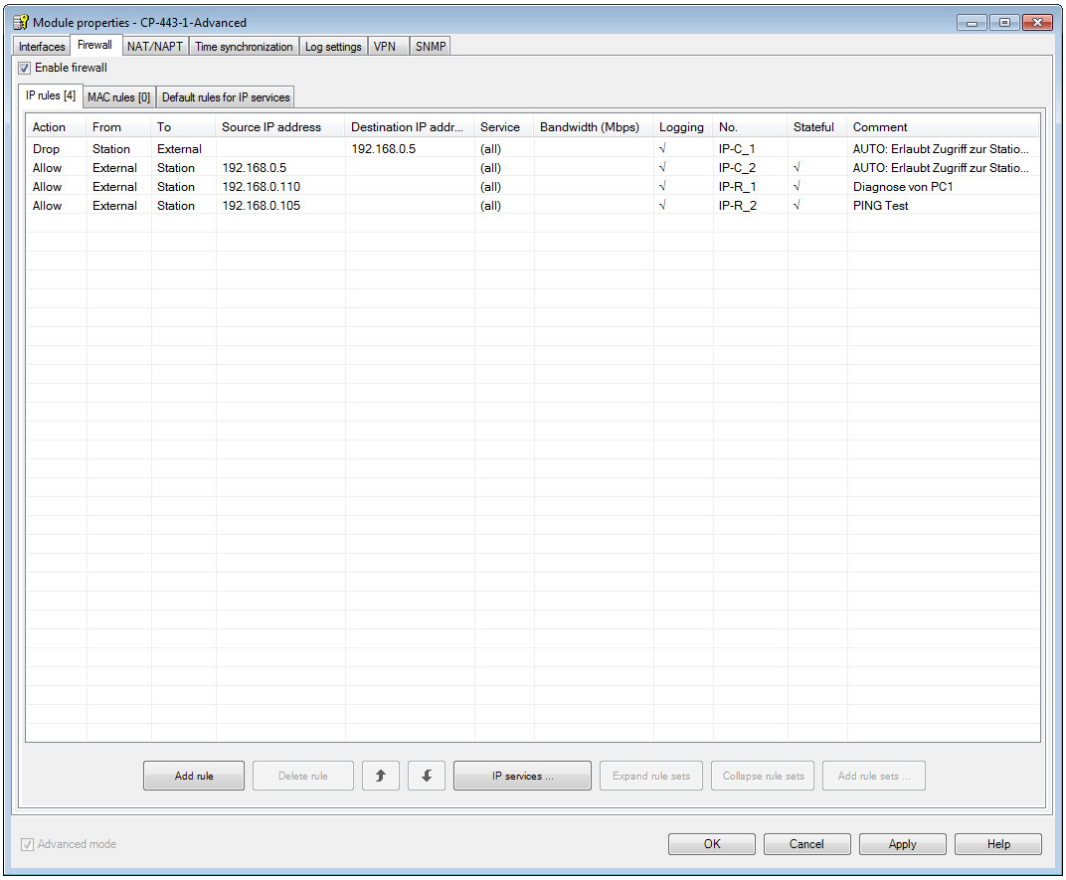


7. Close the dialog with "OK".

Defining a firewall rule for the CP x43-1 Advanced

1. Select the security module of the type "CP443-1 Adv. (GX30)" or "CP343-1 Adv. (GX31)" in the content area.
2. Select the "Edit" > "Properties..." menu command.
3. Select the "Firewall" tab in the displayed dialog.

4. Select the "Enable firewall" check box.
5. Click the "Add rule" button and enter the firewall rules in the third and fourth row as shown below. The first two rules are created automatically for the configured connection.



Result: The offline configuration is complete.

Note: In this example, full access by network nodes or to network nodes without filtering at port level is described. An example of creating highly specific firewall rules can be found in the following section:

Configuring a firewall (Page 67)

For more detailed information, refer to the configuration manual "SIMATIC NET Industrial Ethernet Security - Basics and Application".

5.6.5 Downloading the configuration to the security modules

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Close the Security Configuration Tool.
3. In HW Config, select the "Station" > "Save and Compile" menu for the first CP.

4. Download the new configuration to the security module using the "PLC" > "Download to Module..." menu.
5. Perform steps 3-4 for the second CP.

If the download was completed free of errors, the security modules restart automatically and the new configuration is activated.

Result: Security modules in productive mode

The commissioning of the configuration is complete. The security module 2 protects PC2. Outgoing IP traffic from the CP 1628 (security module 2) to the CP x43-1 Adv. (security module 1) is permitted.

5.6.6 Testing firewall functionality and logging data traffic

How can you test the configured function?

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

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

Note

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

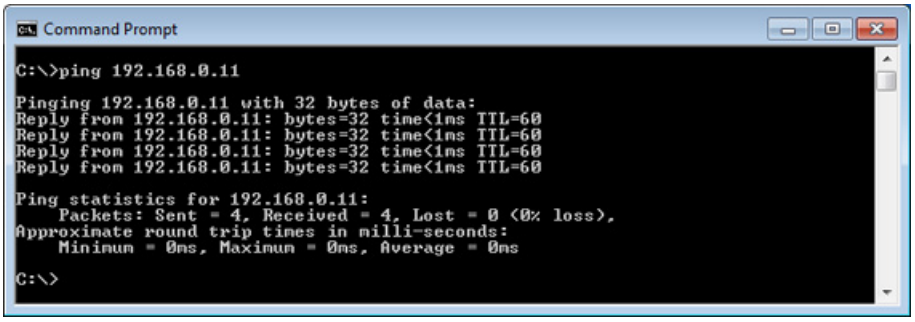
Test phase 1

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

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to the CP x43-1 Adv. (IP address 192.168.0.11)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.0.11" at the cursor position.

   You will then receive the following message (positive reply from CP x43-1 Adv.):



Result

If the IP packets have reached the CP x43-1Adv., the "Ping statistics" for 192.168.0.11 display the following:

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

The ping packets were able to reach the CP x43-1 Adv. due to the configuration of PC2. The CP x43-1 Adv. has replied to the ping packets. Due to the "stateful inspection" function of the firewall, the reply frames arriving from the CP x43-1 Adv. are allowed to PC2.

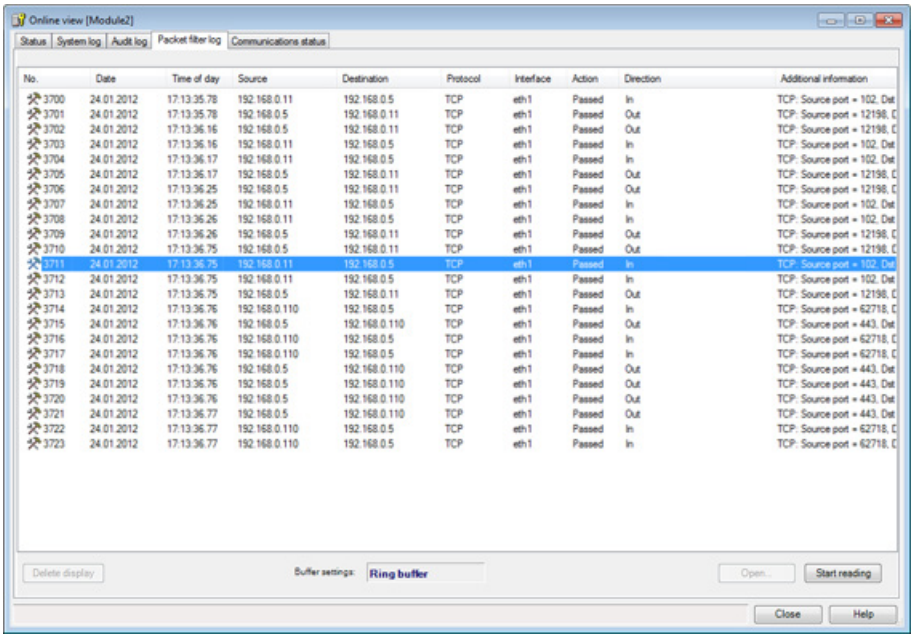
Test part 2 - evaluating the result

1. Change to online mode in the Security Configuration Tool with the "View" > "Online" menu command.
2. Select the module of the type "CP1628" and then select the menu command "Edit" > "Online diagnostics" to open the online dialog.
3. Select the "Packet filter log" tab.
4. Click the "Start reading" button.
5. Acknowledge the displayed dialog with "OK".

   Result: The log entries are read from the security module and displayed here.

Result

In the output rows of the logging, you can recognize frames that have passed through the firewall due to the configured firewall rules:



Configuring a VPN tunnel

6

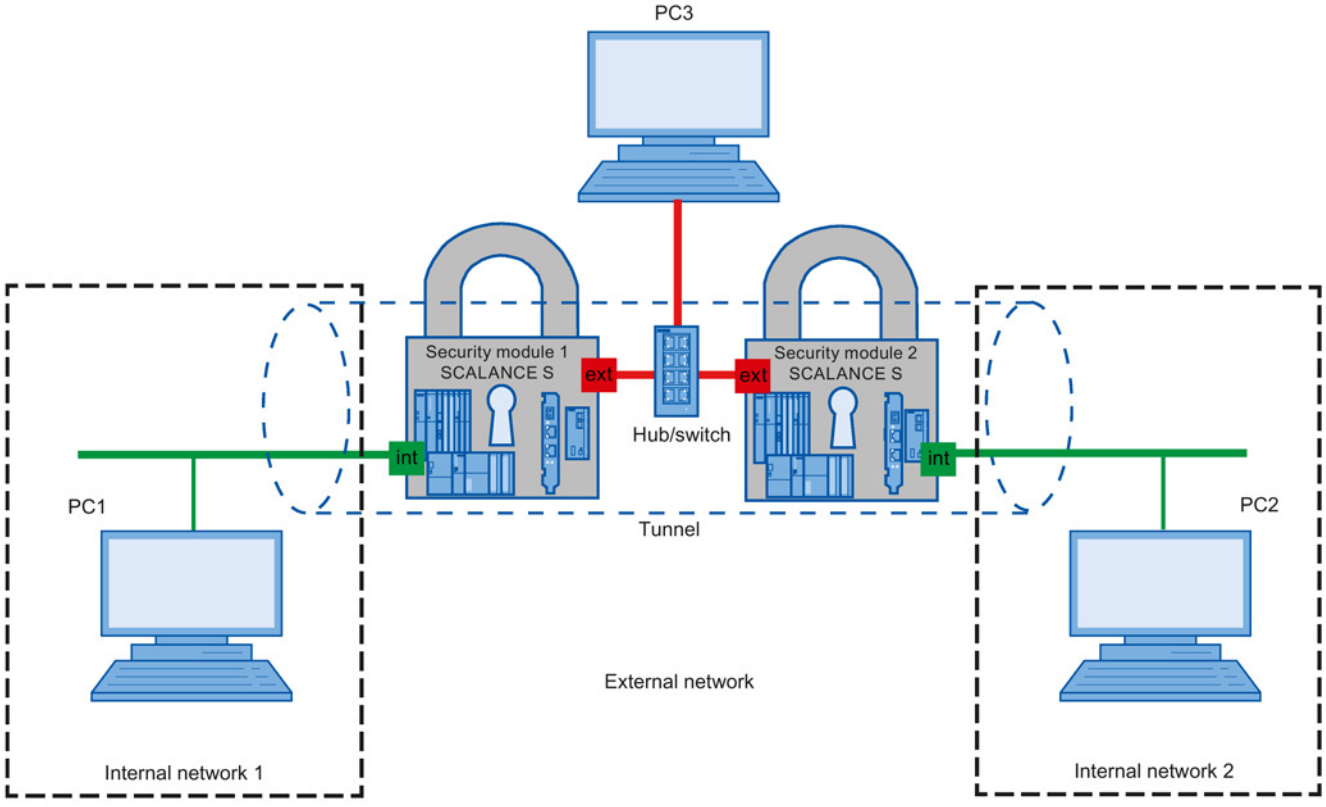
6.1 VPN tunnel between SCALANCE S and SCALANCE S

6.1.1 Overview

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

With this configuration, IP traffic and layer 2 traffic (bridge mode only) is possible only over the established tunnel connections with authorized partners.

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the security module.

  – PC1: Represents a node in internal network 1

  – PC2: Represents a node in internal network 2
- Security module 1: SCALANCE S module (not S602) for protection of internal network 1
- Security module 2: SCALANCE S module (not S602) for protection of internal network 2
- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

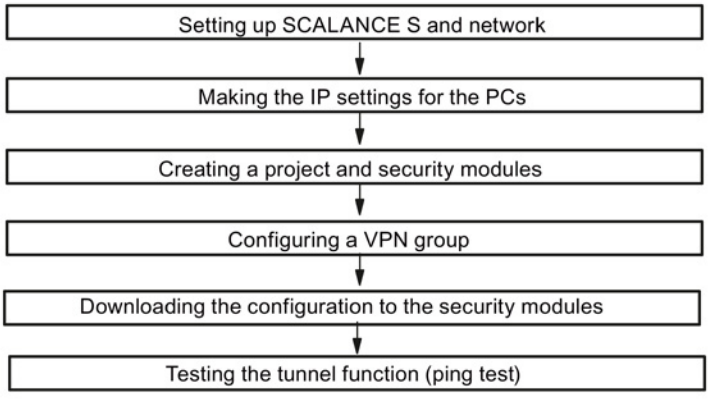
  PC3: PC with the Security Configuration Tool

Required devices/components:

Use the following components to set up the network:

- 2 x SCALANCE S modules (not S602), (optional: one or two suitably installed standard rails with fittings);
- 1 x or 2 x 24 V power supplies with cable connections and terminal block plugs (both modules can also be operated from a common power supply);
- 1 x PC on which the "Security Configuration Tool" is installed;
- 2 x PCs in the internal networks to test the configuration;
- 1 x network hub or switch to set up the network connections with the two security modules and the PCs/PGs;
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

Overview of the next steps:



6.1.2 Set up SCALANCE S and the network

Follow the steps outlined below:

1. First unpack the SCALANCE S devices and check that they are undamaged.
2. Connect the power supply to the SCALANCE S devices.

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

WARNING

Use safety extra-low voltage only

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

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

1. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   - Connect PC1 to the internal interface of security module 1 and PC2 to the internal interface of security module 2.
   - Connect the external interface of security module 1 and the external interface of security module 2 to the hub/switch.
   - Connect PC3 to the hub/switch as well.
2. Now turn on the PCs.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;

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

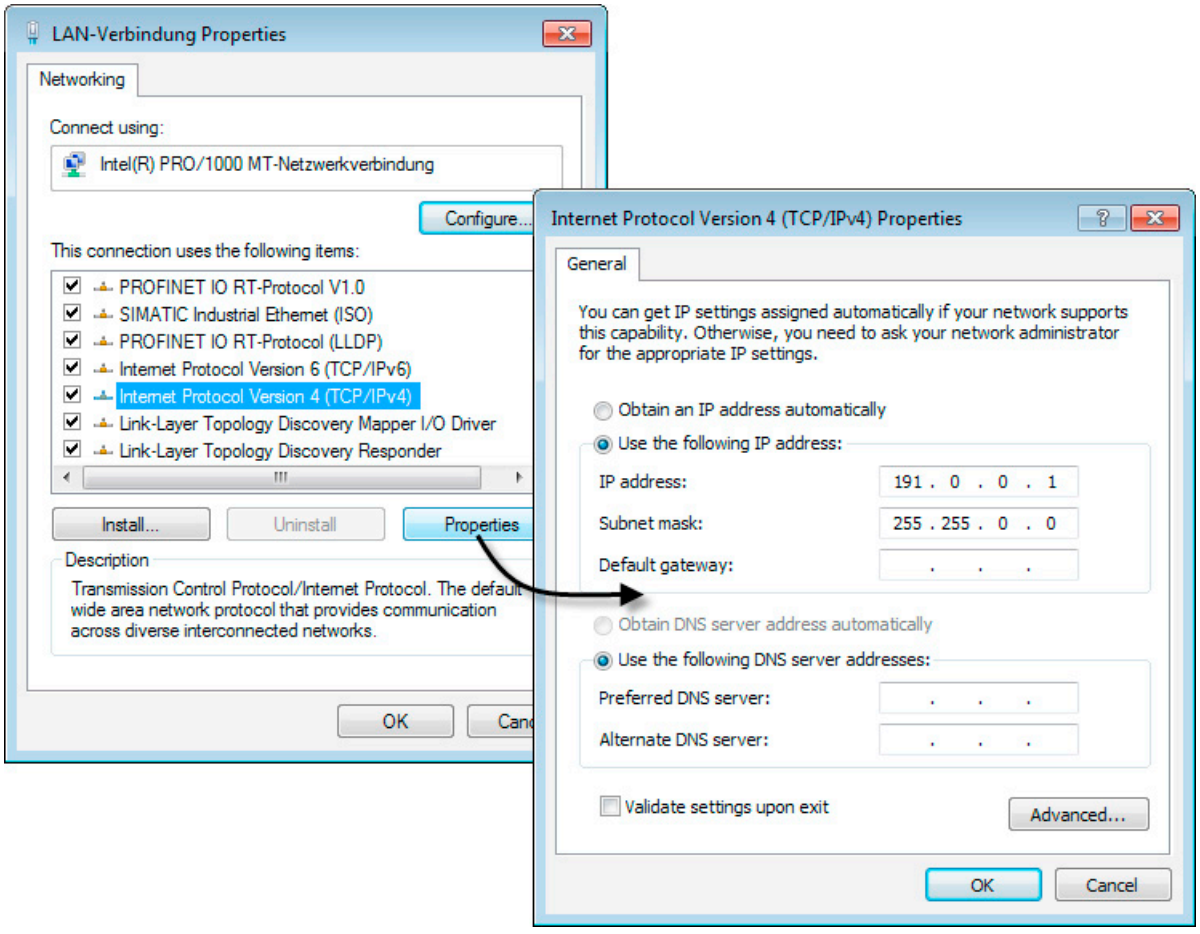
6.1.3 Make the IP settings for the PCs

For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask
PC1	191.0.0.1	255.255.0.0
PC2	191.0.0.2	255.255.0.0
PC3	191.0.0.3	255.255.0.0

Follow the steps below for PC1, PC2, and PC3:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

6.1.4 Creating a project and security modules

Follow the steps below:

1. Install and start the Security Configuration Tool on PC3.
2. Select the "Project" > "New..." menu command.
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

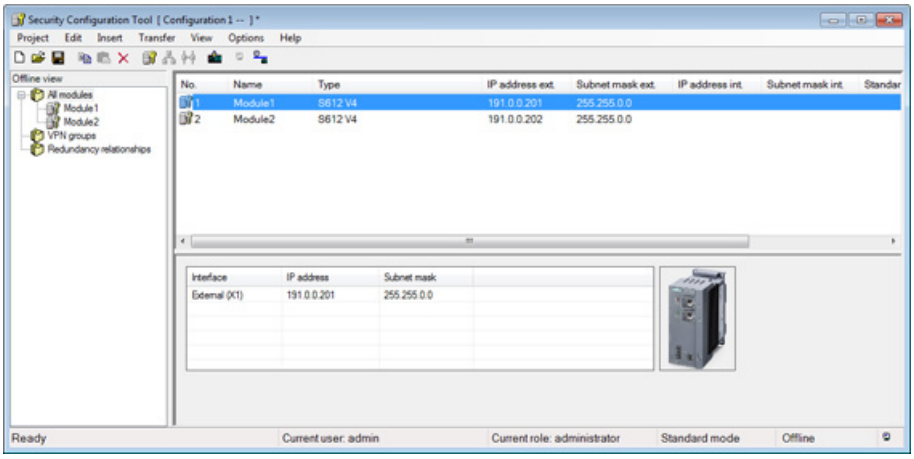
   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.
4. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module: S612
   - Firmware release: V4
5. In the "Configuration" area, enter the MAC address in the required format.

   The MAC address is printed on the front of the SCALANCE S module.
6. In the "Configuration" area, enter the external IP address (191.0.0.201) and the external subnet mask (255.255.0.0) in the required format and confirm the dialog with "OK".

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

   Result: The "Selection of a module or software configuration" dialog opens.

8. Repeat steps 4-6 analogously for security module 2. Assign the following address parameters to the security module:
   - IP address (ext.): 191.0.0.202
   - Subnet mask (ext.): 255.255.0.0



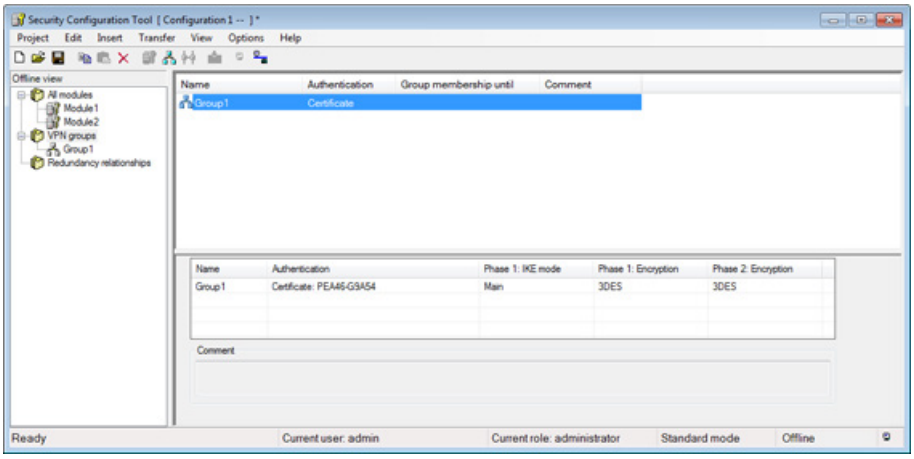
6.1.5 Configuring VPN group

Two security modules can establish an IPsec tunnel for secure communication if they are assigned to the same VPN group in the project.

Follow the steps outlined below:

1. Select the "VPN groups" object in the navigation panel and select the "Insert" > "Group" menu command.

   Result: An VPN group is created The VPN group is automatically given the name "Group1".



2. Select the "All modules" entry in the navigation panel.
3. Select the first security module in the content area and drag it to the VPN group "Group1" in the navigation panel.

   The security module is now assigned to this VPN group.

   The color of the key symbol changes from gray to blue.
4. Select the second security module in the content area and drag it to the VPN group "Group1" in the navigation panel.

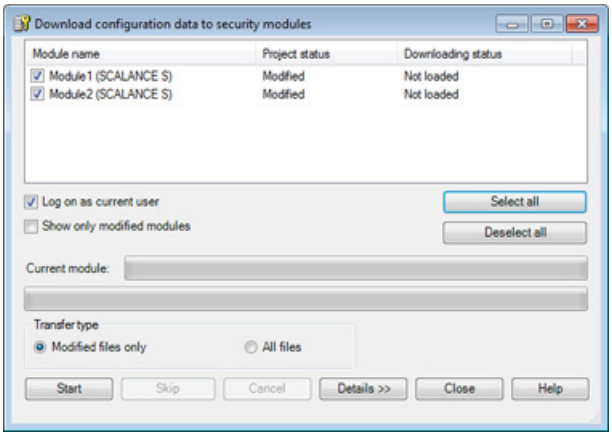
   The security module is now also assigned to this VPN group.
5. Save the project with the "Project" > "Save" menu command.

The configuration of the tunnel connection is complete.

6.1.6 Downloading the configuration to the security modules

Follow the steps below:

1. In the Security Configuration Tool on PC3, select the menu command "Transfer" > "To all modules..." to open the following dialog:



2. Select the two modules using the "Select all" button.
3. Start the download with the "Start" button.

   If the download was completed free of errors, the security modules are restarted automatically and the new configuration activated.

Result: SCALANCE S modules in productive operation

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

The commissioning of the configuration is now complete and the two SCALANCE S modules can establish a communications tunnel via which network nodes from the two internal networks can communicate.

6.1.7 Test the tunnel function (ping test)

How can you test the configured function?

The function can be tested as described below using a ping command. As an alternative, you can also use other communication programs to test the configuration.

Note

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

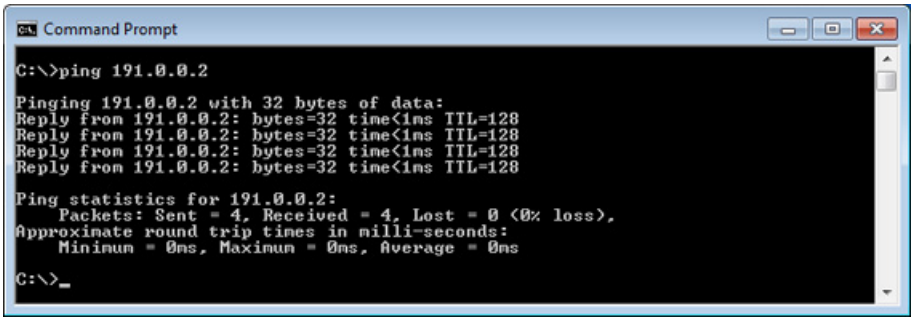
Test phase 1

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

1. On PC1, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the Ping command from PC1 to PC2 (IP address 191.0.0.2)

   In the command line of the "Command Prompt" window, enter the command "ping 191.0.0.2" at the cursor position.

   You will then receive the following message (positive reply from PC2):



Result

If the IP packets have reached PC2, the "Ping statistics for 191.0.0.2" display the following:

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

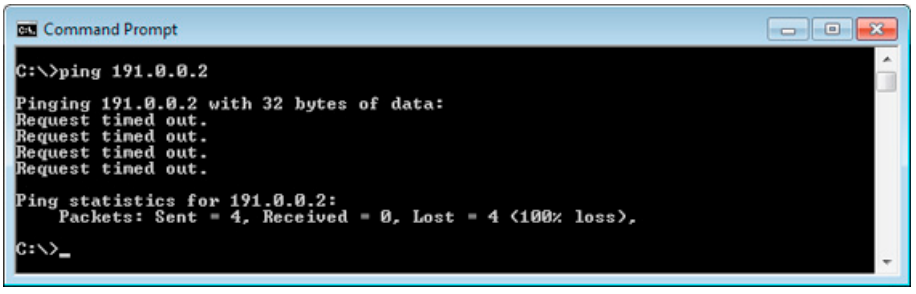
Since no other communication is permitted, these packets must have been transported through the VPN tunnel.

Test phase 2

Repeat the test by sending a ping command from PC3.

1. On PC3, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Send the same ping command ("ping 191.0.0.2") in the Command Prompt window of PC3.

   You will then receive the following message (no reply from PC2):



Result

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

This is shown in the "Ping statistics" for 191.0.0.2 as follows:

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

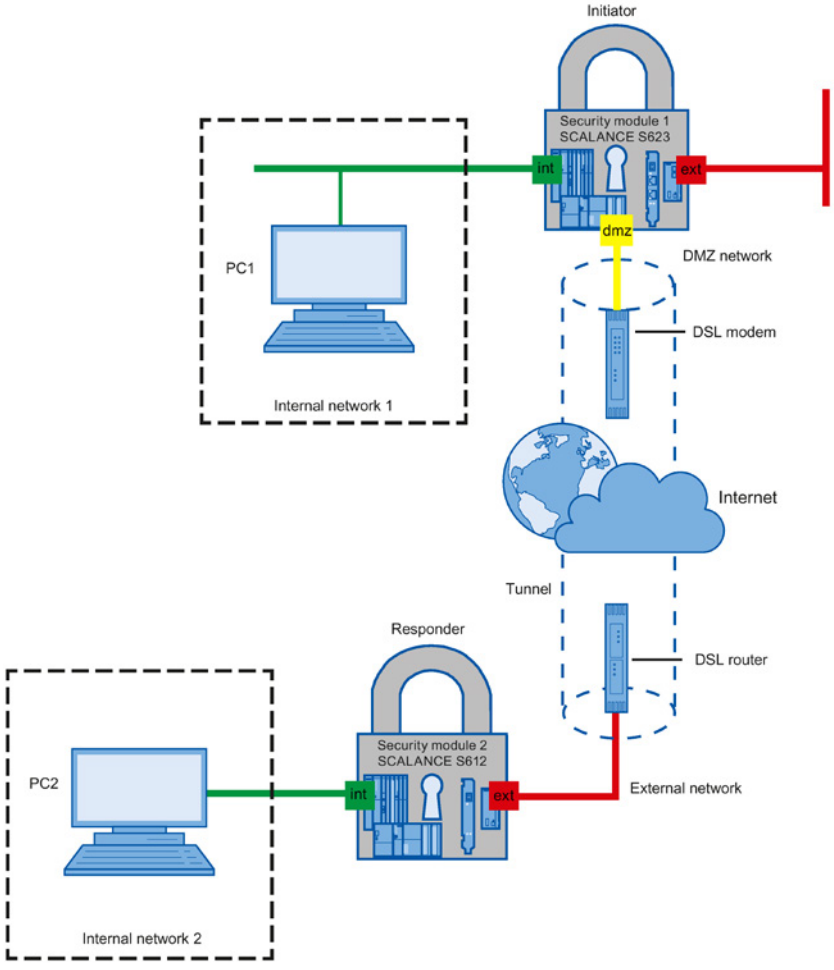
6.2 VPN tunnel between SCALANCE S623 and SCALANCE S612

6.2.1 Overview

In this example, the security modules SCALANCE S623 and SCALANCE S612 are the endpoints of a VPN tunnel that is used to establish secure communication via the Internet. In this case, the VPN tunnel is set up between the remote maintenance interface (DMZ interface) of the SCALANCE S623 module and the external interface of the SCALANCE S612 module. The remote maintenance interface of the SCALANCE S623 obtains its IP address via PPPoE. In this configuration, the SCALANCE S623 module is the VPN initiator whereas the SCALANCE S612 module represents the VPN responder.

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

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  Both internal networks include a PC connected to the internal interface of the corresponding security module.

  – PC1: Represents a node in internal network 1

  – PC2: Represents a node in internal network 2
- Security module 1: SCALANCE S623 module for protection of internal network 1
- Security module 2: SCALANCE S612 module for protection of internal network 2
- DMZ network or external network

  Access to the Internet is via DSL modem or DSL router attached to the DMZ interface of security module 1 or the external interface of security module 2. The VPN tunnel ensures secure communication between PC1 and PC2 via the Internet.

Required devices/components:

Use the following components to set up the network:

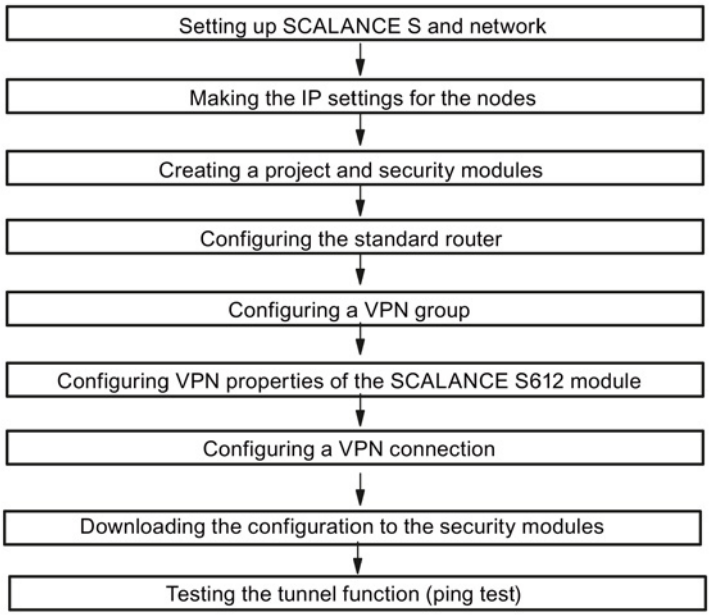
- 1 x SCALANCE S623 (additional option: a suitably installed DIN rail with fittings);
- 1 x SCALANCE S612 (additional option: a suitably installed DIN rail with fittings);
- 1 x or 2 x 24 V power supplies with cable connections and terminal block plugs (both modules can also be operated from a common power supply);
- 2 x PC on which the "Security Configuration Tool" is installed;
- 1x DSL modem (connection to the Internet for PC1)
- 1x DSL router (connection to the Internet for PC2)

  Note: The DSL connection on which the DSL router is operated must have a static IP address.
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

Requirement:

- For the DSL router, port forwarding must be configured so that incoming packets to port numbers UDP 500 or UDP 4500 are forwarded to the IP address configured for the external interface of security module 2.

Overview of the next steps:



6.2.2 Setting up SCALANCE S and network

Follow the steps outlined below:

1. First unpack the SCALANCE S devices and check that they are undamaged.
2. Connect the power supply to the SCALANCE S devices.

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

⚠ WARNING
Use safety extra-low voltage only The SCALANCE S is designed for operation with safety extra-low voltage. This means that only safety extra-low voltages (SELV) complying with IEC950/EN60950/ VDE0805 can be connected to the power supply terminals. The power supply unit to supply the SCALANCE S must comply with NEC Class 2 (voltage range 18 - 32 V, current requirement approx. 250 mA).

3. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   - Connect PC1 to the internal interface of security module 1 and PC2 to the internal interface of security module 2.
   - Connect the DMZ interface of security module 1 with the DSL modem.
   - Connect the external interface of security module 2 with the DSL modem.
4. Now turn on the PCs.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;
- Interface X3 - DMZ port (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.

6.2.3 Making the IP settings for the nodes

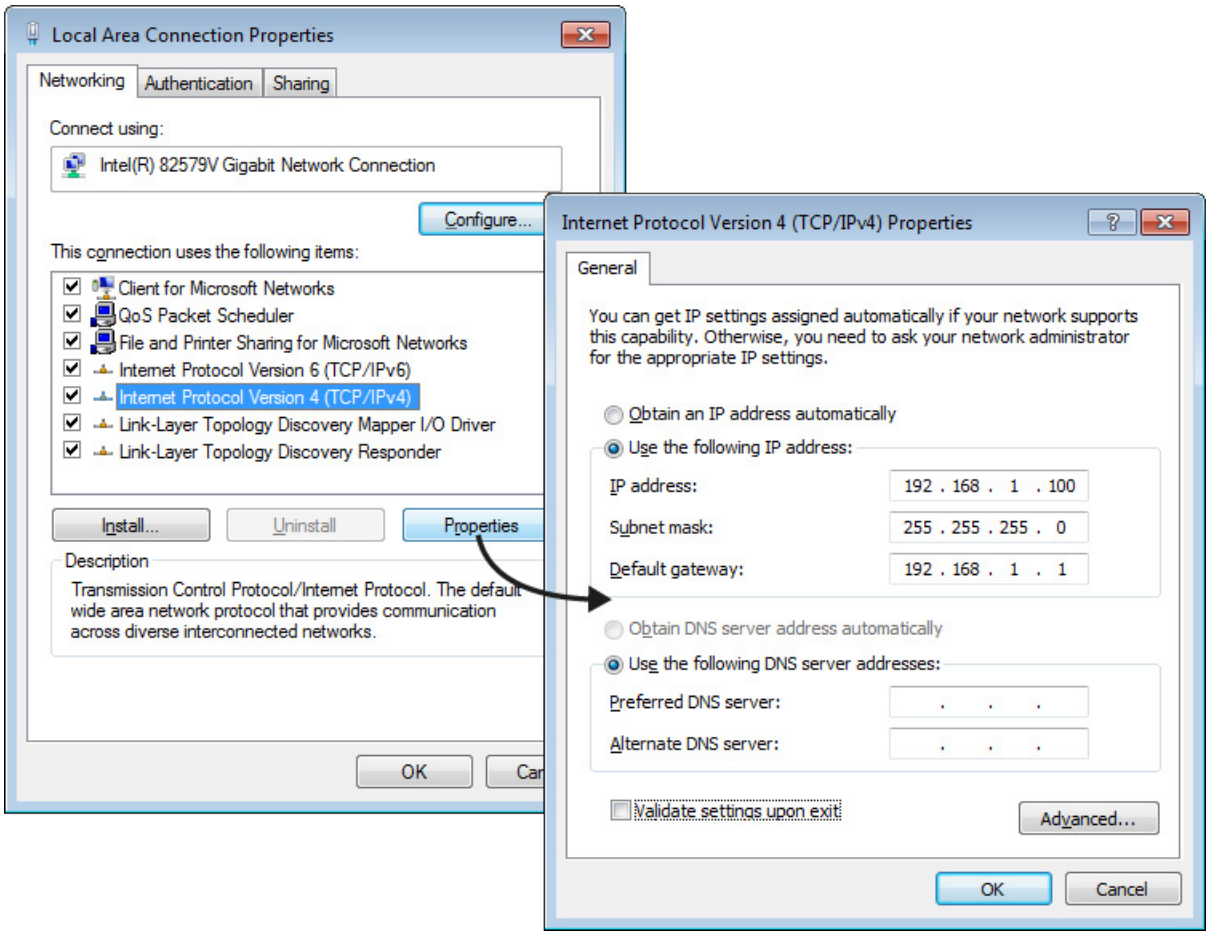
For the test, the PCs and the DSL router are given the following IP address settings: The default gateways must correspond to the configured IP addresses of the interfaces to which the PC is connected.

PC	IP address	Subnet mask	Default gateway
PC1	192.168.1.100	255.255.255.0	192.168.1.1
PC2	192.168.5.100	255.255.255.0	192.168.5.1
DSL router	192.168.8.100	255.255.255.0	-

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.

5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.



6. Enter the values assigned to the PC in the relevant boxes from the table "Making the IP settings for the nodes".
7. Close the dialogs with "OK" and close the Control Panel.

6.2.4 Creating a project and security modules

Follow the steps below:

1. Install the Security Configuration Tool on PC1 and PC2.
2. Start the Security Configuration Tool on PC1.
3. Select the "Project" > "New..." menu command.
4. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.

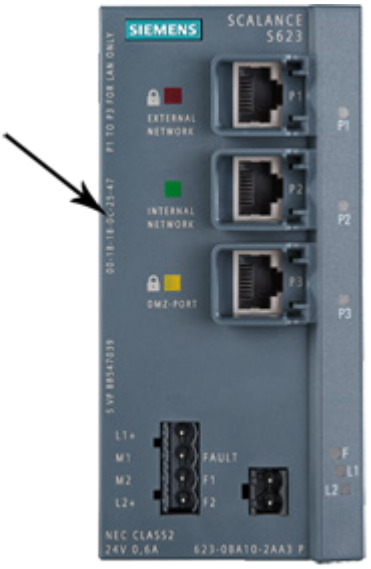
5. Confirm your entries with "OK".

   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.

6. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module: S623
   - Firmware release: V4

7. In the "Configuration" area, enter the MAC address in the required format.

   The MAC address is printed on the front of the SCALANCE S module (see figure).



8. In the "Configuration" area, enter the external IP address (192.168.2.1) and the external subnet mask (255.255.255.0) in the required format.

   Note: The IP address of the external interface is not used in this example. It is specified only to provide a full configuration of the security module.

9. From the drop-down list "Interface routing external/internal", select the "Routing mode".
10. Enter the internal IP address (192.168.1.1) and the internal subnet mask (255.255.255.0) in the required format and confirm the dialog with "OK".
11. Select the security module in the content area and select the "Edit" > "Properties..." menu command.
12. In the area "DMZ port (X3)", select the check box "Activate interface" and select the entry "PPPoE" from the "IP assignment" drop-down list.
13. Confirm with "Apply".
14. On the "Internet connection" tab, enter the data with which you authenticate yourself with your Internet Service Provider (ISP).
15. Confirm with "OK".

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

    Result: The "Selection of a module or software configuration" dialog opens.

17. In the "Product type", "Module" and "Firmware release" areas, select the following options:
    - Product type: SCALANCE S
    - Module: S612
    - Firmware release: V4

18. In the "Configuration" area, enter the MAC address in the required format.

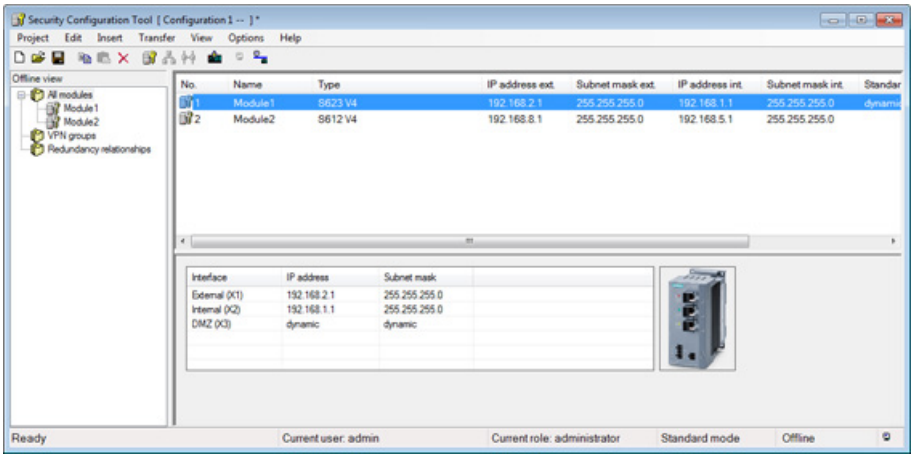
    The MAC address is printed on the front of the SCALANCE S module.

19. In the "Configuration" area, enter the external IP address (192.168.8.1) and the external subnet mask (255.255.255.0) in the required format.

20. From the drop-down list "Interface routing external/internal", select the "Routing mode".

21. Enter the internal IP address (192.168.5.1) and the internal subnet mask (255.255.255.0) in the required format and confirm the dialog with "OK".

Result: The security modules are created and are shown in the content area of the Security Configuration Tool.



6.2.5 Configuring the standard router

Follow the steps below:

1. Select the security module of the type SCALANCE S612.
2. Select the "Edit" > "Properties..." menu command, "Routing" tab.
3. As standard router, enter the IP address of the DSL router the security module is connected to (192.168.8.100).

   Note: The standard router of the SCALANCE S623 module is set by the ISP.

4. Close the dialog with "OK".

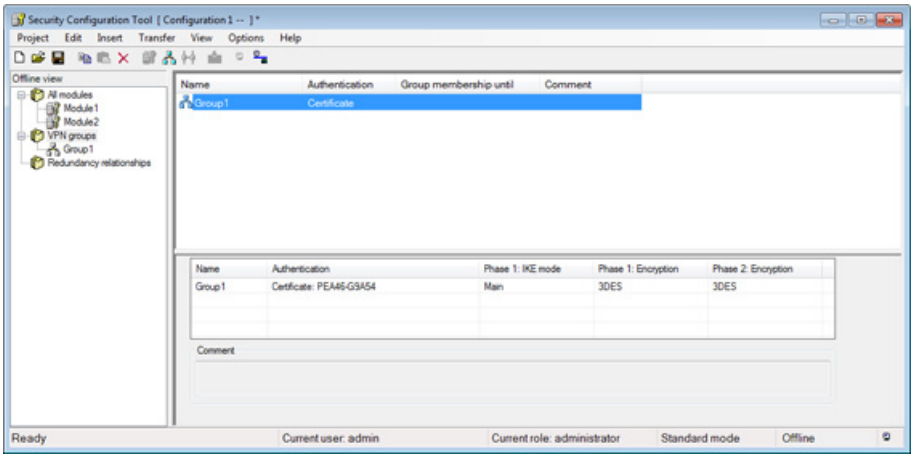
6.2.6 Configuring VPN group

Two security modules can establish an IPsec tunnel for secure communication if they are assigned to the same VPN group in the project.

Follow the steps outlined below:

1. Select the "VPN groups" object in the navigation panel and select the "Insert" > "Group" menu command.

   Result: The VPN group is created. The VPN group is automatically given the name "Group1".



2. Select the "All modules" entry in the navigation panel.
3. Select the first security module in the content area and drag it to the VPN group "Group1" in the navigation panel.

   The security module is now assigned to this VPN group.

   The color of the key symbol changes from gray to blue.
4. Select the second security module in the content area and drag it to the VPN group "Group1" in the navigation panel.

   The security module is now also assigned to this VPN group.
5. Save the project with the "Project" > "Save" menu command.

The configuration of the tunnel connection is complete.

6.2.7 Configuring VPN properties of the SCALANCE S612 module

Follow the steps below:

1. Select the security module of the type SCALANCE S612 in the content area.
2. Select the "Edit" > "Properties..." menu command, "VPN" tab.

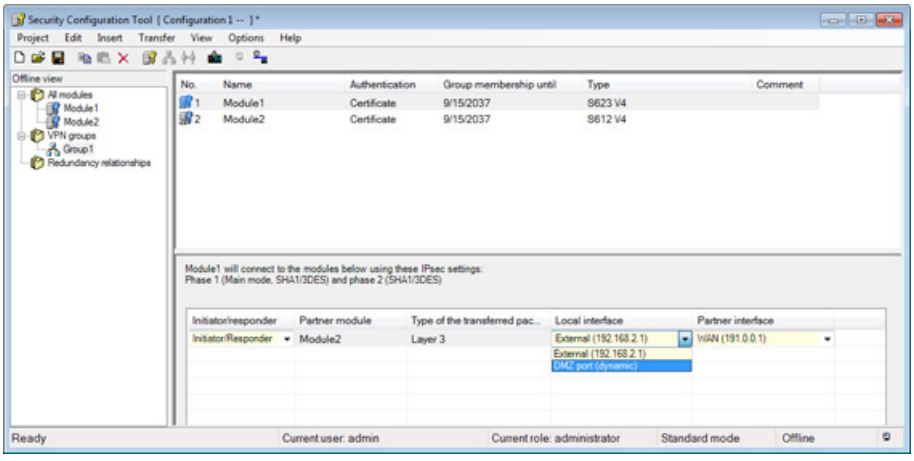
3. From the "Permission to initiate connection establishment" drop-down list, select the "Wait for partner (responder)" entry.
4. Enter the WAN IP address of the DSL router in the "WAN IP address / FQDN" input box. The WAN IP address is a static IP address set by the ISP.
5. Confirm with "OK".

6.2.8 Configuring a VPN connection

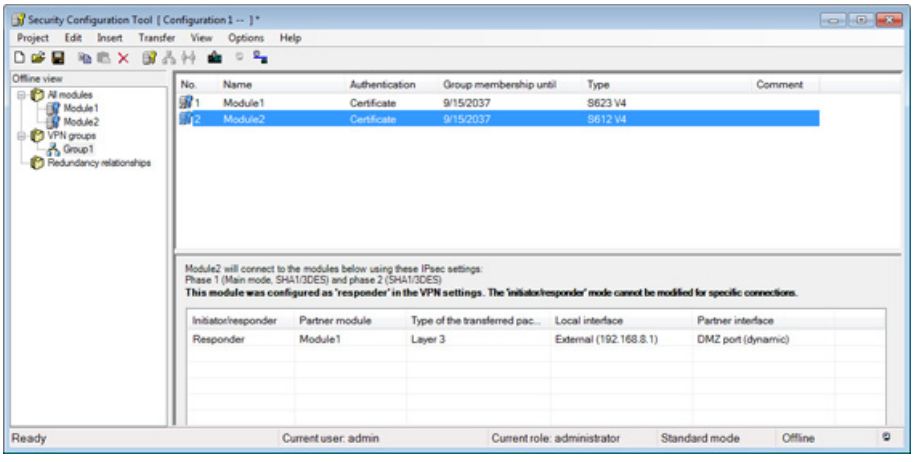
Follow the steps below:

1. Click on "Group1" under "VPN groups" in the navigation panel.
2. Select the security module of the type SCALANCE S623 in the content area.

   Result: In the Details window, details of the VPN partners are displayed.
3. Select the "DMZ port (dynamic)" as the "Local interface".



4. If you select "Module2" in the content area, the "DMZ port (dynamic) of module1 will automatically be displayed as the "Partner interface".

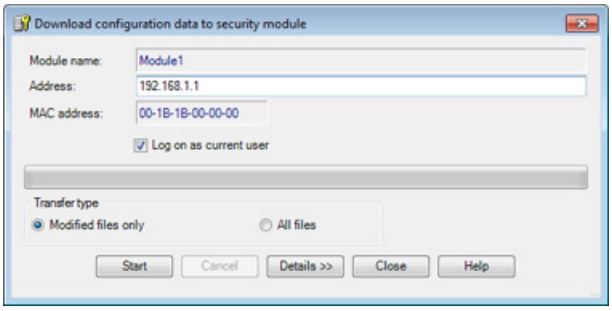


Result: The configuration of the VPN connection is complete.

6.2.9 Downloading the configuration to the security modules

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Select the security module of the type SCALANCE S623 in the Security Configuration Tool on PC1.
3. Select the "Transfer" > "To module(s)..." menu command.



4. Start the download with the "Start" button. If the download was completed free of errors, the SCALANCE S is restarted automatically and the new configuration activated.
5. Save the current project on a removable data medium and transfer the project to PC2.
6. Start the Security Configuration Tool on PC2 and open the project.
7. Repeat steps 2-4 for the security module of the type SCALANCE S612.

Result: SCALANCE S in productive operation

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

The commissioning of the configuration is now complete and the two SCALANCE S modules can establish a communications tunnel via which network nodes from the two internal networks can communicate.

6.2.10 Test the tunnel function (ping test)

How can you test the configured function?

The function can be tested as described below using a ping command. As an alternative, you can also use other communication programs to test the configuration.

Note

Firewall in Windows

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

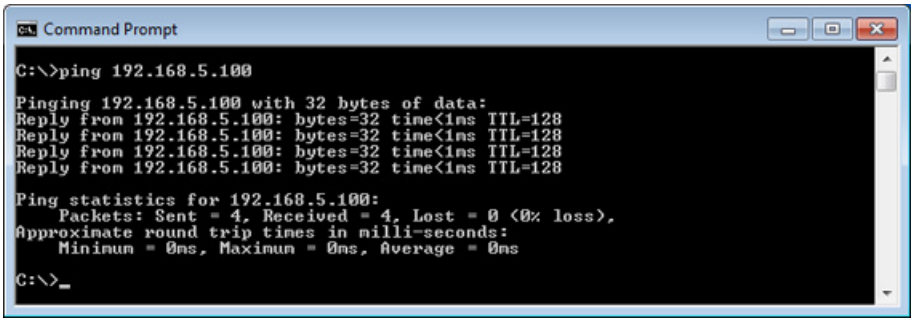
Test phase 1

Now test the function of the tunnel connection established between the security modules, as follows:

1. On PC1, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC1 to PC2 (IP address 192.168.5.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.5.100" at the cursor position.

   You will then receive the following message (positive reply from PC2):



Result

When the IP packets have reached PC2, the "Ping statistics" for 192.168.5.100 display the following:

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

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

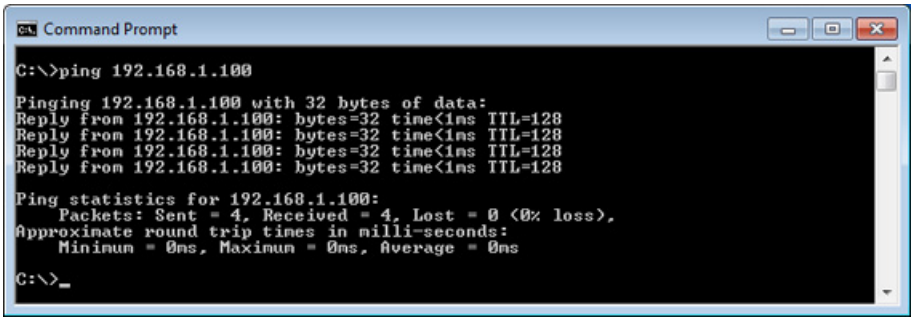
Test phase 2

Now test the function of the established tunnel connection in the opposite direction:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to PC1 (IP address 192.168.1.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.1.100" at the cursor position.

   You will then receive the following message (positive reply from PC1):



Result

If the IP packets have reached PC1, the "Ping statistics" for 192.168.1.100 display the following:

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

Communication via the configured tunnel connection works in both directions.

Note: If an on-demand connection is configured for the DSL router, 1 or 2 frames can be lost.

6.3 VPN tunnel between SCALANCE S CP

6.3.1 Overview

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

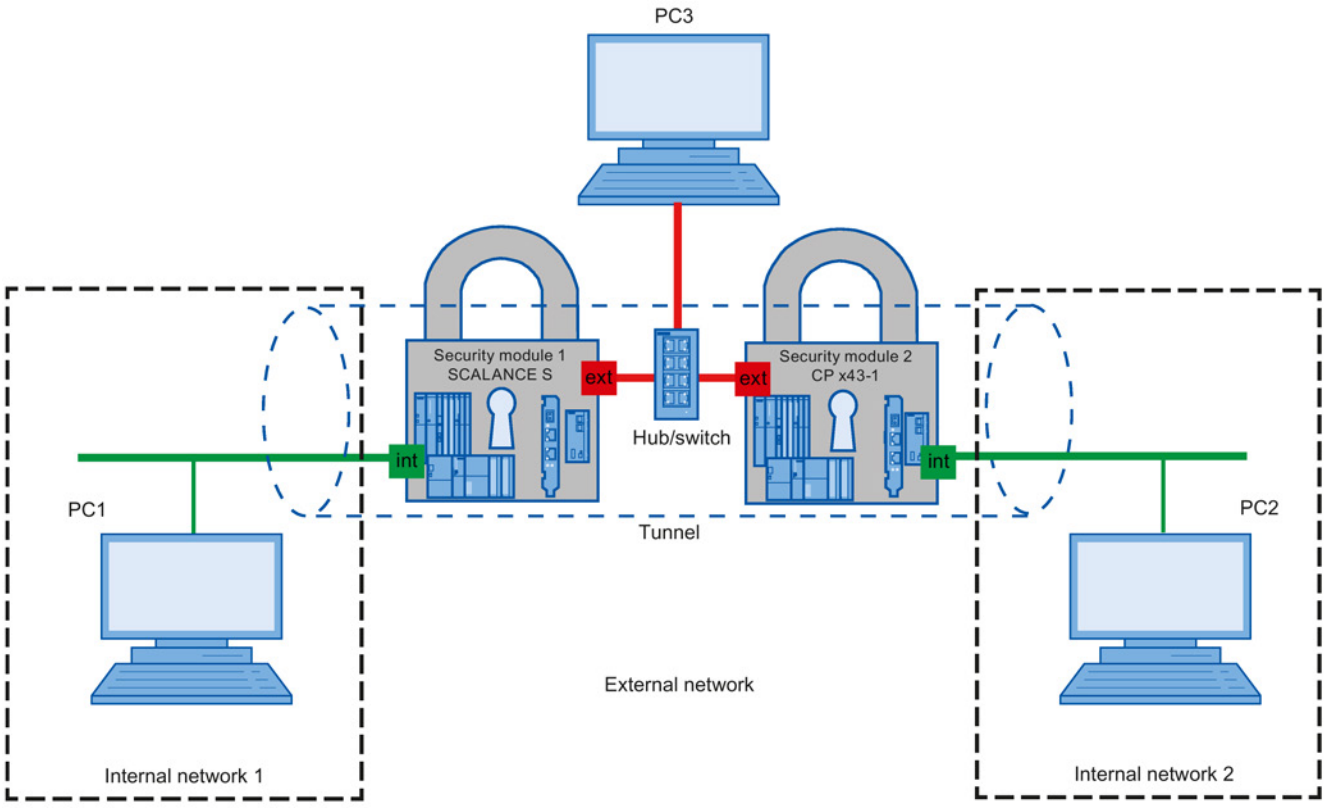
With this configuration, IP traffic is possible only over the tunnel connection with authorized partners.

Note

Please remember that after loading the configuration, your station can only be reached if the S7 protocol (TCP port 102) is allowed from "External => Station" in the firewall. Unencrypted communication from the external network should be avoided following commissioning. If you do not use secure connection establishment from the external network via VPN, you should run STEP 7 diagnostics and reconfigure only from within the internal network.

For this reason, in the following example the port for S7 communication is not open in the firewall.

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the relevant security module.

  – PC1: Represents a node in internal network 1

  – PC2: Represents a node in internal network 2
- Security module 1: SCALANCE S module (not S602) for protection of internal network 1
- Security module 2: CP x43-1 Adv. to protect internal network 2
- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

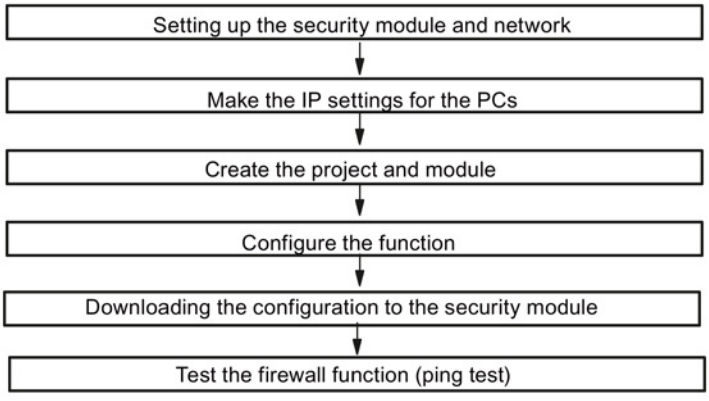
  PC3: PC with the Security Configuration Tool and STEP 7

Requirement:

To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software is installed on PC3.
- The security modules have the current time of day and the current date.
- CP x43-1 Adv. has the following settings in STEP 7:
  – Gigabit IP address: 191.0.0.201, subnet mask: 255.255.0.0
  – PROFINET IP address: 191.1.0.201, subnet mask: 255.255.0.0

Overview of the next steps:



6.3.2 Setting up the security modules and network

Follow the steps outlined below:

1. Establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   - Connect PC1 to the internal interface of security module 1 and PC2 to the internal interface of security module 2.
   - Connect the external interface of security module 1 and the external interface of security module 2 to the hub/switch.
   - Connect PC3 to the hub/switch as well.
2. Now turn on the PCs.

Note

The Ethernet attachments on the internal and external interface are handled differently by the security modules and must not be swapped over when connecting to the communication network:

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

6.3.3 Make the IP settings for the PCs

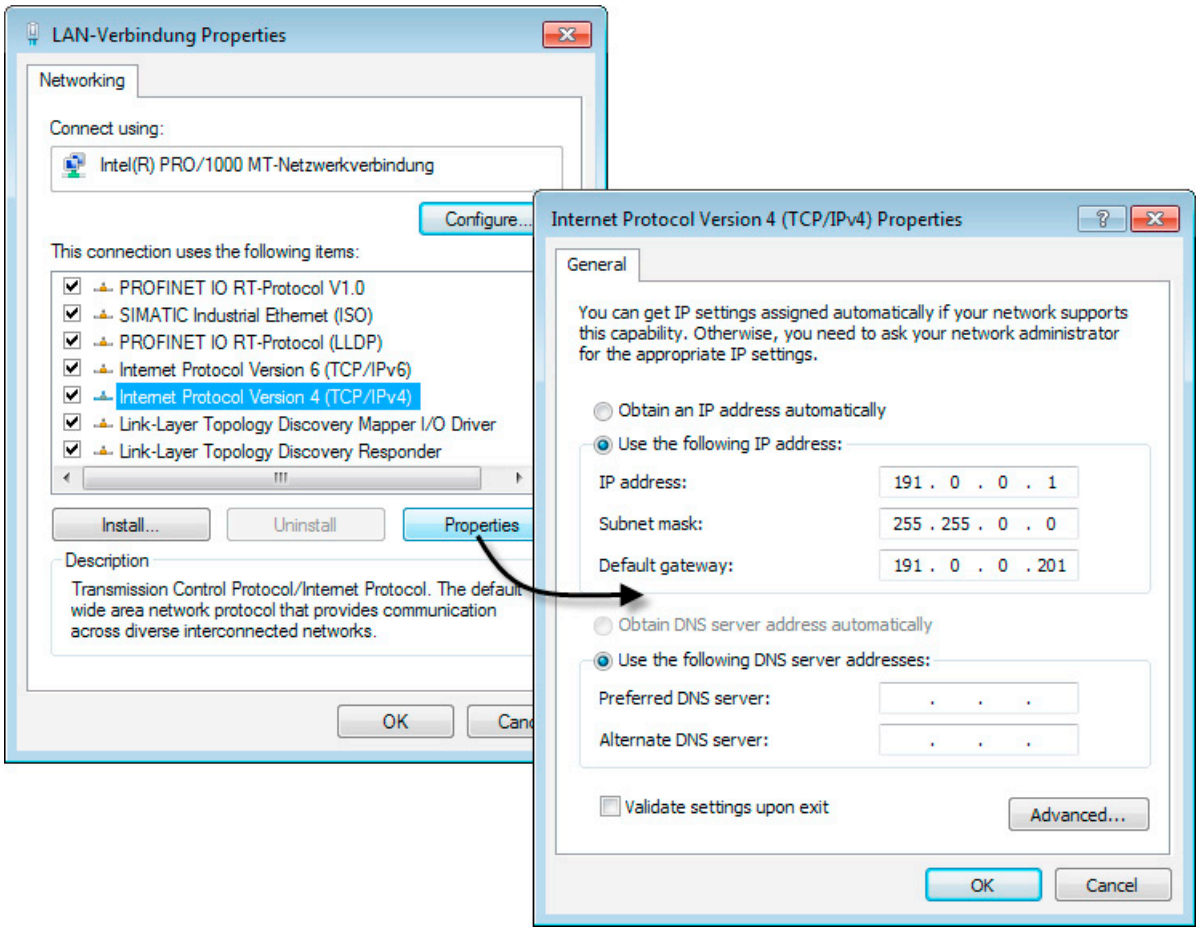
For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask	Default gateway
PC1	191.0.0.1	255.255.0.0	191.0.0.201
PC2	191.1.0.1	255.255.0.0	191.1.0.201
PC3	191.0.0.3	255.255.0.0	191.0.0.201

Follow the steps below for PC1, PC2, and PC3:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

6.3.4 Creating a project and security modules

Follow the steps below:

1. In HW Config in the "Security" tab of the object properties, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

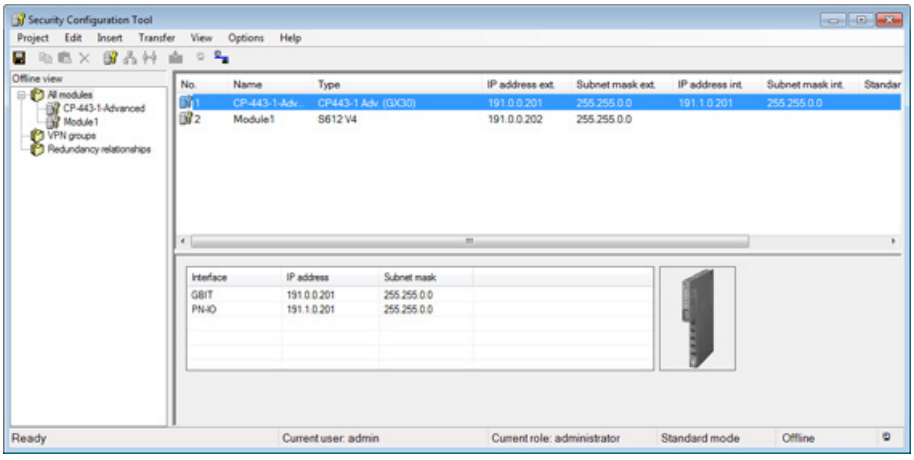
   Result: A new project is created.

3. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.

   Result: The created CP will then be displayed in the list of configured modules.

4. In the Security Configuration Tool, select the "Insert" > "Module" menu command to create a SCALANCE S module with the following parameters:
   - Module: S612
   - Firmware release: V4
   - MAC address: according to the label on the front of the security module
   - IP address (ext.): 191.0.0.202
   - Subnet mask (ext.): 255.255.0.0

Result: The CP and the SCALANCE S module are displayed in the Security Configuration Tool in the list of configured modules.



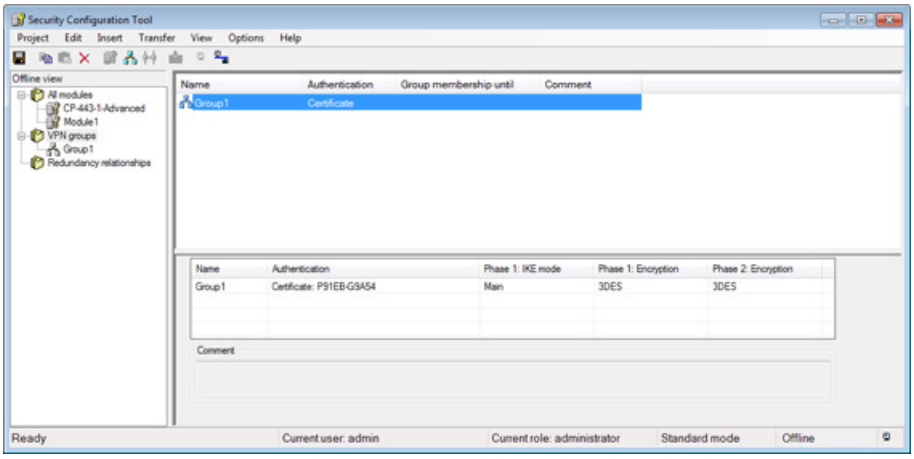
6.3.5 Configuring a VPN group

Two security modules can establish an IPsec tunnel for secure communication if they are assigned to the same VPN group in the project.

Follow the steps outlined below:

1. Select the "VPN groups" object in the navigation panel and select the "Insert" > "Group" menu command.

   Result: The VPN group is created. The VPN group is automatically given the name "Group1".



2. In the navigation panel, click the "All modules" entry and then on the SCALANCE S module in the content area.
3. Drag the SCALANCE S module to the VPN group "Group1" in the navigation panel.

   The security module is now assigned to this VPN group.

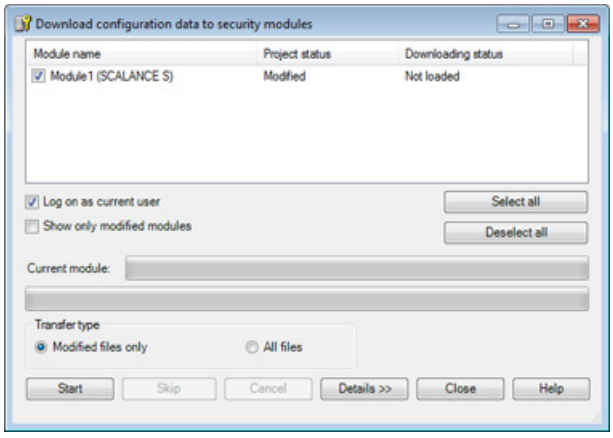
   The color of the key symbol changes from gray to blue.
4. Select the CP in the content area and drag it to the VPN group "Group1" in the navigation panel.

Result: The CP is now also assigned to this VPN group and the configuration of the tunnel connection is complete.

6.3.6 Downloading the configuration to the security modules

SCALANCE S - follow the steps below:

1. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.
2. In the Security Configuration Tool, select the menu command "Transfer" > "To all modules..." to open the following dialog:



The SCALANCE S module is displayed in the list.

1. Make sure that the check box beside the "Module1 (SCALANCE S)" entry is selected.
2. Start the download with the "Start" button.

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

CP - follow the steps below:

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu.
3. Download the new configuration to the security module using the "PLC" > "Download to Module..." menu.

If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.

Result: Security modules in productive mode

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

6.3.7 Test the tunnel function (ping test)

How can you test the configured function?

The function can be tested as described below using a ping command. As an alternative, you can also use other communication programs to test the configuration.

Note

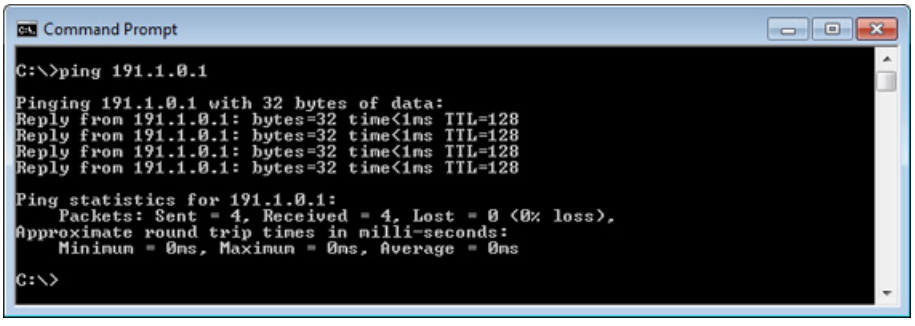
In Windows, the firewall can be set so that as default the ping commands do not pass through. If necessary, you will need to enable the ICMP services of the type "Request" and "Response".

Test phase 1

Now test the function of the established tunnel connection as follows:

1. On PC1, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the Ping command from PC1 to PC2 (IP address 191.1.0.1)

   In the command line of the "Command Prompt" window, enter the command "ping 191.1.0.1" at the cursor position. You will then receive the following message (positive reply from PC2):



Result

If the IP packets have reached PC2, the "Ping statistics for 191.1.0.1" display the following:

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

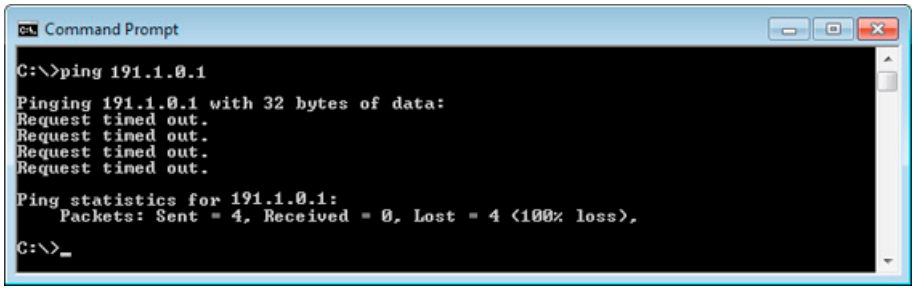
Since no other communication is permitted, these packets must have been transported through the VPN tunnel.

Test phase 2

Repeat the test by sending a ping command from PC3.

1. On PC3, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Send the same ping command ("ping 191.1.0.1") in the Command Prompt window of PC3.

   You will then receive the following message (no reply from PC2):



Result

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

This is shown in the "Ping statistics" for 191.1.0.1 as follows:

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

6.4 VPN tunnel between CP 1628 and CP x43-1 Adv.

6.4.1 Overview

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

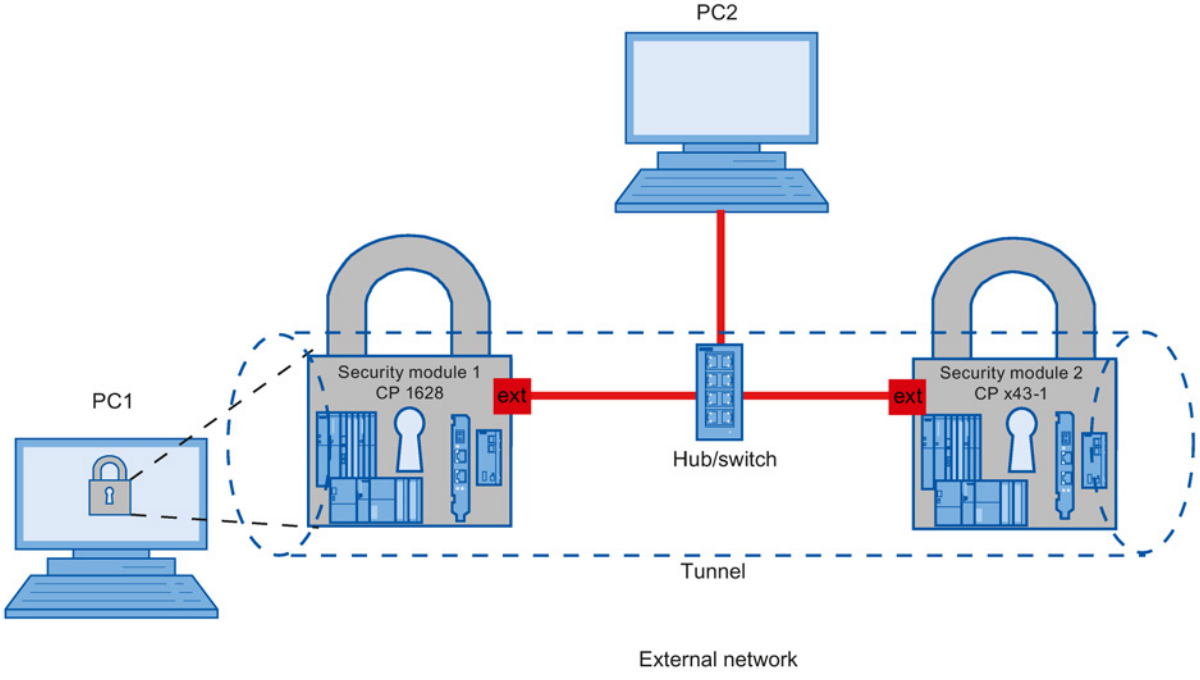
With this configuration, IP traffic and layer 2 traffic is possible only over the established tunnel connections with authorized partners of a VPN group.

Note

Please remember that after loading the configuration, your station can only be reached if the S7 protocol (TCP port 102) is allowed from "External => Station" in the firewall. Unencrypted communication from the external network should be avoided following commissioning. If you do not use secure connection establishment from the external network via VPN, you should run STEP 7 diagnostics and reconfigure only from within the internal network.

For this reason, in the following example the port for S7 communication is not open in the firewall.

Setting up the test network



- PC1 with security module 1: PC with CP 1628
- PC2: PC with the Security Configuration Tool and STEP 7
- Security module 2: CP x43-1 Adv.

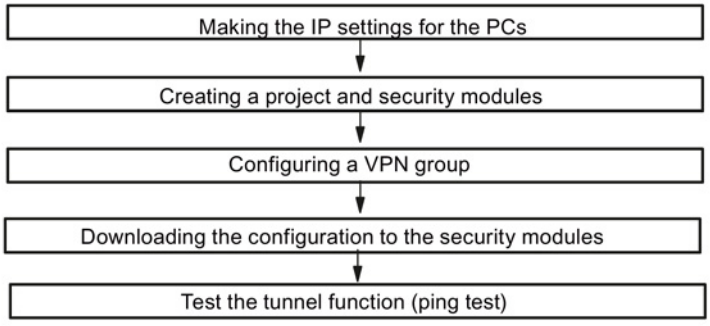
Requirement:

To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software is installed on PC2.
- STEP 7 is installed on PC2 and a STEP 7 project has already been created.
- The CPs have the current time of day and the current date.
- CP 1628 has the following settings in STEP 7:
  - IP address Industrial Ethernet: 192.168.0.5, subnet mask: 255.255.255.0

    The NDIS IP address is set up in the IP settings of the PC.
- CP x43-1 Adv. has the following settings in STEP 7:
  - Gigabit IP address: 192.168.0.11, subnet mask: 255.255.255.0
  - PROFINET IP address: 192.168.1.11, subnet mask: 255.255.255.0

Overview of the next steps:



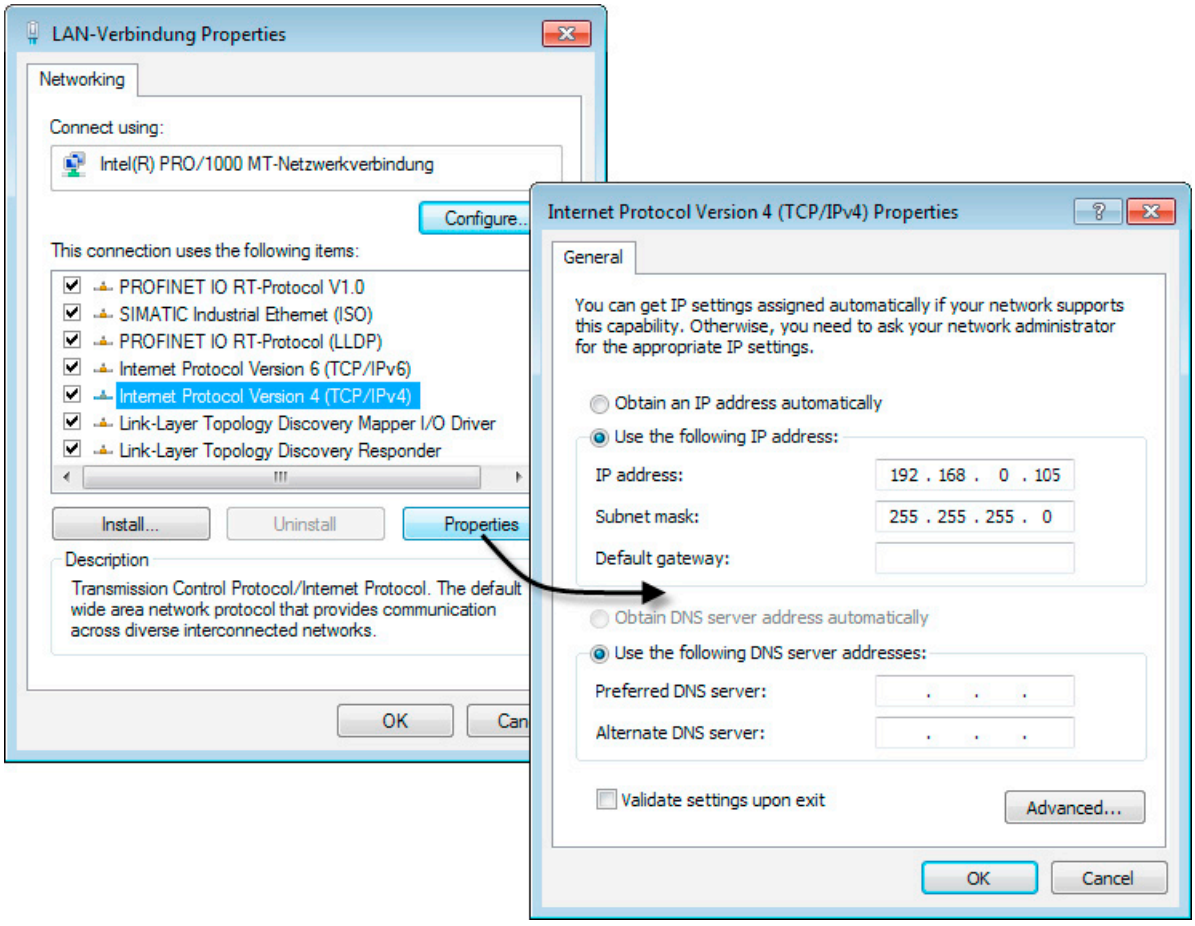
6.4.2 Make the IP settings for the PCs

For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask
PC1	NDIS: 192.168.0.105	255.255.255.0
PC2	192.168.0.110	255.255.255.0

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

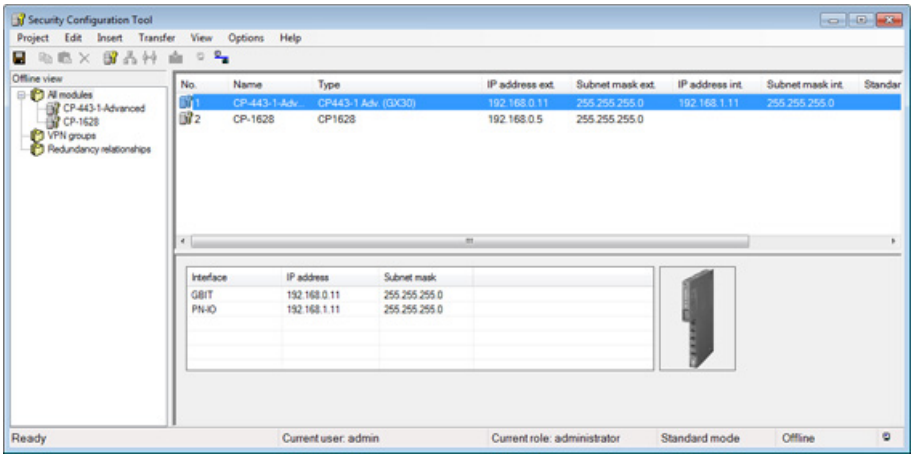
6.4.3 Creating a project and security modules

Follow the steps below:

1. In the "Security" tab of the object properties of the CP 1628, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new security project is created.
3. Change to the object properties of the CP x43-1 Adv. and select the "Enable security" check box on the "Security" tab.
4. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.

Result: The security modules will then be displayed in the list of configured modules.



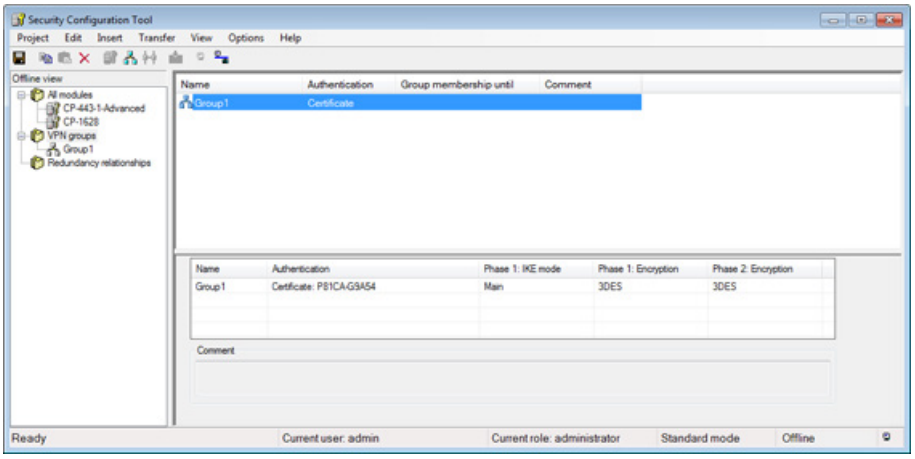
6.4.4 Configuring a VPN group

Two security modules can establish an IPsec tunnel for secure communication if they are assigned to the same VPN group in the project.

Follow the steps outlined below:

1. Select the "VPN groups" object in the navigation panel and select the "Insert" > "Group" menu command.

   Result: The VPN group is created. The VPN group is automatically given the name "Group1".



2. In the navigation panel, click the "All Modules" entry and then on the first CP.
3. Drag the CP to the VPN group "Group1" in the navigation panel.

   The security module is now assigned to this VPN group.

   The color of the key symbol changes from gray to blue.

4. Select the second CP in the content area and drag it to the VPN group "Group1" in the navigation panel.

Result: The second CP is now also assigned to this VPN group and the configuration of the tunnel connection is complete.

6.4.5 Downloading the configuration to the security modules

Follow the steps below:

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu command.
3. Download the new configuration to the security module using the "PLC" > "Download to Module..." menu command.
4. Perform steps 2-3 for the second security module.

If the download was completed free of errors, the security modules restart automatically and the new configuration is activated.

Result: Security modules in productive mode

Commissioning the configuration is therefore completed and the two security modules can establish a communications tunnel.

6.4.6 Test the tunnel function (ping test)

How can you test the configured function?

The function can be tested as described below using a ping command. As an alternative, you can also use other communication programs to test the configuration.

Note

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

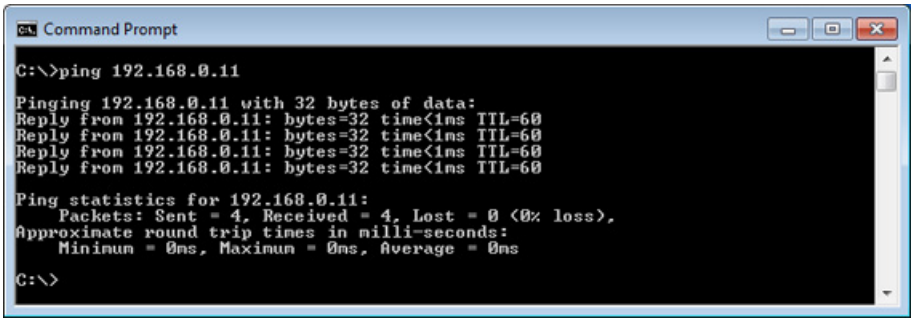
Test phase 1

Now test the function of the tunnel connection established between PC1 and security module 2:

1. On PC1, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC1 to security module 2 (IP address 192.168.0.11)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.0.11" at the cursor position.

   You will then receive the following message (positive reply from security module 2):



Result

If the IP packets have reached security module 2, the "Ping statistics" for 192.168.0.11 display the following:

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

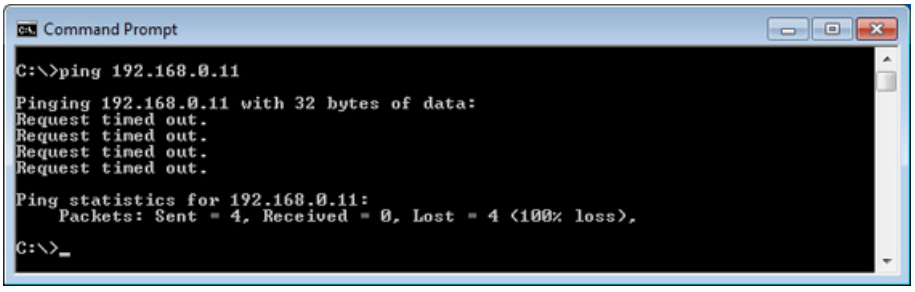
Since no other communication is permitted, these packets must have been transported through the VPN tunnel.

Test phase 2

Repeat the test by sending a ping command from PC2.

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Send the same ping command ("ping 192.168.0.11") in the Command Prompt window of PC2.

   You will then receive the following message (no reply from security module 2):



Result

The IP packets from PC2 cannot reach security module 2 since no tunnel communication between these two devices is configured and normal IP data traffic is not permitted.

This is shown in the "Ping statistics" for 192.168.0.11 as follows:

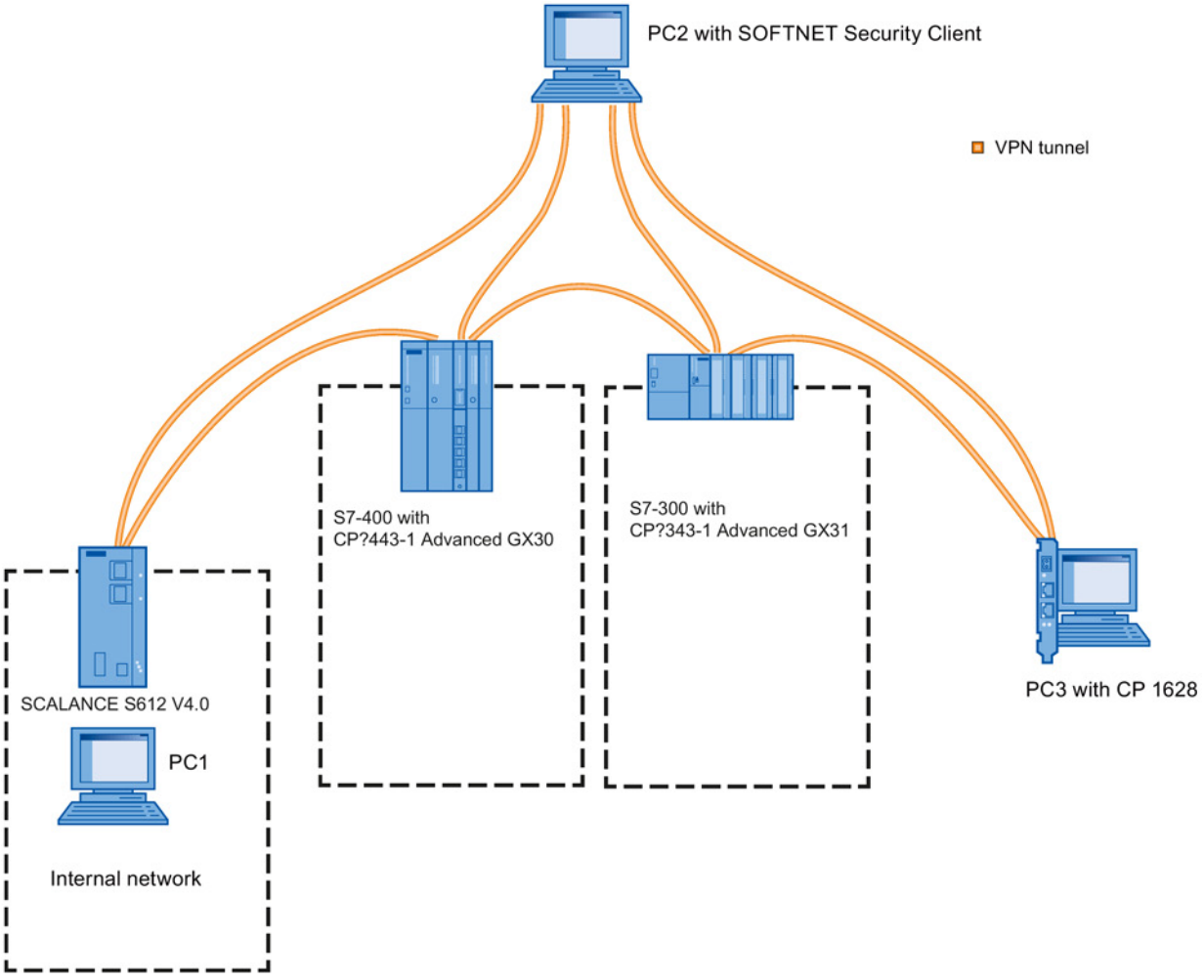
- Sent = 4
- Received = 0
- Lost = 4 (100% loss)

6.5 VPN tunnel between all security products

6.5.1 Overview

Overview

In this example, the tunnel function is configured in the "standard mode" project engineering view. With this configuration, IP traffic is possible only over the established VPN tunnel connections between authorized partners or the individual VPN groups. Access from the service PG on which the SOFTNET Security Client is installed is allowed for all four security modules.



VPN group	VPN node
1	SCALANCE S612 V4.0 CP 443-1 Advanced GX30 SOFTNET Security Client
2	CP 343-1 Advanced GX31 CP 443-1 Advanced GX30 SOFTNET Security Client
3	CP 1628 CP 343-1 Advanced GX31 SOFTNET Security Client

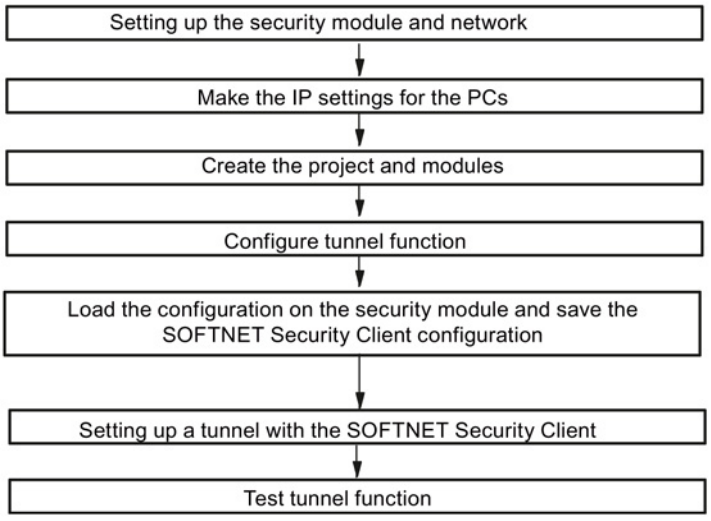
Requirement:

To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software and the SOFTNET Security Client are installed on PC2.
- STEP 7 is installed on PC2 and a STEP 7 project with the following security modules has already been created.
- All security modules have the current time of day and the current date.

Security module	IP address	Subnet mask
CP 443-1 Advanced GX30	Gigabit: 90.12.150.41	255.255.0.0
	PROFINET: 110.100.150.41	255.255.255.0
CP 343-1 Advanced GX31	Gigabit: 90.12.150.11	255.255.0.0
	PROFINET: 110.100.150.11	255.255.255.0
CP 1628	Industrial Ethernet: 90.12.150.101	255.255.0.0

Overview of the next steps:



6.5.2 Make the IP settings for the PCs

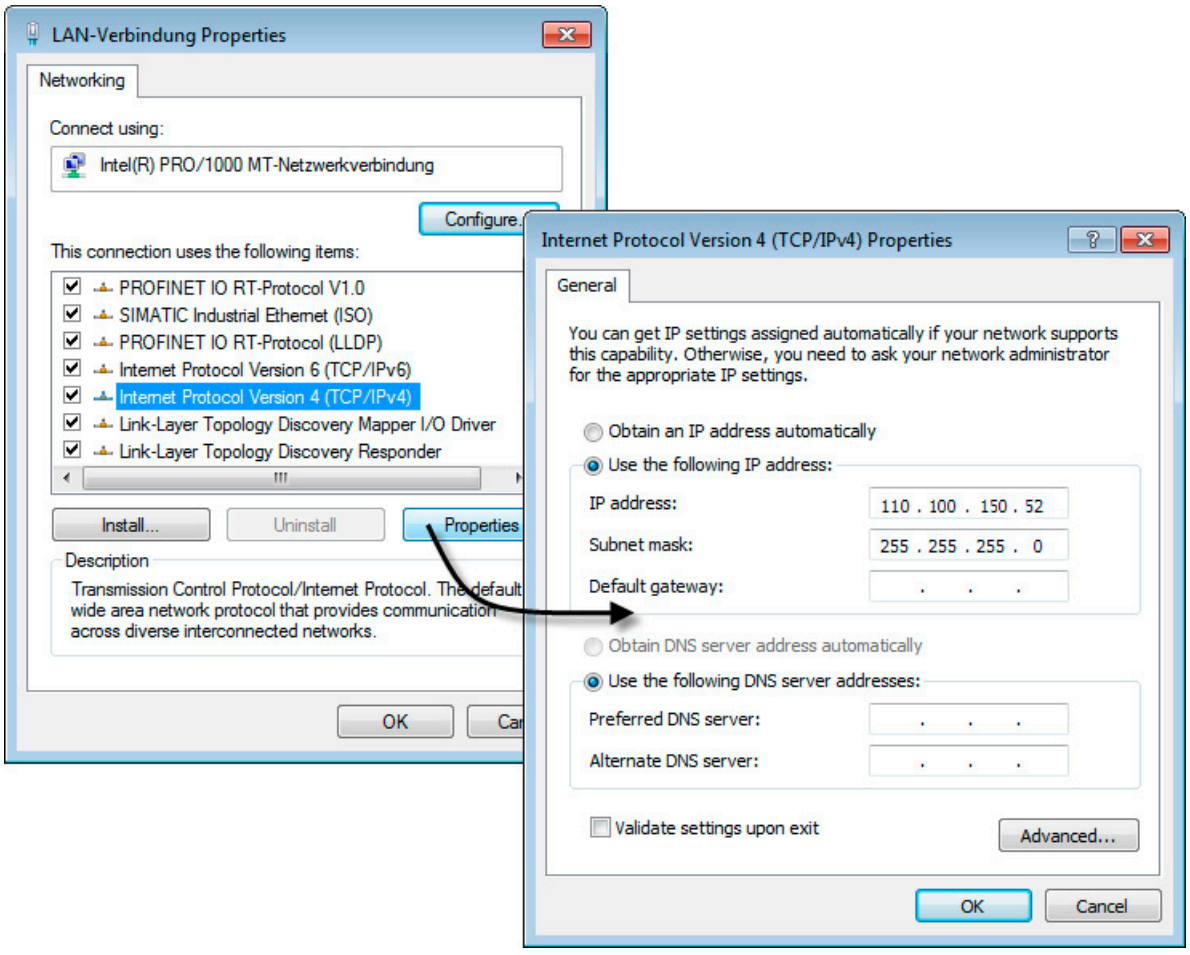
For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask
PC1	110.100.150.52	255.255.255.0
PC2	90.12.150.117	255.255.0.0

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Now enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

6.5.3 Creating a project and security modules

Enabling security for the CPs

1. IN HW Config, in the object properties of the CP 443-1 Advanced GX30, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new security project is created.
3. In the "Security" tab of the object properties of the CP 343-1 Advanced GX31 and CP 1628, enable the "Enable security" check box one after the other.
4. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.

Result: The created CPs on which security is activated are displayed in the list of configured modules.

Creating SCALANCE S and SOFTNET Security Client

1. Select the "All modules" entry in the navigation panel.
2. Create a new security module with the "Insert" > "Module" menu command. Configure the following parameters:
   - Product type: SCALANCE S
   - Module: S612
   - Firmware release V4
   - MAC address: according to the label on the front of the security module
   - IP address (ext.): 90.12.150.51, subnet mask (ext.): 255.255.0.0.
3. From the drop-down list "Interface routing external/internal", select the "Routing mode" and enter the following address data:
   - IP address (int.): 110.100.150.51, subnet mask (int.): 255.255.255.0
4. Click the "OK" button.

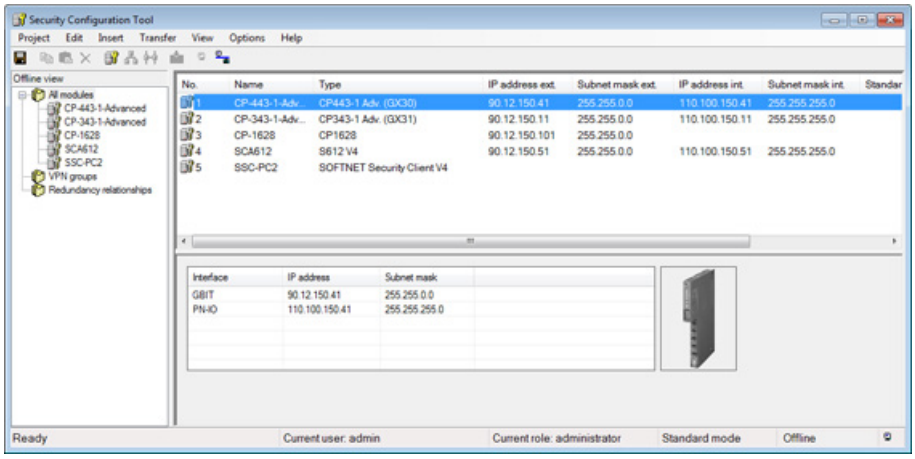
   Result: The created SCALANCE S module will be displayed in the list of configured modules as "Module1".
5. Select the "All modules" entry in the navigation panel.

6. Generate a second module with the "Insert" > "Module" menu command. Configure the following parameters:
   - Product type: SOFTNET Configuration (SOFTNET Security Client, VPN device, NCP VPN client)
   - Module: SOFTNET Security Client
   - Firmware release: V4

     Note: With the selection of the option “V4”t, the full range of functions of SOFTNET Security V4 and SOFTNET Security client V5 ia available.
7. Click the "OK" button.

   Result: The created SOFTNET Security Client will then be displayed in the list of configured modules as "Module2".
8. In the navigation panel, click the "All modules" entry and then on the row with the module name "Module1" in the content area.
9. Click in the "Name" column and enter the name "SCA612".
10. Click on the row with the module name "Module2".
11. Click in the "Name" column and enter the name "SSC-PC2".

Result: The CPs, the SCALANCE S module and the SOFTNET Security Client are displayed in the Security Configuration Tool in the list of configured modules.



6.5.4 Configuring VPN groups

Security modules can establish an IPsec tunnel for secure communication if they are assigned to the same VPN group in the project.

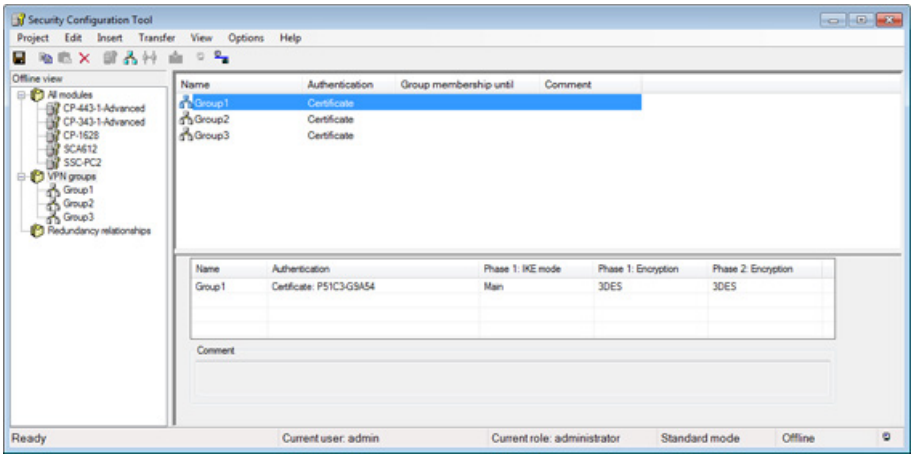
Follow the steps outlined below:

1. Select the "VPN groups" object in the navigation panel and select the "Insert" > "Group" menu command.

   Result: The VPN group is created. The VPN group is automatically given the name "Group1".

2. Create two further VPN groups.

   Result: The VPN groups are automatically given the names "Group2" and "Group3".



3. Select the "All modules" object in the navigation panel.
4. One after the other, drag the SCALANCE S module, the CP 443-1 Advanced GX30 and the SOFTNET Security Client to "Group1" in the navigation panel.

   Result: The modules are now assigned to the VPN group "Group1". The color of the key symbols changes from gray to blue.

5. One after the other, drag the CP 343-1 Advanced GX31, the CP 443-1 Advanced GX30 and the SOFTNET Security Client to "Group2" in the navigation panel.

   Result: The modules are now assigned to the VPN group "Group2". The color of the key symbol of the CP 343-1 Advanced GX31 changes from gray to blue.

6. One after the other, drag the CP 1628, the CP 343-1 Advanced GX31 and the SOFTNET Security Client to "Group3" in the navigation panel.

   Result: The modules are now assigned to the VPN group "Group3". The color of the key symbol of the CP 1628 changes from gray to blue.

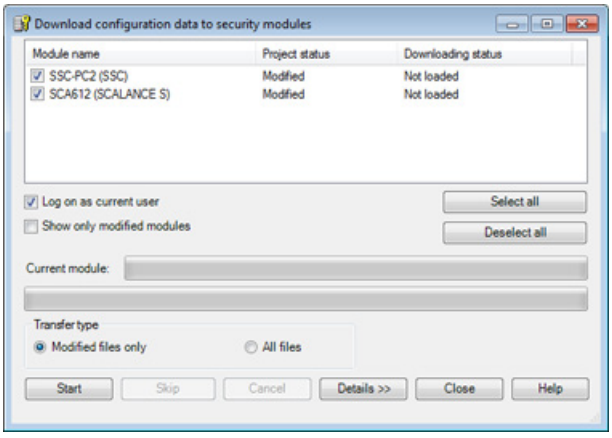
7. Select the "Project" > "Save" menu command.
8. Close SCT.

The configuration of the tunnel connection is complete.

6.5.5 Loading the configuration on security modules and saving the SOFTNET Security Client configuration

SCALANCE S and SOFTNET Security Client - Follow the steps below:

1. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.
2. In the Security Configuration Tool, select the menu command "Transfer" > "To all modules..." to open the following dialog:



3. Start the download with the "Start" button.
4. Save the configuration file "projectname.SSC-PC2.dat" in a folder of your choice and assign a password for the private key of the certificate.

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

CPs - follow the steps below:

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu command for the CP 443-1 Advanced.
3. Download the new configuration to the security module using the "PLC" > "Download to Module..." menu command.
4. Perform steps 2-3 analogously for the CP 343-1 and CP 1628.

If the download was completed free of errors, the security modules restart automatically and the new configuration is activated.

6.5.6 Setting up a tunnel with the SOFTNET Security Client

Note

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

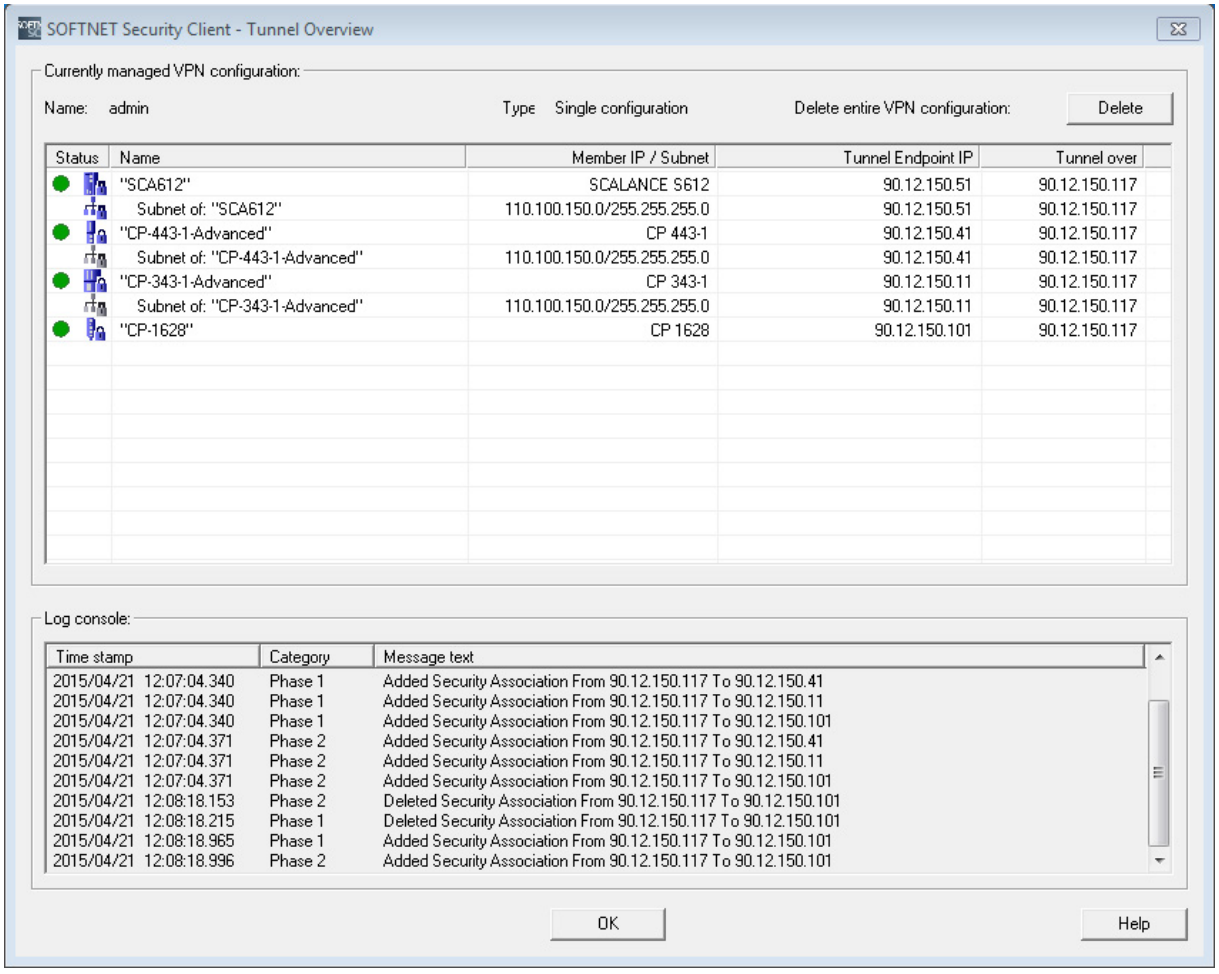
Follow the steps outlined below:

1. Start the SOFTNET Security Client on PC2.
2. Click the "Load configuration" button, change to the folder you selected above and download the "Projectname.SSC-PC2.dat" configuration file.
3. In the "VPN configuration" dialog, enable the "Establish VPN tunnel to the internal nodes" check box.
4. Select the network adapter from whose IP the VPN tunnel will be established.
5. Enter the password for the private key of the certificate and confirm with "Next".
6. Click the "Tunnel Overview" button.
7. To allow the learned subnets to communicate, enable this using the shortcut menu.

Result: Active tunnel connection

The tunnels between the SOFTNET Security Client and the security modules were established. This status is indicated by the green circle.

In the Logging Console of the Tunnel Overview, among other things information on the sequence of executed connection attempts is displayed.



Commissioning the configuration is now complete and the security modules of the configured VPN groups and the SOFTNET Security Client have established communications tunnels via which they can communicate.

6.5.7 Test the tunnel function (ping test)

How can you test the configured function?

The function can be tested as described below using a ping command. As an alternative, you can also use other communication programs to test the configuration.

Note

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

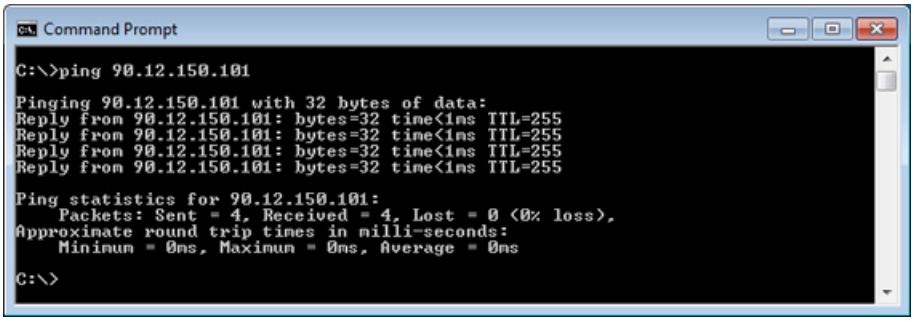
Testing

Now test the function of the tunnel connection established between PC2 and PC3:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the Ping command from PC2 to PC3 (IP address 90.12.150.101)

   In the command line of the "Command Prompt" window, enter the command "ping 90.12.150.101" at the cursor position.

   You will then receive the following message (positive reply from PC3):



Result

If the IP packets have reached PC3, the "Ping statistics" for 90.12.150.101 display the following:

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

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

Repeating the test section

One after the other, test the functionality of the tunnel connections established between PC2 and PC1, PC2 and CP 443-1 Advanced GX30 and PC2 and CP 343-1 Advanced GX31 as described in the section "Test section". If the tunnel connection is correctly established, you will receive a positive response to the ping query from each PC or security module.

Configuring remote access via a VPN tunnel 7

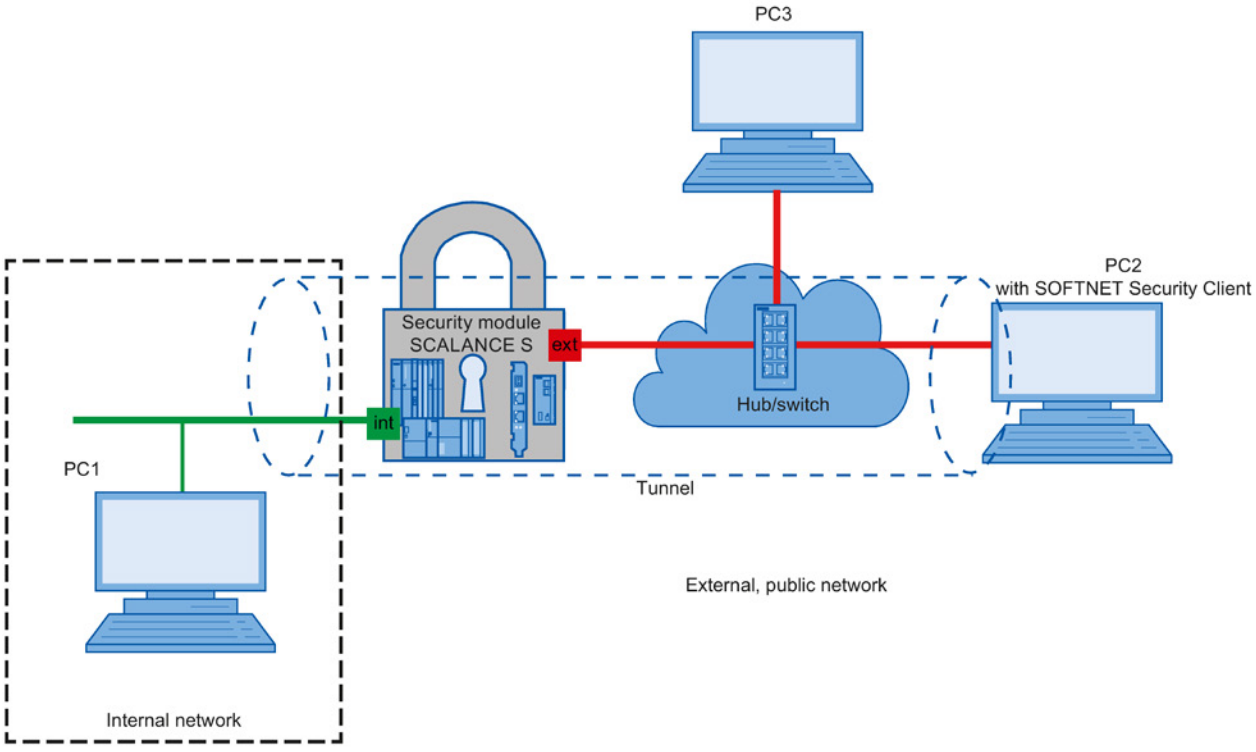
7.1 Remote access - VPN tunnel example with SCALANCE S612 and SOFTNET Security Client

7.1.1 Overview

In this example, the VPN tunnel function is configured in the "standard mode" configuration view. In this example, a security module and the SOFTNET Security Client form the two tunnel endpoints for the secure tunnel connection via a public network.

With this configuration, IP traffic is possible only over the established VPN tunnel connection between the two authorized partners.

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the security module.

  – PC1: Represents a node in the internal network

- Security module: SCALANCE S module (not S602) for protection of the internal network
- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

  – PC2: PC with Security Configuration Tool configuration software and the SOFTNET Security Client software for secure VPN access to the internal network

  – PC3: Test PC for test phase 2

Note

In the example, a local area network is used as a substitute for an external public WAN (Internet) to illustrate the principles of the functionality.

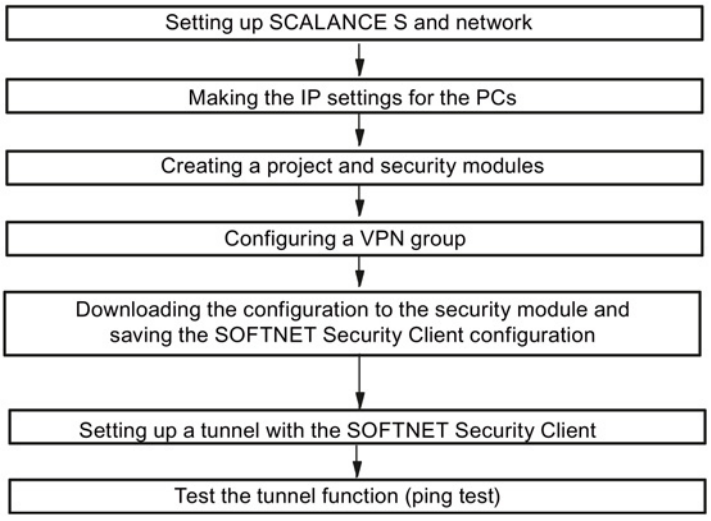
Explanations relating to the use of a WAN are provided where necessary.

Required devices/components:

Use the following components to set up the network:

- 1 x SCALANCE S module, (not S602), (optional: a suitably installed DIN rail with fittings);
- 1 x 24 V power supply with cable connector and terminal block plug;
- 1 x PC on which the "Security Configuration Tool" and VPN client "SOFTNET Security Client" are installed;
- 1 x PC in the internal network to test the configuration;
- 1 x PC in the external network to test the configuration;
- 1 x network hub or switch to set up the network connections to the SCALANCE S module and the PCs;
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

Overview of the next steps:



7.1.2 Set up SCALANCE S and the network

Follow the steps outlined below:

1. First unpack the SCALANCE S and check that it is undamaged.
2. Connect the power supply to the SCALANCE S.

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

⚠ WARNING

Use safety extra-low voltage only

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

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

1. Now establish the physical network connections by plugging the connectors into the interfaces being used:
   – Connect PC1 to the internal interface of the security module.
   – Connect the external interface of the security module to the hub/switch.
   – Connect PC2 and PC3 to the hub/switch as well.
2. Now turn on the PCs.

Note

To use a WAN as an external public network, the connections to the hub/switch must be replaced by the connections to the WAN (Internet access).

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;

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

7.1.3 Make the IP settings for the PCs

For the test, the PCs are given the following IP address settings.

PC	IP address	Subnet mask	Default gateway
PC1	192.168.0.1	255.255.255.0	192.168.0.201
PC2	191.0.0.2	255.255.0.0	191.0.0.201
PC3	191.0.0.3	255.255.0.0	191.0.0.201

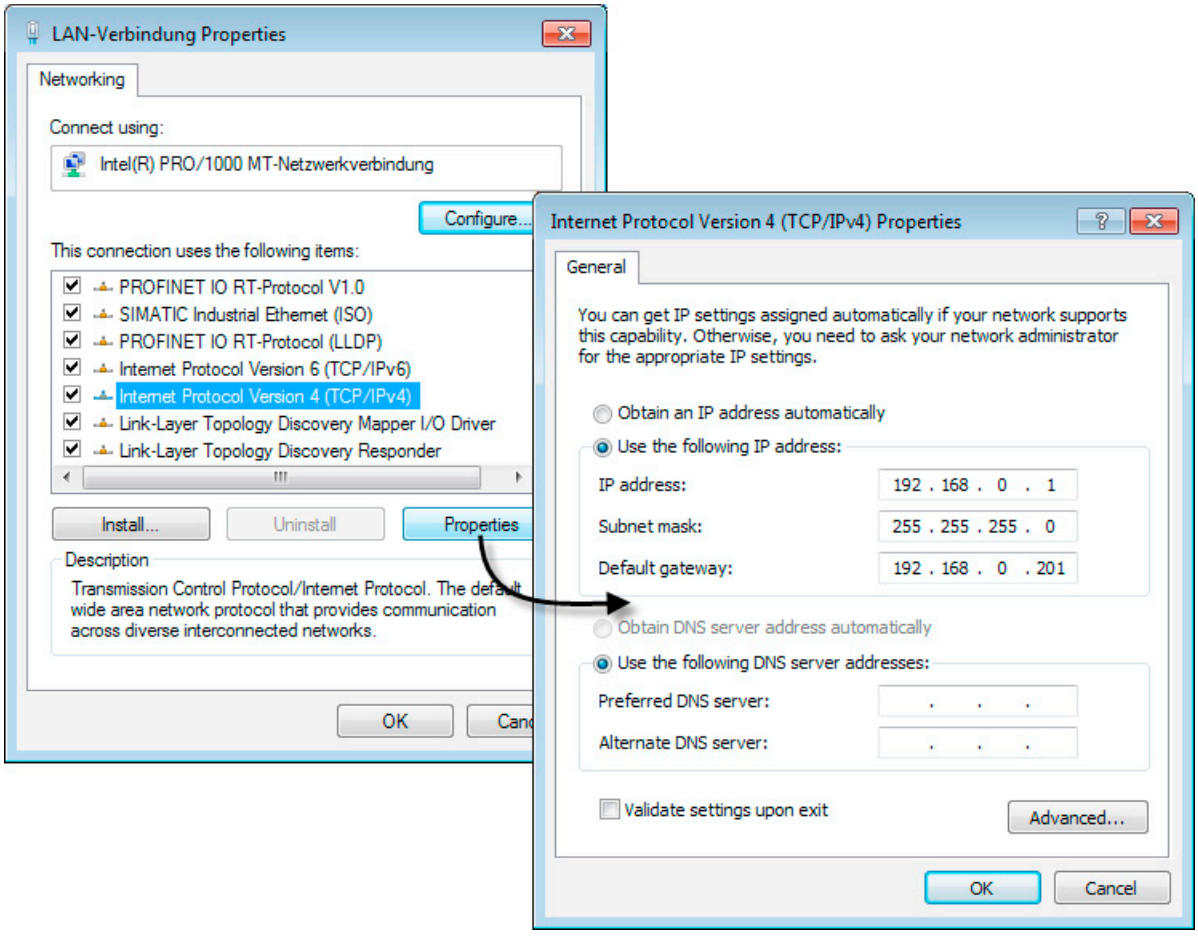
Note

To use a WAN as an external public network, the relevant IP settings for the connection to the WAN (Internet) must be made on PC2, PC3 and the security module.

Follow the steps below for PC1, PC2, and PC3:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.

3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

7.1.4 Creating a project and security modules

Follow the steps below:

1. Select the "Project" > "New..." menu command.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.

3. Confirm your entries.

   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.

4. Select from the following options:
   - Product type: SCALANCE S
   - Module: S612
   - Firmware release: V4
   - MAC address: according to the label on the front of the security module
   - IP address (ext.): 191.0.0.201, subnet mask (ext.): 255.255.0.0

   Note

   If a WAN is used as an external public network, enter an IP address from the internal subnet of your DSL router as "IP address ext.". As the standard router, the internal IP address of the DSL router must be entered. Enter the public IP address assigned by the provider in the "VPN" tab of the module properties in "WAN IP address / FQDN".

   If you use a DSL router as Internet gateway, at least the following ports of the router must be forwarded to the IP address of the security module:

   • Port 500 (ISAKMP)

   • Port 4500 (NAT-T)

5. From the drop-down list "Interface routing external/internal", select the "Routing mode" and enter the following address data for the internal interface of the security module:
   - IP address (int.): 192.168.0.201, subnet mask (int.): 255.255.255.0
6. Click the "OK" button.

   Result: The module will then be displayed in the list of configured modules.

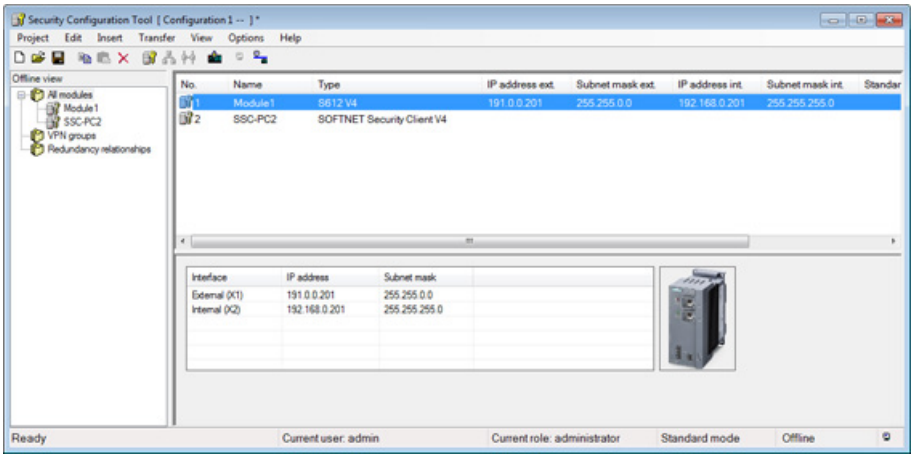
7. Use the "Insert" > "Module" menu command and specify the following parameters:
   - Product type: SOFTNET Configuration (SOFTNET Security Client, VPN device, NCP VPN client)
   - Module: SOFTNET Security Client
   - Firmware release: V4

     Note: With the selection of the option “V4”t, the full range of functions of SOFTNET Security V4 and SOFTNET Security client V5 ia available.
8. Click the "OK" button.

   Result: The module will then be displayed in the list of configured modules.

9. In the navigation panel, click the "All modules" object and then on the row with the module name "Module2" in the content area.
10. Click in the "Name" column and enter the name "SSC-PC2".

    Result: The settings are complete and should match the following figure:



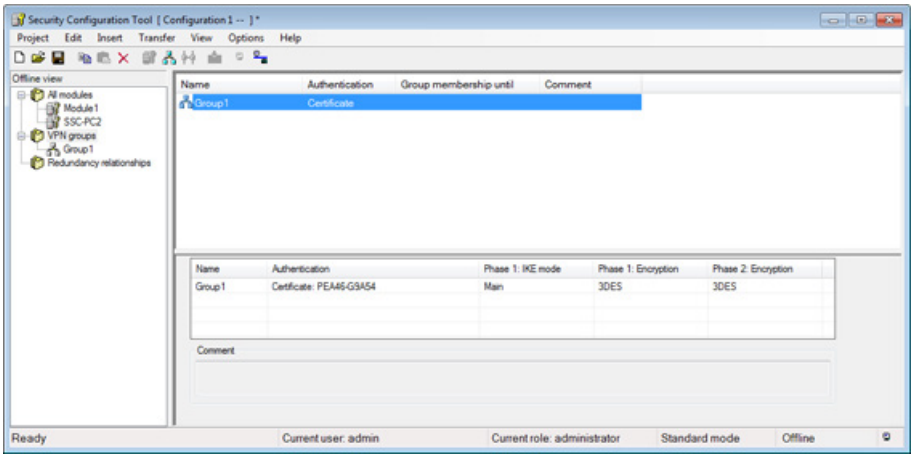
7.1.5 Configuring a VPN group

A SCALANCE S and the SOFTNET Security Client can establish an IPsec tunnel for secure communication when they are assigned to the same group in the project.

Follow the steps outlined below:

1. Select the "VPN groups" object in the navigation panel and select the "Insert" > "Group" menu command.

   Result: The VPN group is created. The VPN group is automatically given the name "Group1".



2. In the navigation panel, click the "All modules" entry and then on the SCALANCE S module in the content area.

3. Drag the SCALANCE S module to the VPN group "Group1" in the navigation panel.

   The security module is now assigned to this VPN group.

   The color of the key symbol changes from gray to blue.

4. Select the SOFTNET Security Client module in the content area and drag it to the VPN group "Group1" in the navigation panel.

   The module is now also assigned to this VPN group.

   The color of the key symbol changes from gray to blue.

5. Select the "Project" > "Save" menu command.

Result: The configuration of the tunnel connection is complete.

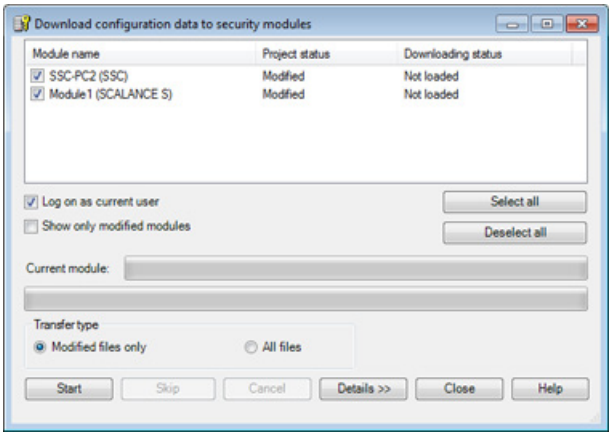
7.1.6 Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

Note

If a WAN is used as an external public network, a security module with the factory settings cannot be configured via this WAN. In this case, configure the security module from within the internal network.

Follow the steps outlined below:

1. Using the menu command "Transfer" > "To all modules...", open the following dialog:



2. Start the download with the "Start" button.
3. Save the configuration file "projectname.SSC-PC2.dat" in your project folder and assign a password for the private key of the certificate.

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

Result: SCALANCE S in productive operation

The security module is in productive operation. This mode is indicated by the Fault LED being lit green.

7.1.7 Setting up a tunnel with the SOFTNET Security Client

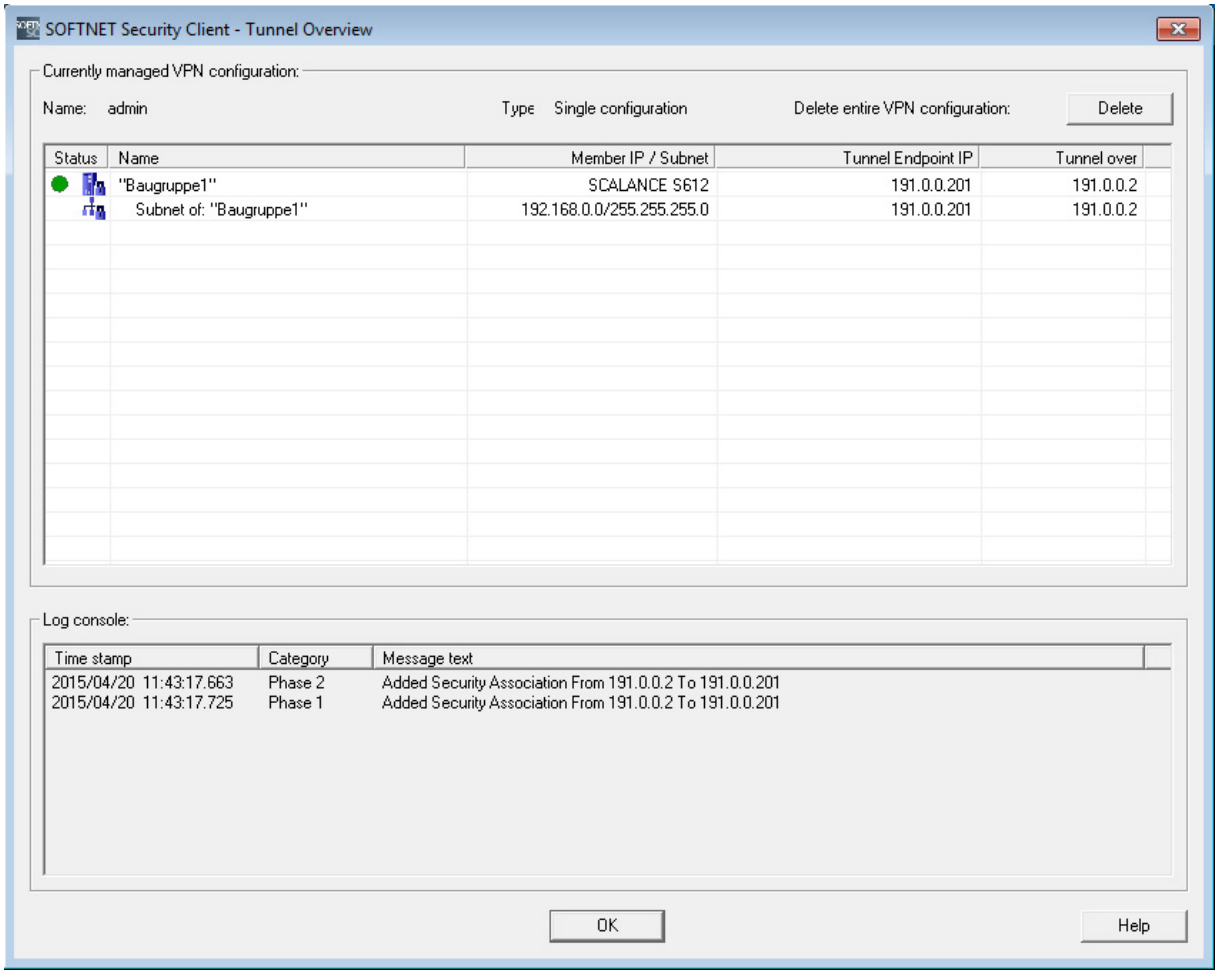
Follow the steps outlined below:

1. Start the SOFTNET Security Client on PC2.
2. Click the "Load Configuration" button, change to your project folder and load the "Projectname.SSC-PC2.dat" configuration file.
3. In the "VPN configuration" dialog, enable the "Establish VPN tunnel to the internal nodes" check box.
4. Select the network adapter from whose IP the VPN tunnel will be established.
5. Enter the password for the private key of the certificate and confirm with "Next".
6. Click the "Tunnel Overview" button.

Result: Active tunnel connection

The tunnel between SCALANCE S and SOFTNET Security Client was established. This status is indicated by the green circle beside the "Module1" entry.

In the Logging Console of the Tunnel Overview, among other things information on the sequence of executed connection attempts is displayed.



The configuration has now been commissioned and the SCALANCE S module and the SOFTNET Security Client have established a communication tunnel over which network nodes can communicate securely with PC2 from within the internal network.

7.1.8 Test the tunnel function (ping test)

How can you test the configured function?

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

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

Note

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

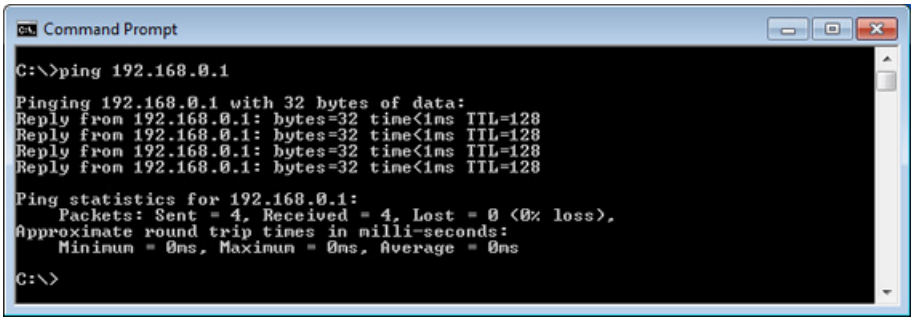
Test phase 1

Now test the function of the established tunnel connection as follows:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to PC1 (IP address 192.168.0.1).

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.0.1" at the cursor position.

You will then receive the following message (positive reply from PC1):



Result

If the IP packets have reached PC1, the "Ping statistics for 192.168.0.1" display the following:

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

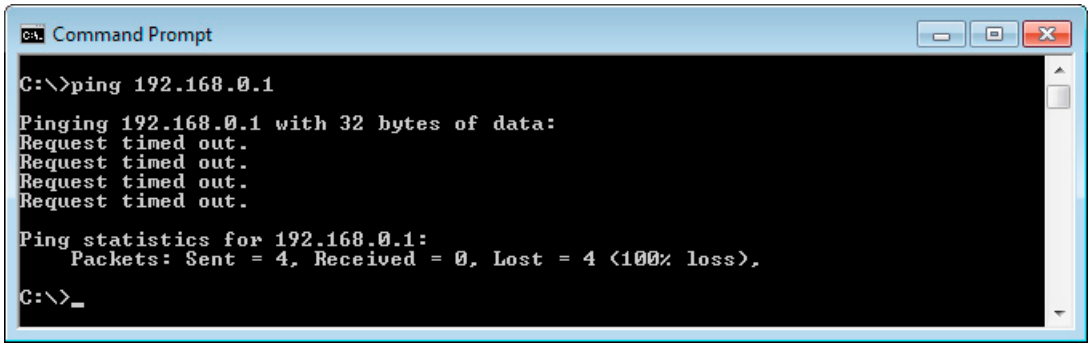
Since no other communication is permitted, these packets must have been transported through the VPN tunnel.

Test phase 2

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

1. On PC3, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Send the same ping command ("ping 192.168.0.1") in the Command Prompt window of PC3.

You will then receive the following message (no reply from PC1):



Result

The IP packets from PC3 cannot reach PC1 since neither tunnel communication between these two devices is configured nor is normal IP data traffic permitted.

This is shown in the "Ping statistics" for 192.168.0.1 as follows:

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

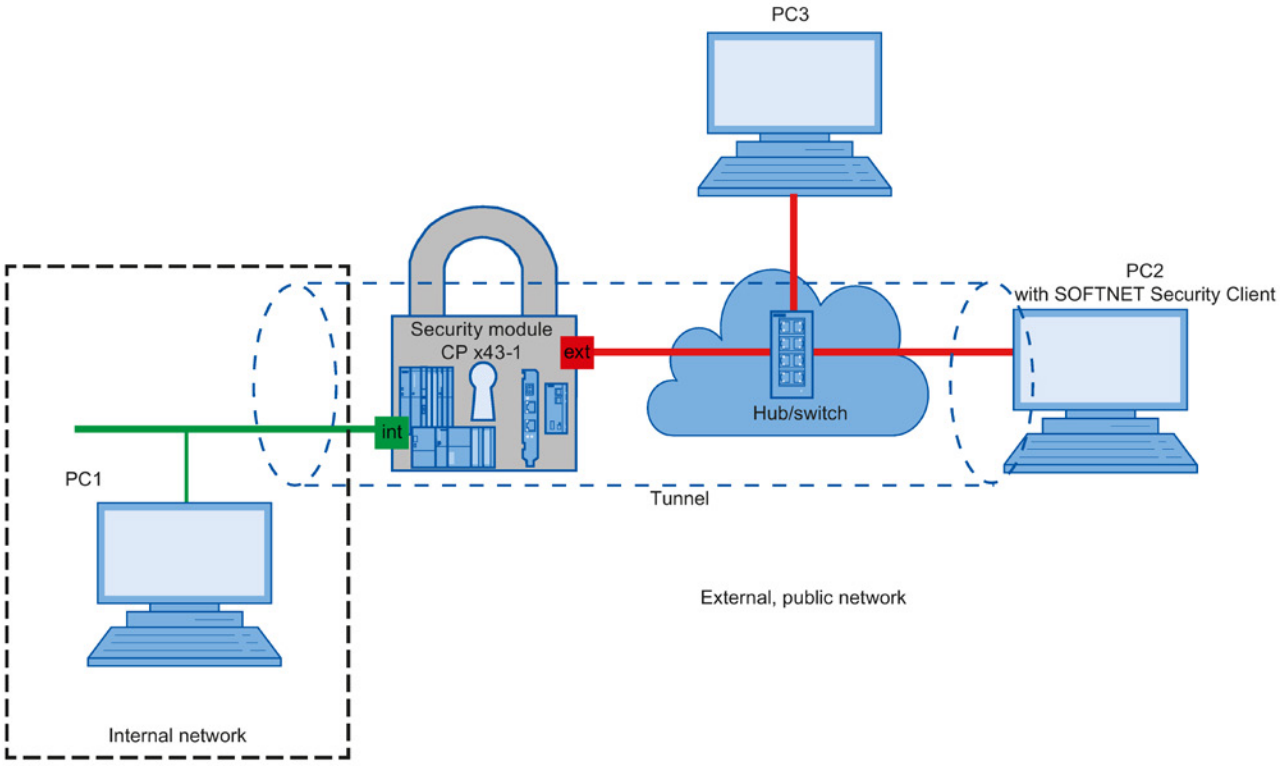
7.2 Remote access - VPN tunnel example with CP x43-1 Advanced and SOFTNET Security Client

7.2.1 Overview

In this example, the VPN tunnel function is configured in the "standard mode" configuration view. In this example, a security module and a SOFTNET Security Client form the two tunnel endpoints for the secure tunnel connection via a public network.

With this configuration, IP traffic is possible only over the established VPN tunnel connection between the two authorized partners.

Setting up the test network



- Internal network - attachment to the internal interface of the security module

  In the test setup, in the internal network, the network node is implemented by a PC connected to the internal interface of the security module.

  – PC1: Represents a node in the internal network

- Security module: CP x43-1 Adv. to protect the internal network

- External network - attachment to the external interface of the security module

  The public, external network is connected to the external interface of the security module.

  – PC2: PC with STEP 7 configuration software, Security Configuration Tool and the SOFTNET Security Client software for secure VPN access to the internal network

  – PC3: Test PC for test phase 2

Note

In the example, a local area network is used as a substitute for an external public WAN (Internet) to illustrate the principles of the functionality.

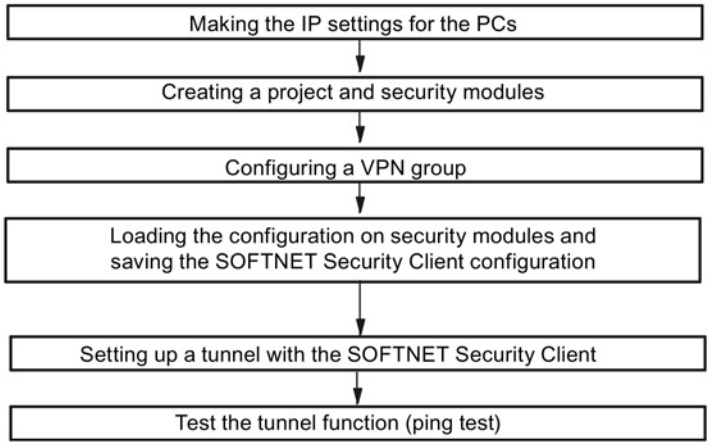
Explanations relating to the use of a WAN are provided where necessary.

Requirement:

To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software is installed on PC2.
- STEP 7 is installed on PC2 and a STEP 7 project has already been created.
- The security module has the current time of day and the current date.
- CP x43-1 Adv. has the following settings in STEP 7:
  – Gigabit IP address: 191.0.0.201, subnet mask: 255.255.0.0
  – PROFINET IP address: 192.168.0.201, subnet mask: 255.255.255.0

Overview of the next steps:



7.2.2 Make the IP settings for the PCs

For the test, the PCs are given the following IP address settings.

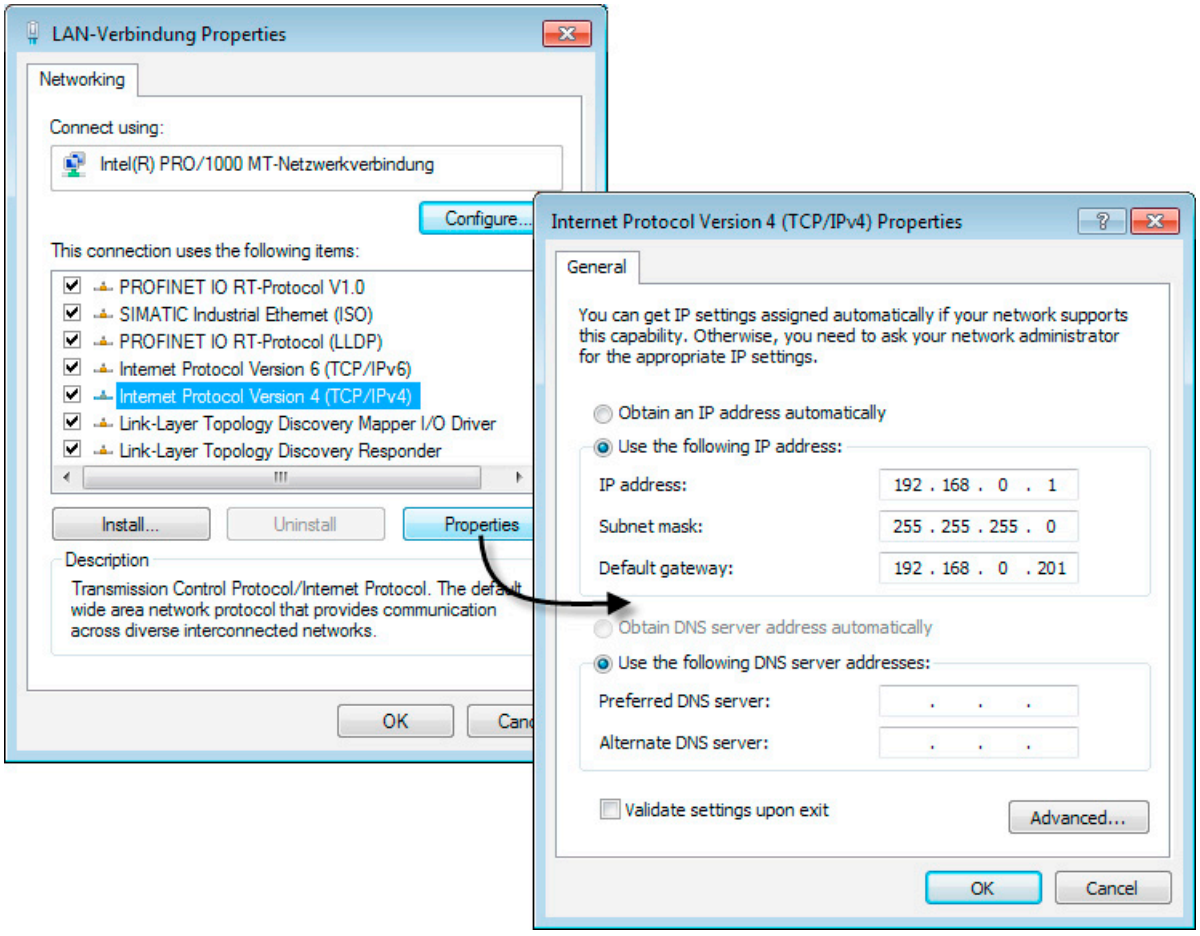
PC	IP address	Subnet mask	Default gateway
PC1	192.168.0.1	255.255.255.0	192.168.0.201
PC2	191.0.0.2	255.255.0.0	191.0.0.201
PC3	191.0.0.3	255.255.0.0	191.0.0.201

Note

To use a WAN as an external public network, the relevant IP settings for the connection to the WAN (Internet) must be made on PC2, PC3 and the security module.

Follow the steps below for PC1, PC2, and PC3:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

7.2.3 Creating a project and security modules

Follow the steps below:

1. In the "Security" tab of the STEP 7 object properties of the security module, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically. Confirm your entries with "OK".

   Result: A new security project is created.
3. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.

Result: The security module will then be displayed in the list of configured modules.

1. Click on the "All modules" object in the navigation panel.
2. Generate a second module with the "Insert" > "Module" menu command.

   Configure:

   – Product type: SOFTNET Configuration (SOFTNET Security Client, VPN device, NCP VPN client)

   – Module: SOFTNET Security Client

   – Firmware release: V4

     Note: With the selection of the option “V4”t, the full range of functions of SOFTNET Security V4 and SOFTNET Security client V5 ia available.
3. Close the dialog with "OK".

   Result: The module will then be displayed in the list of configured modules.

Note

If a WAN is used as an external public network, enter an IP address from the internal subnet of your DSL router as gigabit IP address in HW Config. As the standard router, the internal IP address of the DSL router must be entered. In SCT, enter the public IP address assigned by the provider in the "VPN" tab of the module properties in "WAN IP address / FQDN".

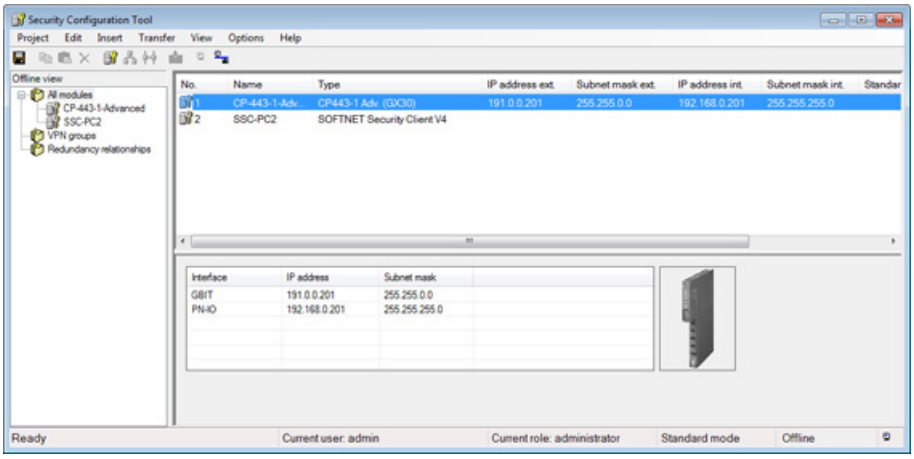
If you use a DSL router as Internet gateway, at least the following ports of the router must be forwarded to the IP address of the security module:

• Port 500 (ISAKMP)

• Port 4500 (NAT-T)

4. In the navigation panel, click the "All modules" object and then on the row with the module name "Module1" in the content area.
5. Click in the "Name" column and enter the name "SSC-PC2".

   Result: The settings are complete and should match the following figure:



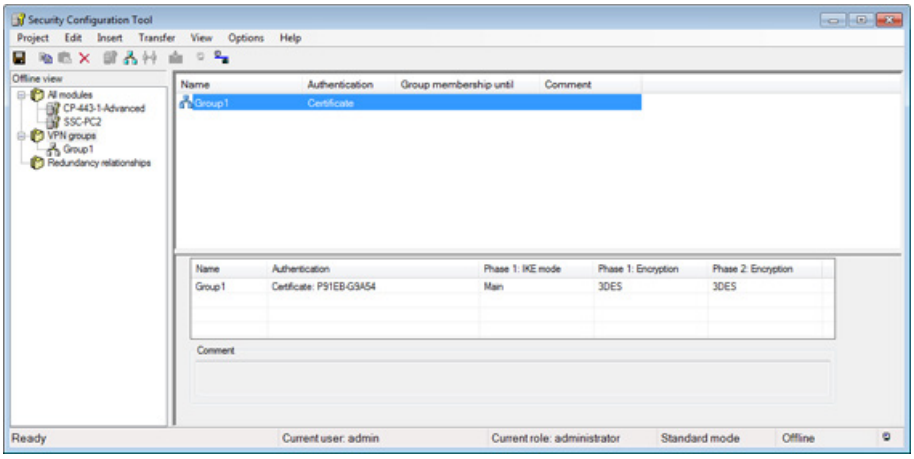
7.2.4 Configuring a VPN group

The security module and the SOFTNET Security Client can establish an IPsec tunnel for secure communication when they are assigned to the same VPN group in the project.

Follow the steps outlined below:

1. Select the "VPN groups" object in the navigation panel and select the "Insert" > "Group" menu command.

   Result: The VPN group is created. The VPN group is automatically given the name "Group1".



2. Select the "All modules" object in the navigation panel.
3. Select the CP in the content area and drag it to the VPN group "Group1" in the navigation panel.

   The security module is now assigned to this VPN group.

   The color of the key symbol changes from gray to blue.
4. Select the SOFTNET Security Client module in the content area and drag it to the VPN group "Group1" in the navigation panel.

   The module is now also assigned to this VPN group.
5. Select the "Project" > "Save" menu command.

The configuration of the tunnel connection is complete.

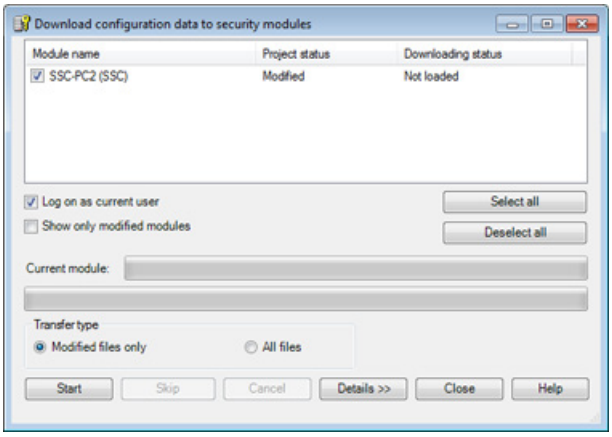
7.2.5 Loading the configuration on security modules and saving the SOFTNET Security Client configuration

Note

If a WAN is used as an external public network, a security module with the factory settings cannot be configured via this WAN. In this case, configure the security module from within the internal network.

Follow the steps outlined below:

1. Using the menu command "Transfer" > "To all modules", open the following dialog:



2. Start the download with the "Start" button.
3. Save the configuration file "projectname.SSC-PC2.dat" in a folder of your choice and assign a password for the private key of the certificate.
4. Close the Security Configuration Tool.
5. In HW Config, select the "Station" > "Save and Compile" menu.
6. Download the new configuration to the security module using the "PLC" > "Download to Module..." menu.

   If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.

7.2.6 Setting up a tunnel with the SOFTNET Security Client

Follow the steps outlined below:

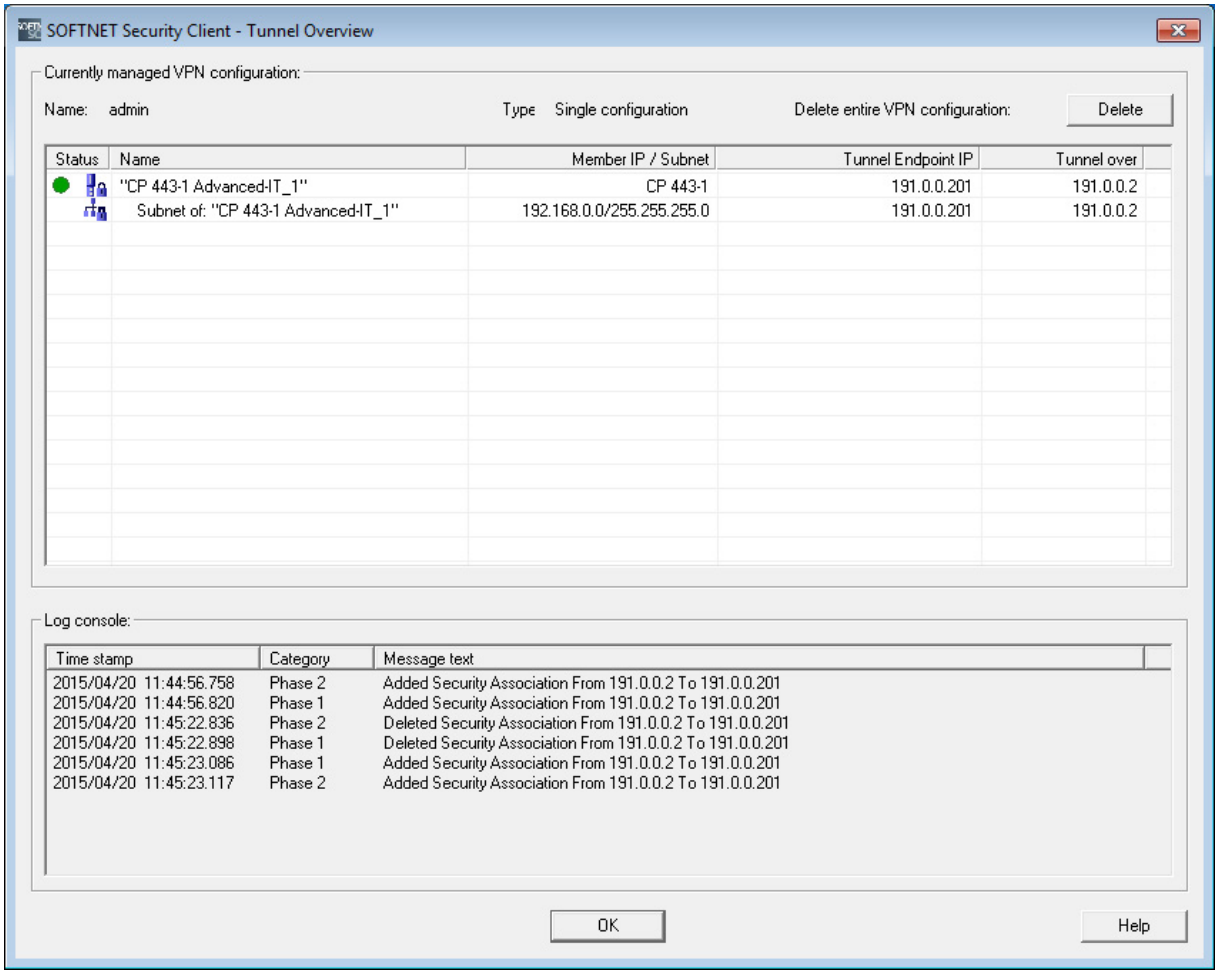
1. Start the SOFTNET Security Client on PC2.
2. Click the "Load Configuration" button, change to your project folder and load the "Projectname.SSC-PC2.dat" configuration file.

3. In the "VPN configuration" dialog, enable the "Establish VPN tunnel to the internal nodes" check box.
4. Select the network adapter from whose IP the VPN tunnel will be established.
5. Enter the password for the private key of the certificate and confirm with "Next".
6. Click the "Tunnel Overview" button.

Result: Active tunnel connection

The tunnel between the security module and the SOFTNET Security Client was established. This status is indicated by the green circle beside the "CP-443-1-Advanced" entry.

In the Logging Console of the Tunnel Overview, among other things information on the sequence of executed connection attempts is displayed.



The configuration has now been commissioned and the security module and the SOFTNET Security Client have established a communication tunnel over which network nodes can communicate securely with PC2 from within the internal network.

7.2.7 Test the tunnel function (ping test)

How can you test the configured function?

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

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

Note

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

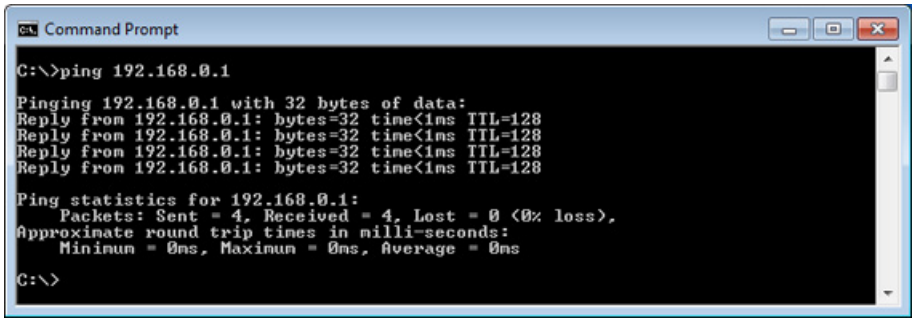
Test phase 1

Now test the function of the established tunnel connection as follows:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to PC1 (IP address 192.168.0.1).

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.0.1" at the cursor position.

You will then receive the following message (positive reply from PC1):



Result

If the IP packets have reached PC1, the "Ping statistics for 192.168.0.1" display the following:

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

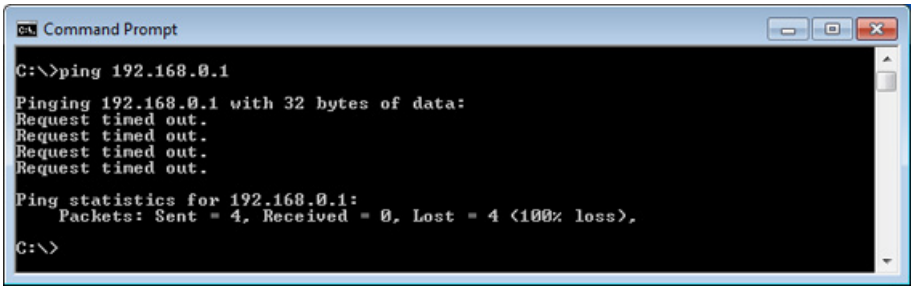
Since no other communication is permitted, these packets must have been transported through the VPN tunnel.

Test phase 2

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

1. On PC3, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Send the same ping command ("ping 192.168.0.1") in the Command Prompt window of PC3.

You will then receive the following message (no reply from PC1):



Result

The IP packets from PC3 cannot reach PC1 since neither tunnel communication between these two devices is configured nor is normal IP data traffic permitted.

This is shown in the "Ping statistics" for 192.168.0.1 as follows:

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

7.3 Remote access - VPN tunnel example with SCALANCE M and SOFTNET Security Client

7.3.1 Overview

In this example, the VPN tunnel function is configured in the "advanced mode" project engineering view. A SCALANCE M and the SOFTNET Security Client form the two tunnel endpoints for the secure tunnel connection via a public network.

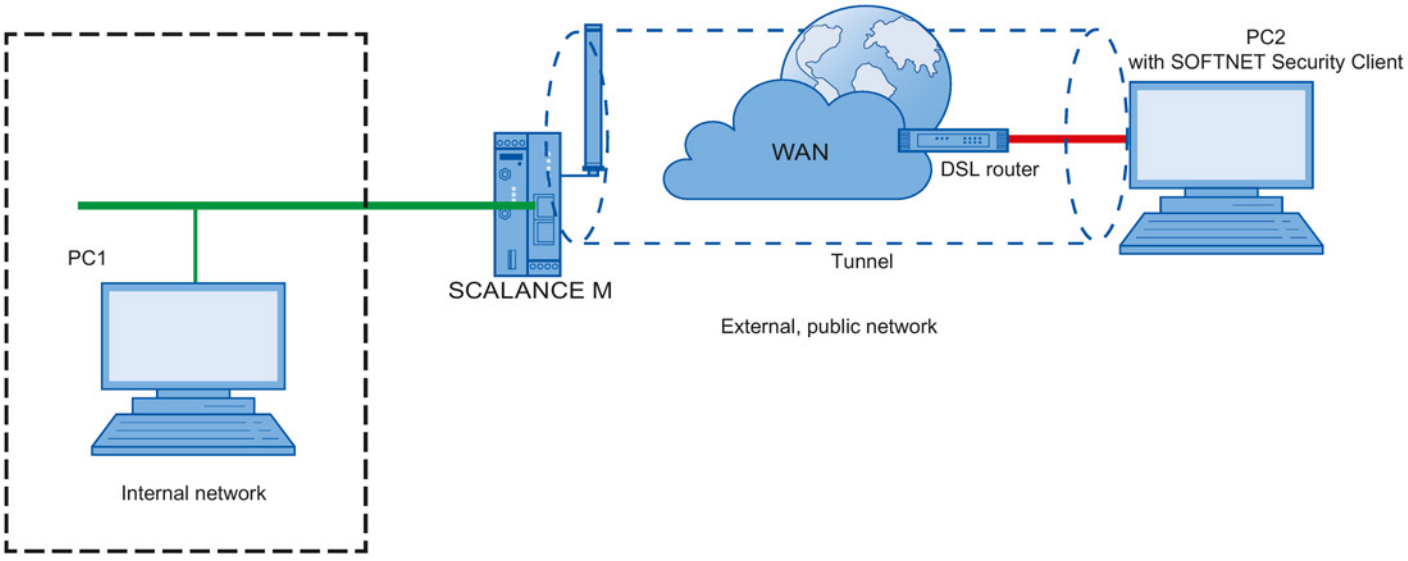
With this configuration, IP traffic is possible only over the established VPN tunnel connection with authorized partners.

Note

To configure this example, you need a public, fixed IP address from your provider (mobile wireless provider) for the SIM card of the SCALANCE M that can also be reached from the Internet.

As an alternative, it is also possible to work with a DynDNS address for the SCALANCE M.

Setting up the test network:



- Internal network - attachment to SCALANCE M interface X2 ("internal network")

  In the test setup, in the internal network, a network node is implemented by a PC connected to the internal interface ("X2") of a SCALANCE M module.

  – PC1: Represents a node in the internal network
- SCALANCE M: SCALANCE M module for protection of the internal network

- External, public network - connection via SCALANCE M antenna ("external network")

  The external, public network is a GSM or mobile wireless network for the SCALANCE M that can be selected by the user at the provider (mobile wireless provider) and that is reached via the antenna of the SCALANCE M module. PC2 connects via a suitable SIM card of a provider to a GSM or mobile wireless network or is connected to the Internet via a DSL router.

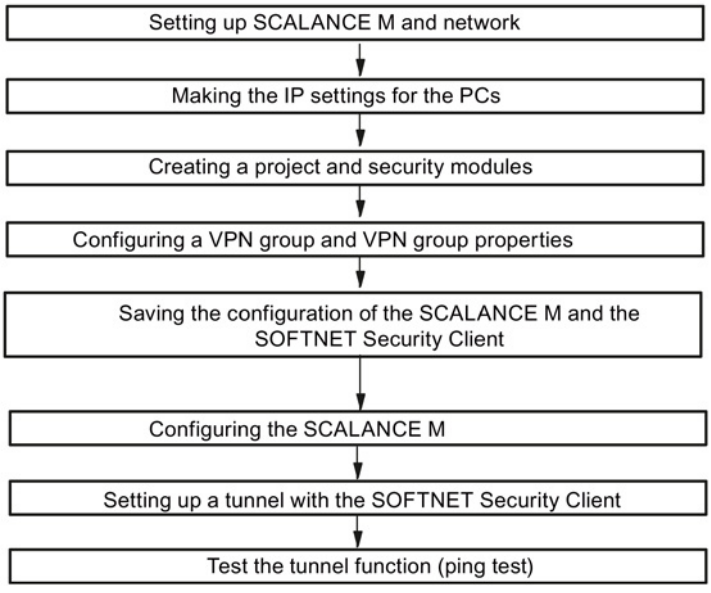
  – PC2: PC with Security Configuration Tool configuration software and the SOFTNET Security Client software for secure VPN access to the internal network

Required devices/components:

Use the following components to set up the network:

- 1 x SCALANCE M module with SIM card, (optional: a suitably installed DIN rail with fittings);
- 1 x 24 V power supply with cable connector and terminal block plug;
- 1 x PC on which the "Security Configuration Tool" and VPN client "SOFTNET Security Client" are installed;
- 1 x PC in the internal network of the SCALANCE M with a Web browser for configuring the SCALANCE M and testing the configuration;
- 1 x DSL router (connection to the Internet for the PC with the VPN client (ISDN, DSL, UMTS etc.));
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

Overview of the next steps



7.3.2 Setting up SCALANCE M and network

Follow the steps outlined below:

1. First unpack the SCALANCE M and check that it is undamaged.
2. Follow the step-by-step commissioning as described in the SCALANCE M system manual up to the point at which you need to set it up to suit your own requirements. Use PC1 for this.
3. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   - Connect PC1 with the internal interface X2 ("internal network") of the SCALANCE M
   - Connect PC2 with the DSL router
4. Now turn on the PCs involved.
   Setting up the SCALANCE M, see section:
   Configuring the SCALANCE M (Page 196)

7.3.3 Make the IP settings for the PCs

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

PC	IP address	Subnet mask	Default gateway
PC1	192.168.1.101	255.255.255.0	192.168.1.1
PC2	192.168.2.202	255.255.255.0	192.168.2.1

For the default gateway for PC1, specify the IP address that you will assign to the SCALANCE M module for the internal network interface in the subsequent configuration. Specify the IP address of the DSL router for PC2.

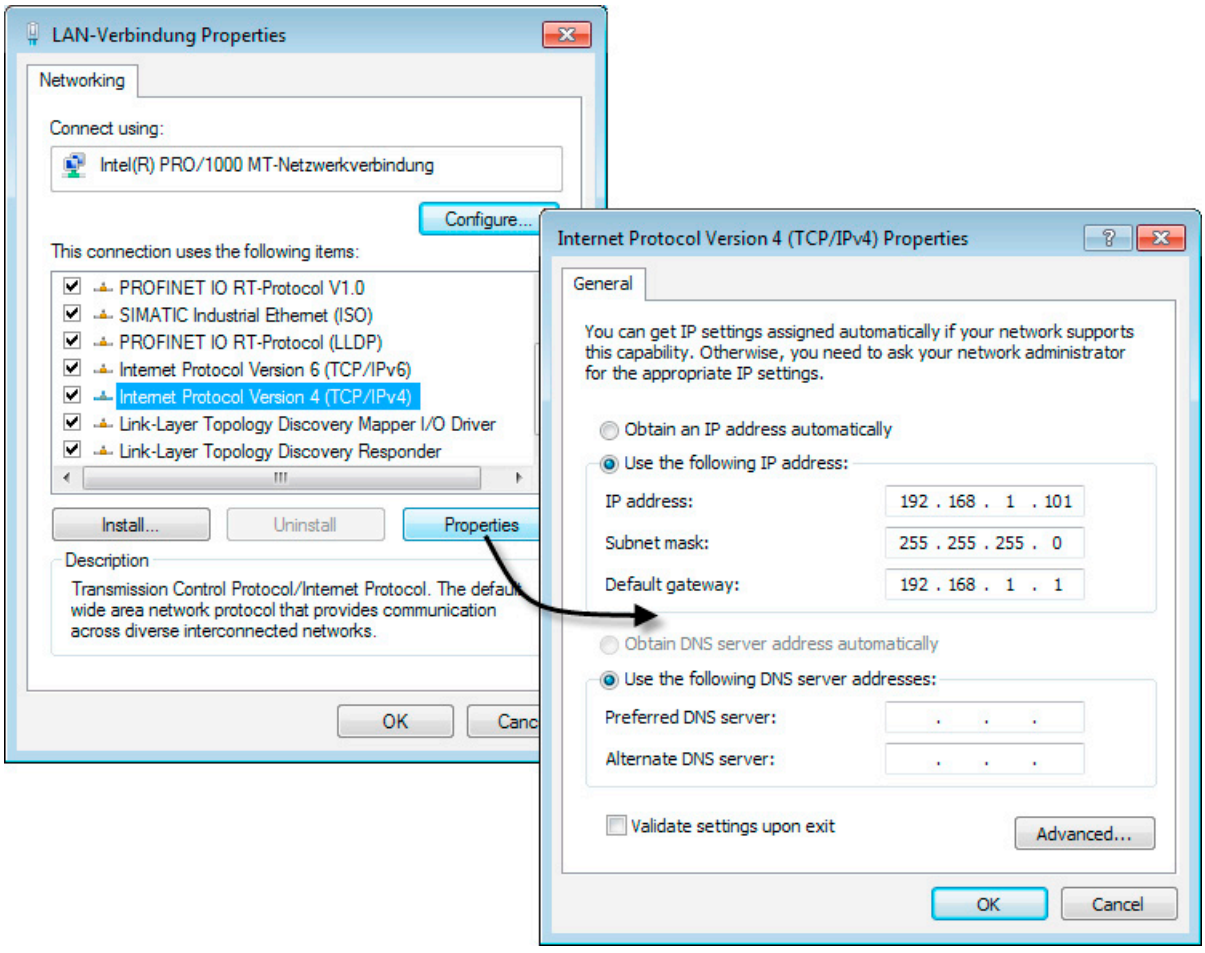
Note

The IP address of PC2 must be located in the internal network of the DSL router (192.168.2.0/24).

Follow the steps below for both PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

4. Click the "Properties" button.



5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.
6. Enter the values assigned to the PC from the table "Make the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

7.3.4 Creating a project and security modules

Follow the steps below:

1. Install and start the Security Configuration Tool on PC2.
2. Select the "Project" > "New..." menu command.
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.

4. Confirm your entries.

   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.

5. Configure the following parameters:
   - Product type: SOFTNET Configuration (SOFTNET Security Client, VPN device, NCP VPN client)
   - Module: SOFTNET Security Client
   - Firmware release: V4

     Note: With the selection of the option “V4”t, the full range of functions of SOFTNET Security V4 and SOFTNET Security client V5 ia available.

     Assign the module name "SSC-PC2" and close the dialog with "OK".

6. Click on the "All modules" object in the navigation panel.
7. Generate a second module with the "Insert" > "Module" menu command. Configure the following parameters:
   - Product type: SCALANCE M
   - Module: SCALANCE M875/MD741-1
   - Firmware release: V1
8. In the "Configuration" area, assign the module name "SCALANCE-M" and enter the external IP address and the external subnet mask you have received from your provider in the required format.

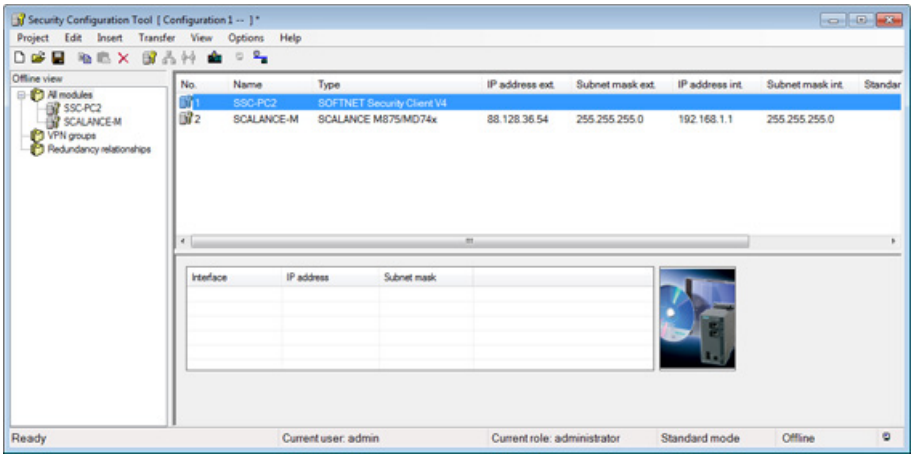
   Note

   To configure this example, you need a public, fixed IP address from your provider (mobile wireless provider) for the SIM card of the SCALANCE M that can also be reached from the Internet. Enter this IP address as the external IP address for your module.

   If you work with dynamic addresses for the SCALANCE M, you require a DynDNS address for the module. In this case, you do not need to adapt the external IP address at this point. The IP address entered therefore serves simply as a placeholder. When configuring the SOFTNET Security Client later, specify a DNS name instead of an external IP address.

9. In the "Configuration" area, enter the internal IP address (192.168.1.1) and the internal subnet mask (255.255.255.0) in the required format and confirm the dialog with "OK".

   Result: The settings are complete and should match the following figure:



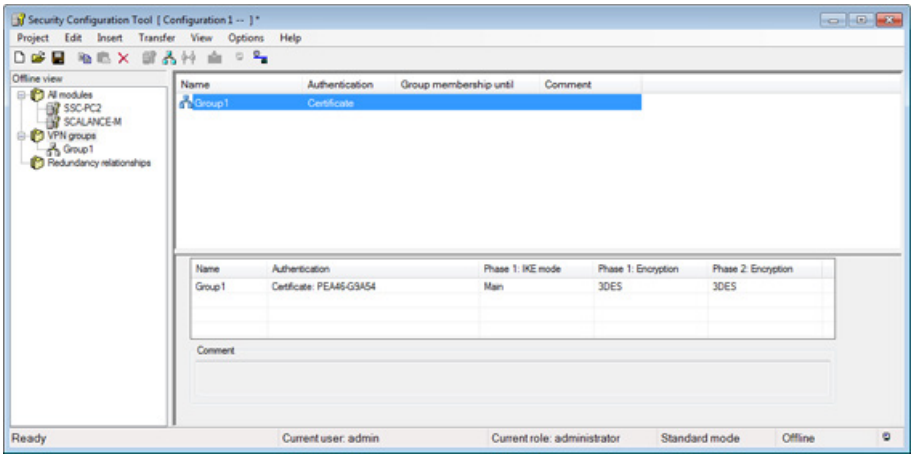
7.3.5 Configuring a VPN group and VPN group properties

A SCALANCE M and the SOFTNET Security Client can establish an IPsec tunnel for secure communication when they are assigned to the same group in the project.

Follow the steps outlined below:

1. Select the "VPN groups" object in the navigation panel and select the "Insert" > "Group" menu command.

   Result: The VPN group is created. The VPN group is automatically given the name "Group1".



2. Select the "All modules" object in the navigation panel.
3. Select the SCALANCE M module in the content area and drag it to the VPN group "Group1" in the navigation panel.

   Result: The module is assigned to this VPN group.

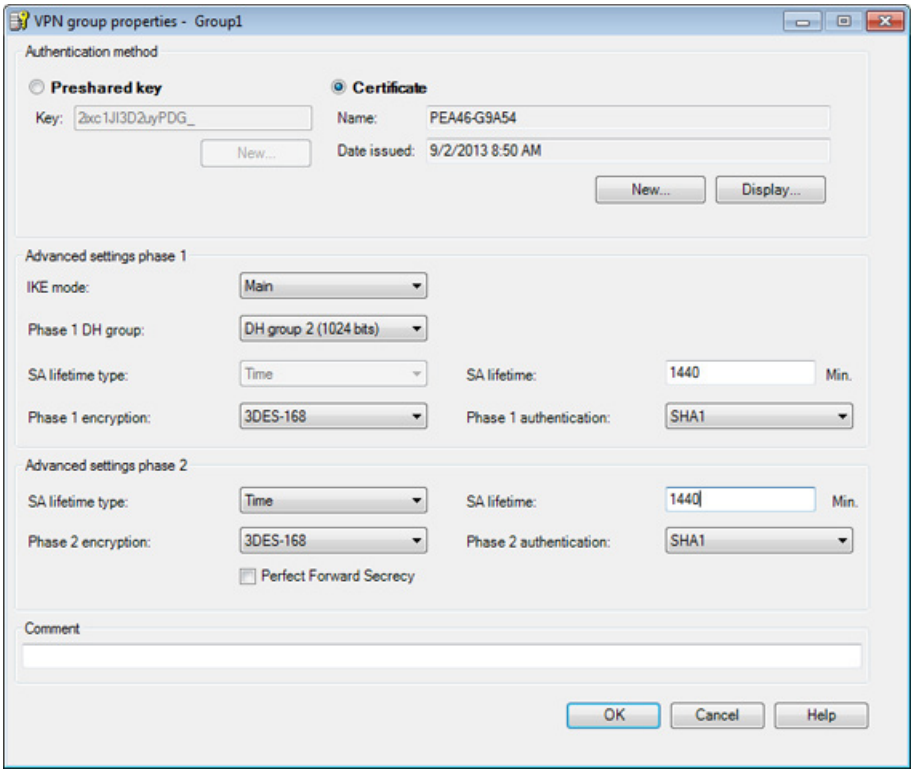
   The color of the key symbol changes from gray to blue.

4. Select the SOFTNET Security Client module "SSC-PC2" in the content area and drag it to the VPN group "Group1" in the navigation panel.

   Result: The module is also assigned to this VPN group.

   The color of the key symbol changes from gray to blue.

5. Change to advanced mode with the menu command "View" > "Advanced mode".
6. Select the VPN group "Group1" in the navigation panel.
7. Select the "Edit" > "Properties..." menu command to open the VPN group properties of the VPN group.
8. Change the SA lifetime for phase 1 and phase 2 to 1440 minutes and leave all other settings. Using parameters that differ from the figure below may mean that the two tunnel partners cannot establish a VPN connection to each other.



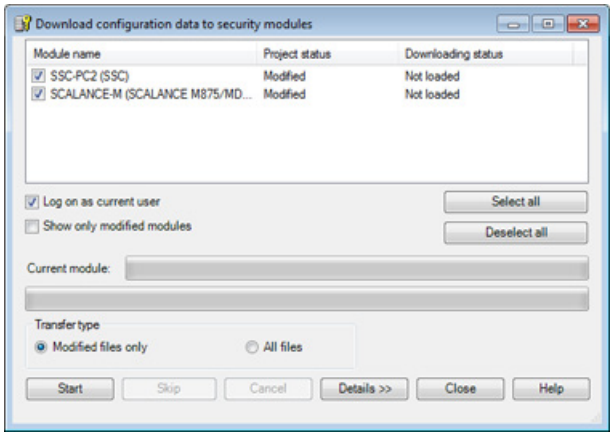
9. Save the project with the "Project" > "Save" menu command.

The configuration of the tunnel connection is complete.

7.3.6 Saving the configuration of the SCALANCE M and the SOFTNET Security Client

Follow the steps outlined below:

1. Using the menu command "Transfer" > "To all modules...", open the following dialog:



2. Start the download with the "Start" button.
3. Save the configuration file "projectname.SSC-PC2.dat" in the project folder and assign a password for the private key of the certificate. The following files will be saved in the project directory:
   - "Projectname.SSC-PC2.dat"
   - "Projectname.string.SSC-PC2.p12"
   - "Projectname.group1.cer"
4. Save the configuration file "projectname.SCALANCE-M.txt" in your project folder and assign a password for the private key of the certificate. The following files will be saved in the project directory:
   - "Projectname.SCALANCE-M.txt"
   - "Projectname.string.SCALANCE-M.p12"
   - "Projectname.group1.SCALANCE- M.cer"

You have now saved all the necessary files and certificates and can put the SCALANCE M and the SOFTNET Security Client into operation.

7.3.7 Configuring the SCALANCE M

By using the saved text file "projectname.SCALANCE-M.txt", you can create the configuration of the SCALANCE M very simply based on its Web user interface. Below, this example shows you the configuration of the SCALANCE M step-by-step.

The following is assumed for the configuration:

- SCALANCE M can be reached via the Internet suing a public, fixed IP address;
- The SOFTNET Security Client uses a dynamic IP address.

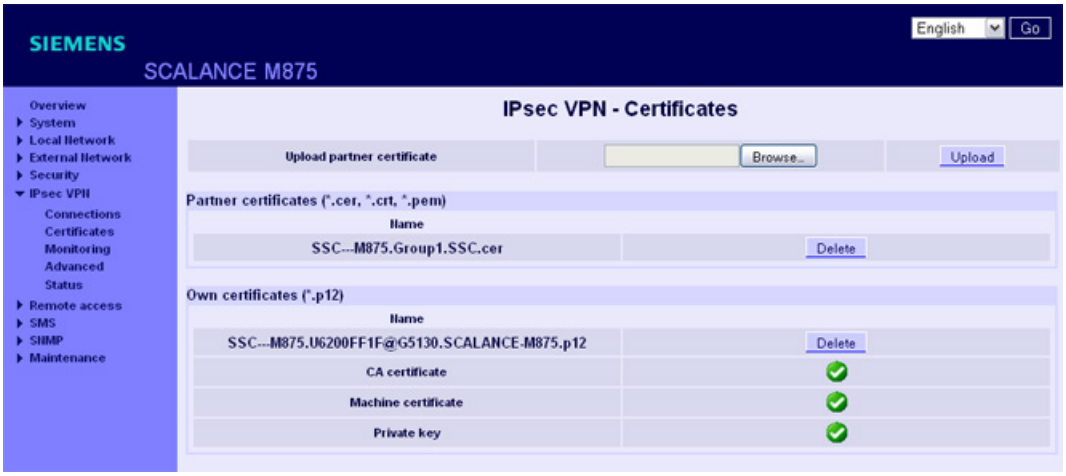
At the relevant points, you will also be given information about configuring a DynDNS name for the SCALANCE M.

Follow the steps outlined below:

1. Connect to the Web user interface of the SCALANCE M via PC1.

   Note: If the SCALANCE M has its factory settings, the internal interface of the module has the IP address 192.168.1.1

2. Go to the "IPSec VPN" > "Certificates" folder.
3. You saved the required certificates on PC2 in the last section and assigned a password for the private key. Transfer the certificates ("projectname.string.SCALANCE-M.p12", "projectname.group1.SCALANCE-M.cer") for the SCALANCE M initially to PC1.
4. Now download the certificate of the partner "projectname.group1.SCALANCE-M.cer" and the PKCS 12 file "projectname.string.SCALANCE-M.p12" to the module.



VPN Roadwarrior mode of the SCALANCE M

Since the SOFTNET Security Client is connected to the Internet using a dynamic IP address, the VPN Roadwarrior mode of the SCALANCE M is used to establish a secure connection.

- Roadwarrior mode of the SCALANCE M:
  - In the VPN Roadwarrior mode, the SCALANCE M can accept VPN connections from partners with an unknown address. These can, for example, be mobile partners that obtain their IP address dynamically.
  - The VPN connection must be established by the partner. Only one VPN connection is possible in Roadwarrior mode. VPN connections in standard mode can be operated at the same time.

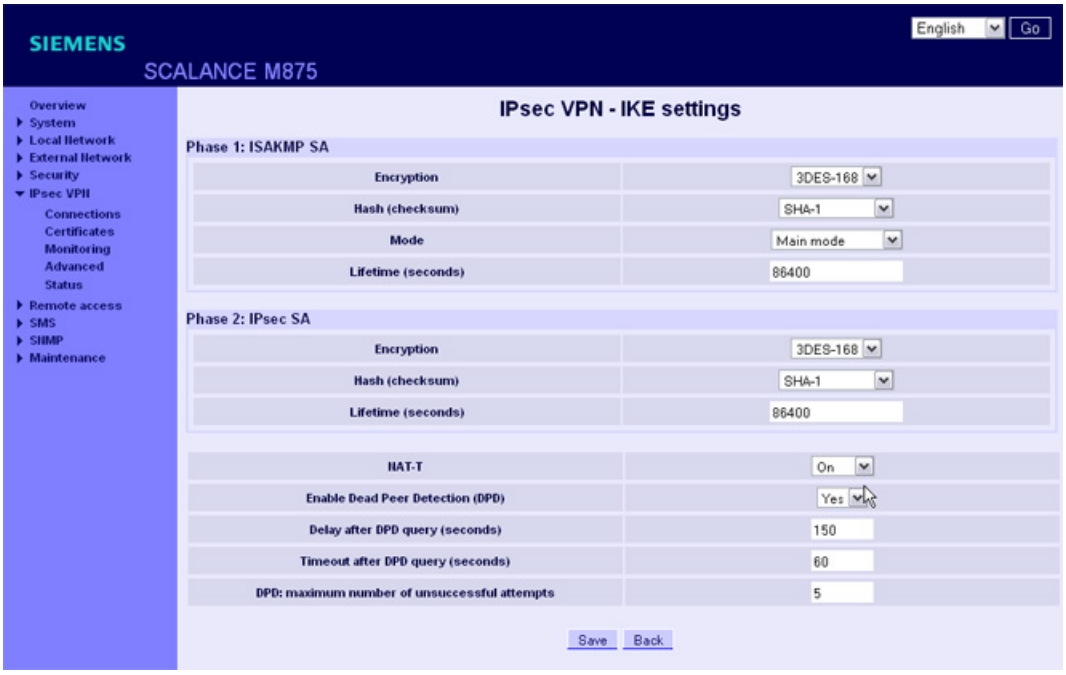
Follow the steps outlined below:

1. Go to the "IPSec VPN" > "Connections" folder.
2. Under "Settings", click the "Edit" button.
3. Edit the settings of the Roadwarrior VPN as shown in the following figure and save your entries.

   You can get the "remote ID" from the "projectname.SCALANCE-M.txt" text file. As an option, you can enter the remote ID here.

4. In the "IPSec VPN - Connections" window, click the "Edit" button below IKE.

5. Edit the IKE settings of the Roadwarrior VPN as shown in the following figure and save your entries.



Note

A successful tunnel connection between SCALANCE M and the SOFTNET Security Client can only be established if you keep exactly to the parameters listed below.

If you use different parameter settings, the two tunnel partners will not be able to set up a VPN connection between them.

Authentication method: X509 partner certificate

Phase 1 - ISKAMP SA:

- ISAKMP SA encryption: 3DES-168
- ISAKMP-SA hash: SHA-1
- ISAKMP-SA mode: Main mode
- ISAKMP-SA Lifetime (seconds): 86400

Phase 2 - IPSec SA:

- IPSec SA encryption: 3DES-168
- IPSec SA hash: SHA-1
- IPSec SA lifetime (seconds): 86400

DH/PFS group: DH-2 1024

6. To be able to use the diagnostics function of the SOFTNET Security Client for successfully established VPN tunnels in conjunction with the SCALANCE M, you need to allow a ping from the external network of the SCALANCE M.

   To do this, go to the directory "Security" > "Advanced".

Set the "External ICMP to the SCALANCE M" setting to the value "Allow ping" and save your entry.

Note

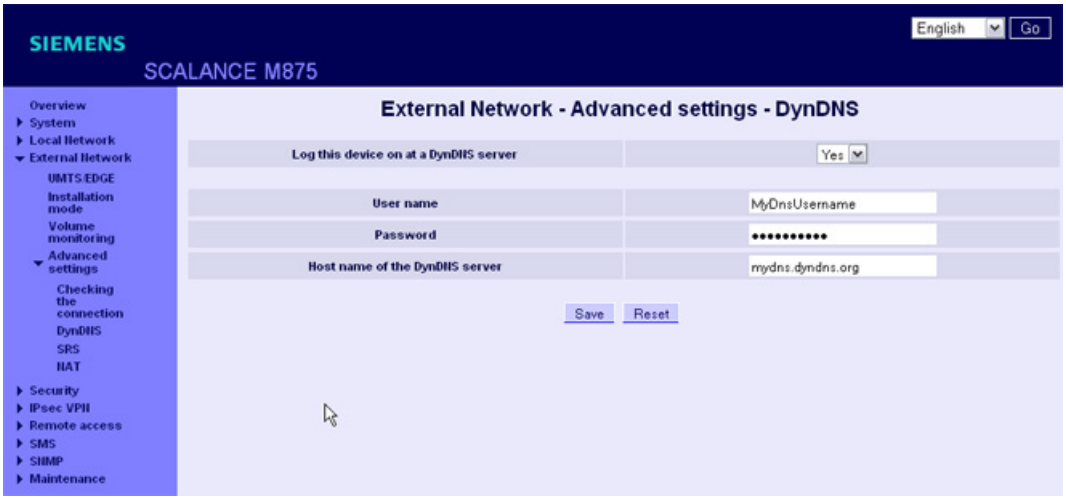
If you do not enable this function, you will not be able to use the diagnostics function of the SOFTNET Security Client for successfully established VPN tunnels in conjunction with the SCALANCE M. You then do not receive any feedback as to whether the tunnel was successfully established but can nevertheless communicate securely via the tunnel. You then do not receive any message that the tunnel was successfully established but can nevertheless communicate securely via the tunnel.

Note

If you want to access the SCALANCE M using a DNS name, make the settings for the DynDNS server connection in the following directory. The SCALANCE M supports only the "dyndns.org" provider.

"External Network" > "Advanced Settings" >"DynDNS"

1. Change the setting "Log this device on at a DynDNS server" to the value "Yes".
2. Specify your user name and the password of your DynDNS account.
3. Enter the full DynDNS address in the "Host name of the DynDNS server" box. Enter the domain for this address as well (e.g. "mydns.dyndns.org").

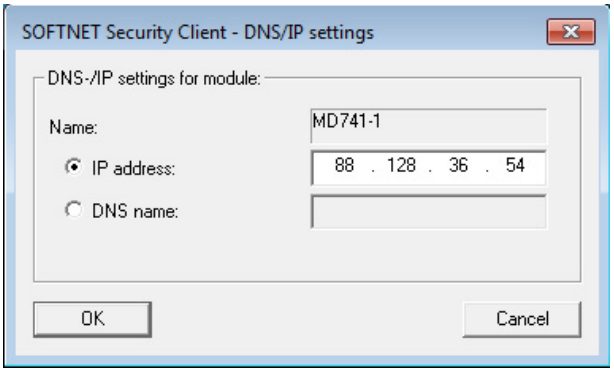


7.3.8 Setting up a tunnel with the SOFTNET Security Client

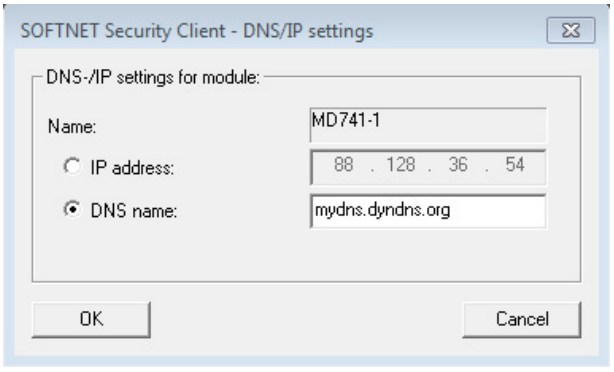
Follow the steps outlined below:

1. Start the SOFTNET Security Client on PC2.
2. Click the "Load Configuration" button, change to your project folder and load the "Projectname.SSC-PC2.dat" configuration file.

3. For a SCALANCE M configuration, the SOFTNET Security Client opens the dialog “DNS/IP settings". In this dialog, enter the public IP address of the SCALANCE M module that you received from your provider. Confirm the dialog with "OK".



Note: If you work with a DNS name, you can configure this instead of an IP address in this dialog.



4. In the "VPN configuration" dialog, enable the "Establish VPN tunnel to the internal nodes" check box.
5. Select the network adapter from whose IP the VPN tunnel will be established.
6. Enter the password for the private key of the certificate and confirm with "Next".
7. Click the "Tunnel Overview" button.

Result: Active tunnel connection

The tunnel between SCALANCE M and SOFTNET Security Client was established.

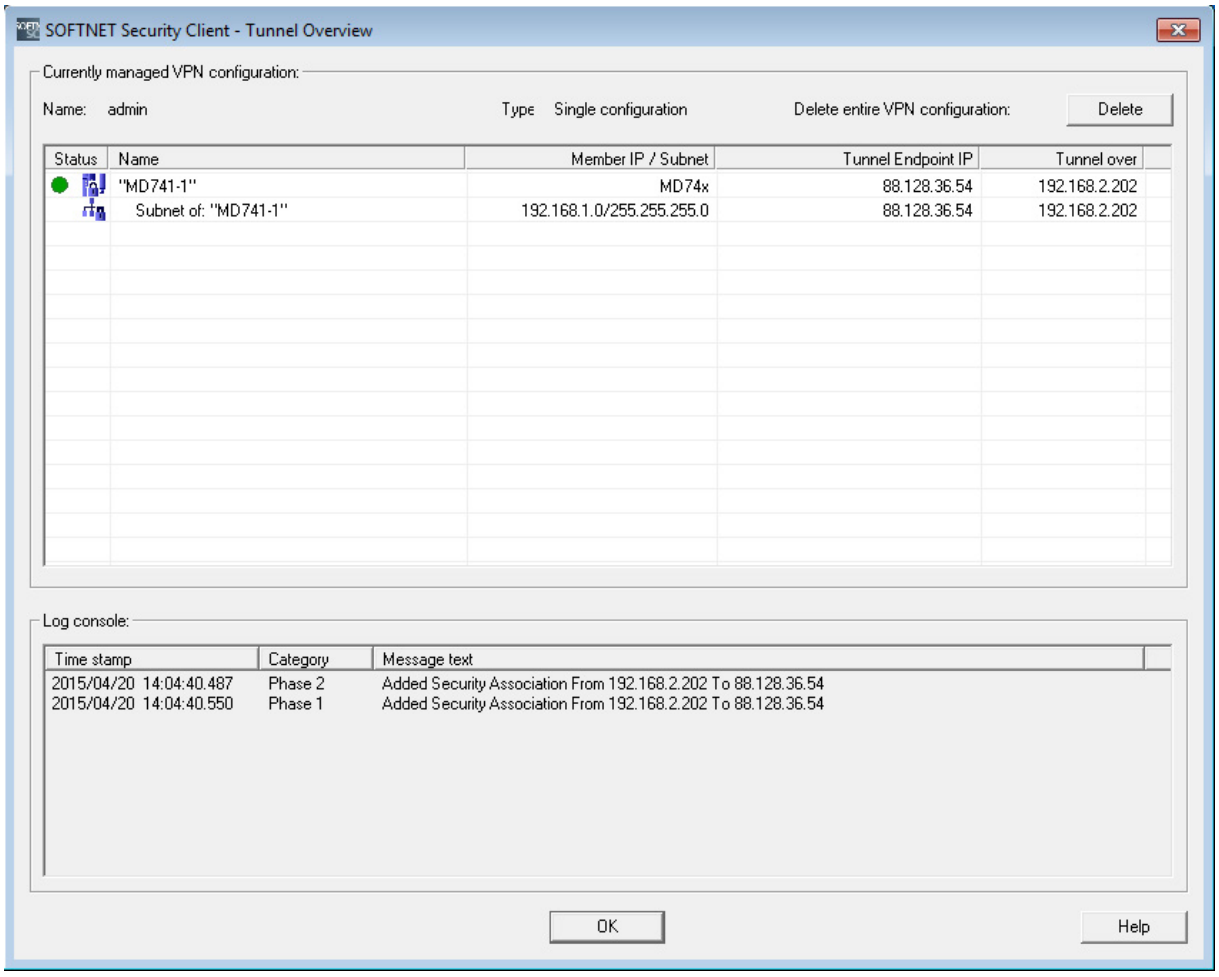
The blue icon beside the "MD741-1" entry indicates that a policy was created for this communication connection.

Accessibility of the SCALANCE M is indicated by the "green circle" beside the "MD741-1" entry.

Note

Remember that this function depends on enabling the ping function on the SCALANCE M module.

In the Logging Console of the Tunnel Overview, among other things information on the sequence of executed connection attempts is displayed.



The commissioning of the configuration is now complete. The SCALANCE M and the SOFTNET Security Client have established a communication tunnel over which network nodes can communicate securely with PC2 from within the internal network.

7.3.9 Test the tunnel function (ping test)

How can you test the configured function?

The function is tested as described below using a ping command.

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

Note

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

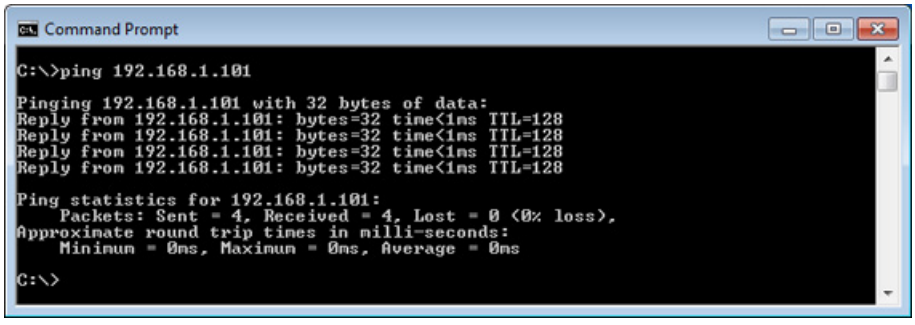
Testing

Now test the function of the established tunnel connection as follows:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to PC1 (IP address 192.168.1.101).

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.1.101" at the cursor position.

You will then receive the following message (positive reply from PC1):



Result

If the IP packets have reached PC1, the "Ping statistics for 192.168.1.101" display the following:

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

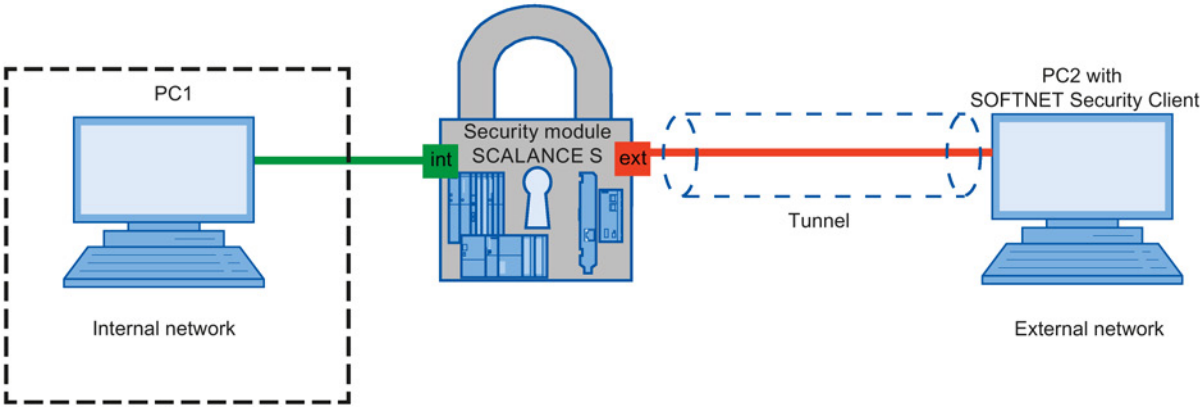
Since no other communication is permitted, these packets must have been transported through the VPN tunnel.

7.4 Remote access - SCALANCE S and SOFTNET Security Client with user-specific access

7.4.1 Overview

Overview

In this example, a VPN tunnel is established between a PC and a security module using the SOFTNET Security Client. Downstream from the security module there is a PC in the internal network. The firewall is now configured in the Security Configuration Tool so that access from PC2 in the external network to PC1 in the protected internal network behind the security module via the VPN tunnel is possible for a specific user only.



Required devices/components:

Use the following components to set up the network:

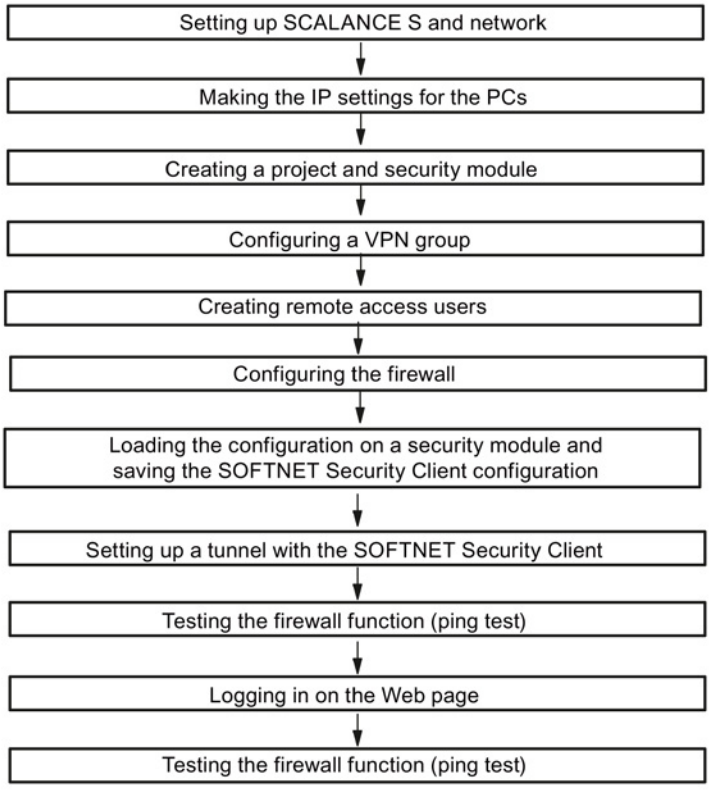
- 1 x SCALANCE S612 module, (option: a suitably installed DIN rail with fittings);
- 1 x 24 V power supply with cable connector and terminal block plug;
- 1 x PC in the external network on which the Security Configuration Tool as well as SOFTNET Security Client are installed;
- 1 x PC in the internal network to test the configuration;
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

Requirement:

To be able to work through the example, the following requirements must be met:

- The Security Configuration Tool configuration software and the SOFTNET Security Client are installed on PC2.

Overview of the next steps:



7.4.2 Setting up SCALANCE S and network

Follow the steps below:

1. First unpack the SCALANCE S and check that it is undamaged.
2. Connect the power supply to the SCALANCE S.

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

⚠ WARNING
Use safety extra-low voltage only The SCALANCE S is designed for operation with safety extra-low voltage. This means that only safety extra-low voltages (SELV) complying with IEC950/EN60950/ VDE0805 can be connected to the power supply terminals. The power supply unit to supply the SCALANCE S must comply with NEC Class 2 (voltage range 18 - 32 V, current requirement approx. 250 mA)

3. Now establish the physical network connections by plugging the network cable connectors into the interfaces being used:
   – Connect PC1 to the internal interface of the security module.
   – Connect PC2 to the external interface of the security module.
4. Now turn on the PCs.

Note

The Ethernet interfaces are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network:

- Interface X1 - external network
  Red marking = unprotected network area;
- Interface X2 - internal network
  Green marking = network protected by SCALANCE S;

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

7.4.3 Making the IP settings for the PCs

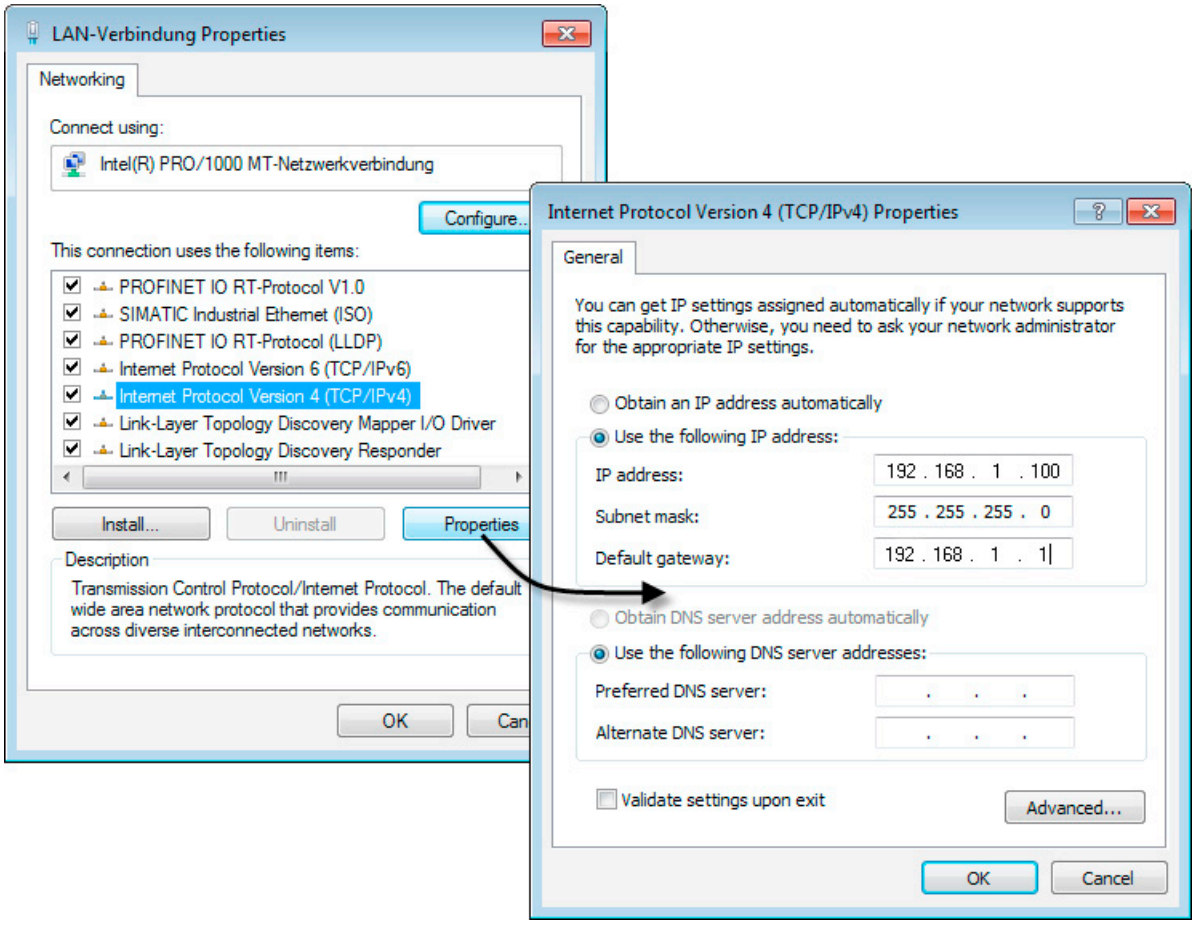
For the test, the PCs are given the following IP address settings:

PC	IP address	Subnet mask	Default gateway
PC1	192.168.1.100	255.255.255.0	192.168.1.1
PC2	192.168.2.100	255.255.255.0	192.168.2.1

Follow the steps below for PC1 and PC2:

1. On the relevant PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Click the "Properties" button.

5. In the "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog, select the "Use the following IP address" radio button: off.



6. Now enter the values assigned to the PC from the table "Making the IP settings for the PCs" in the relevant boxes.
7. Close the dialogs with "OK" and close the Control Panel.

7.4.4 Creating a project and security module

Follow the steps below:

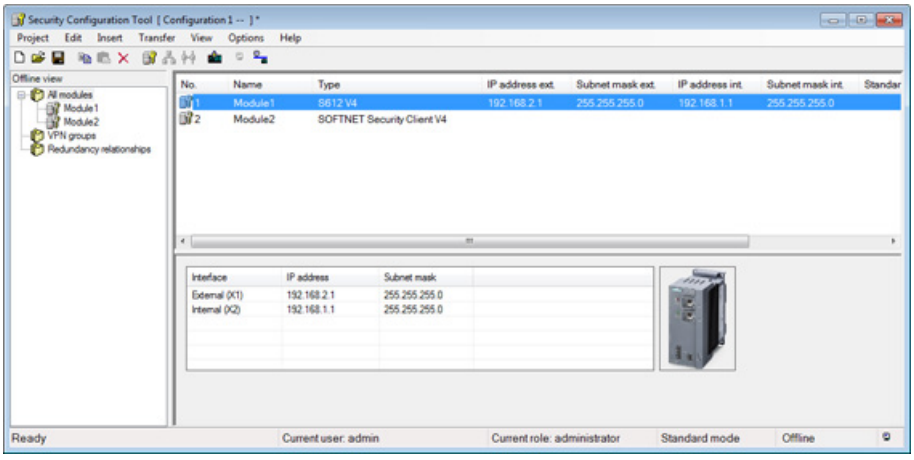
1. Install and start the Security Configuration Tool on PC2.
2. Select the "Project" > "New..." menu command in the Security Configuration tool.
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
4. Confirm your entries with "OK".

   Result: A new project is created. The "Selection of a module or software configuration" dialog opens.

5. In the "Product type", "Module" and "Firmware release" areas, select the following options:
   - Product type: SCALANCE S
   - Module: S612
   - Firmware release: V4
6. In the "Configuration" area, enter the MAC address in the required format. The MAC address is printed on the front of the SCALANCE S module.
7. In the "Configuration" area, enter the external IP address (192.168.2.1) and the external subnet mask (255.255.255.0) in the required format.
8. From the drop-down list "Interface routing external/internal", select the "Routing mode".
9. Enter the internal IP address (192.168.1.1) and the internal subnet mask (255.255.255.0) in the required format and confirm the dialog with "OK".
10. Use the "Insert" > "Module" menu command to create a new module with the following parameters:
    - Product type: SOFTNET Configuration (SOFTNET Security Client, VPN device, NCP VPN client)
    - Module: SOFTNET Security Client
    - Firmware release: V4

      Note: With the selection of the option “V4”t, the full range of functions of SOFTNET Security V4 and SOFTNET Security client V5 ia available.

Result: The modules are created and are shown in the content area of the Security Configuration Tool.



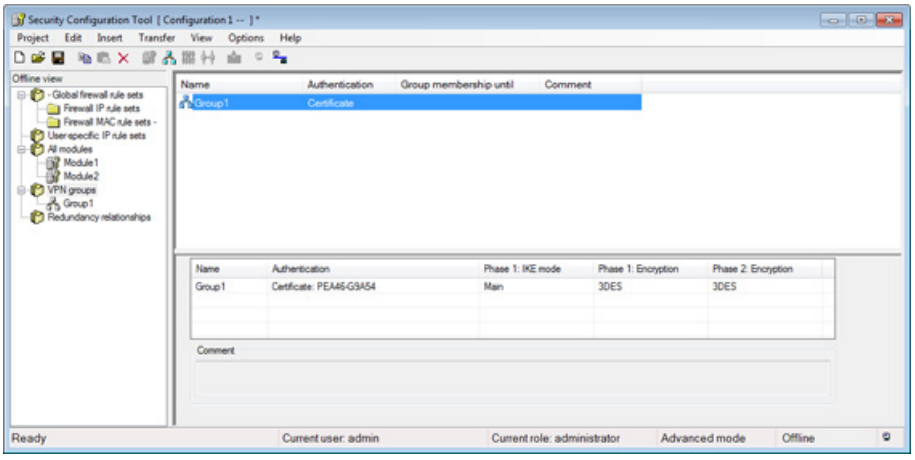
7.4.5 Configuring a VPN group

Two security modules can establish an IPsec tunnel for secure communication if they are assigned to the same VPN group in the project.

Follow the steps outlined below:

1. Change the configuration view to advanced mode with the menu command "View" > "Advanced mode".
2. Select the "VPN groups" object in the navigation panel and create a new VPN group with the menu command "Insert" > "Group".

   Result: The VPN group is created. The VPN group is automatically given the name "Group1".



3. In the navigation panel, click on the "All modules" object and then on the first security module in the content area.
4. Drag the security module to the VPN group "Group1" in the navigation panel.

   Result: The security module is now assigned to this VPN group.

   The color of the key symbol changes from gray to blue.
5. Select the second security module in the content area and drag it to the VPN group "Group1" in the navigation panel.

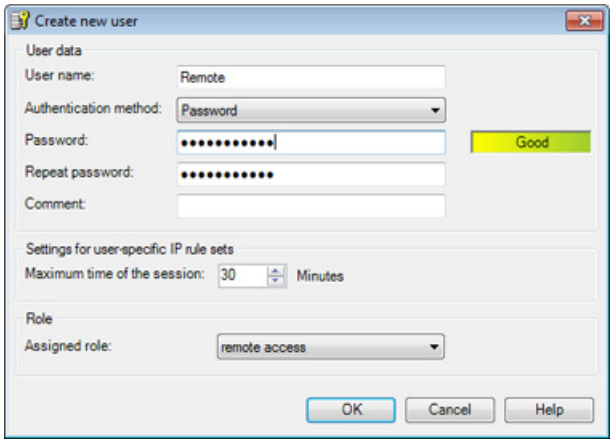
Result: The second security module is now also assigned to this VPN group and the configuration of the tunnel connection is complete.

7.4.6 Creating remote access users

Creating a remote access user

1. Select the "Options" > "User management..." menu command.
2. Click the "Add..." button in the "User" tab.

3. Create a new user with the following settings:



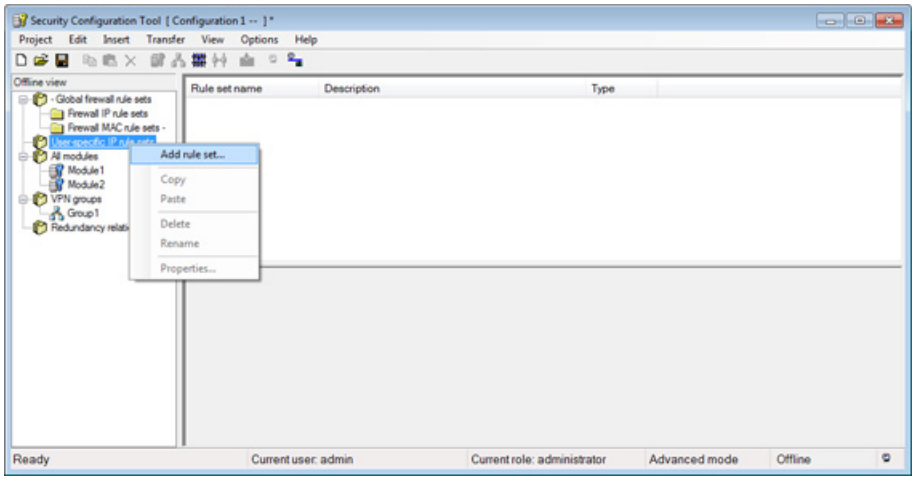
4. Close the dialog with "OK".
5. Close the user management with "OK".

7.4.7 Configuring a firewall

In this example, configure the firewall so that access via a VPN tunnel to the PC in the internal network is only possible for the created remote access user.

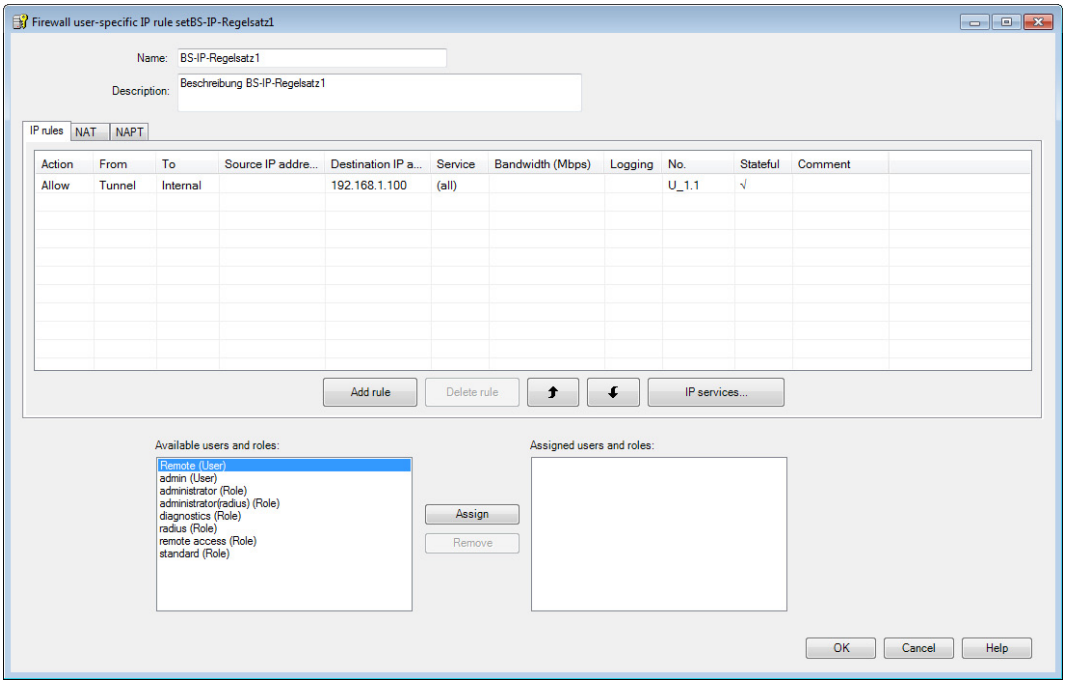
Setting a user-specific firewall rule set - Follow the steps below:

1. Select the "User-specific IP rule sets" object in the navigation panel.
2. Select the "Insert rule set..." entry in the shortcut menu.



3. Click the "Add rule" button in the dialog that opens to add a new rule.

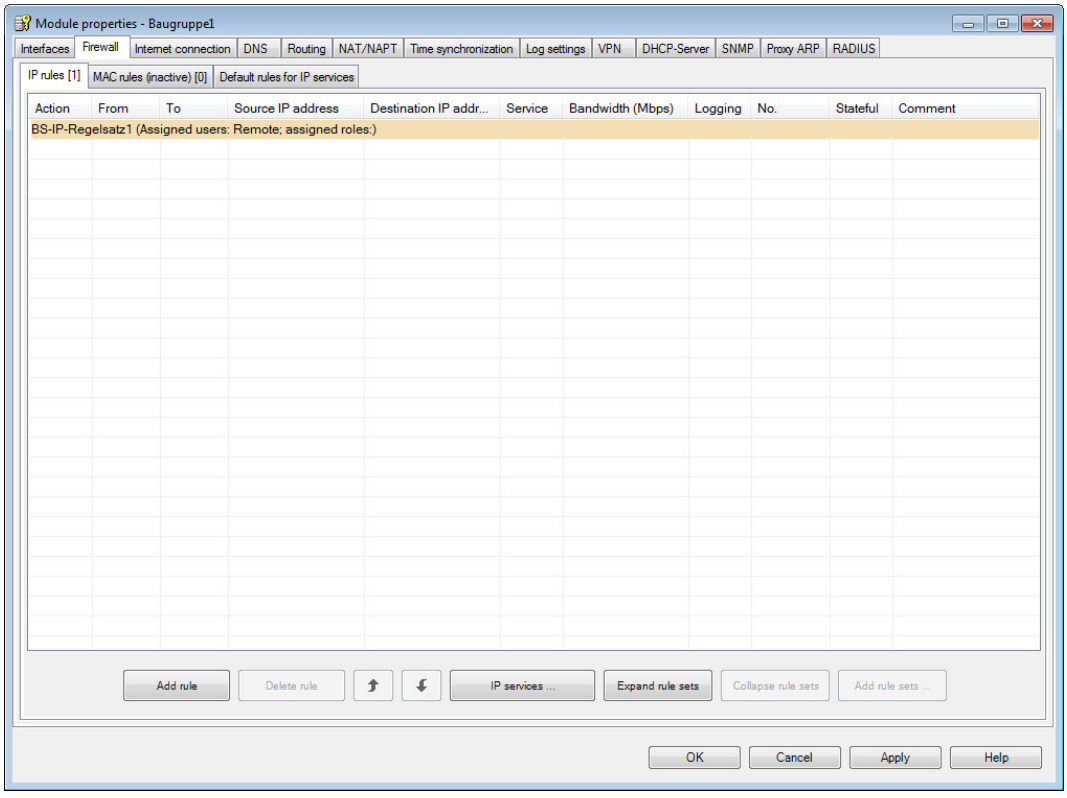
4. Enter an IP rule set as shown below:



5. From the "Available users and roles" list, select the "Remote (user)" entry and click the "Assign" button.
6. Confirm the dialog with "OK".

Assigning a user-specific firewall rule set - Follow the steps below:

1. In the navigation panel, click the "All modules" entry, select the security module of the type "S612 V4" in the content area and holding down the left mouse button drag it to the newly created user-specific firewall rule set.
2. You can check the assignment by opening the dialog for setting the module properties and selecting the "Firewall" tab. The user-specific IP rule set was saved in the "IP rules" tab.

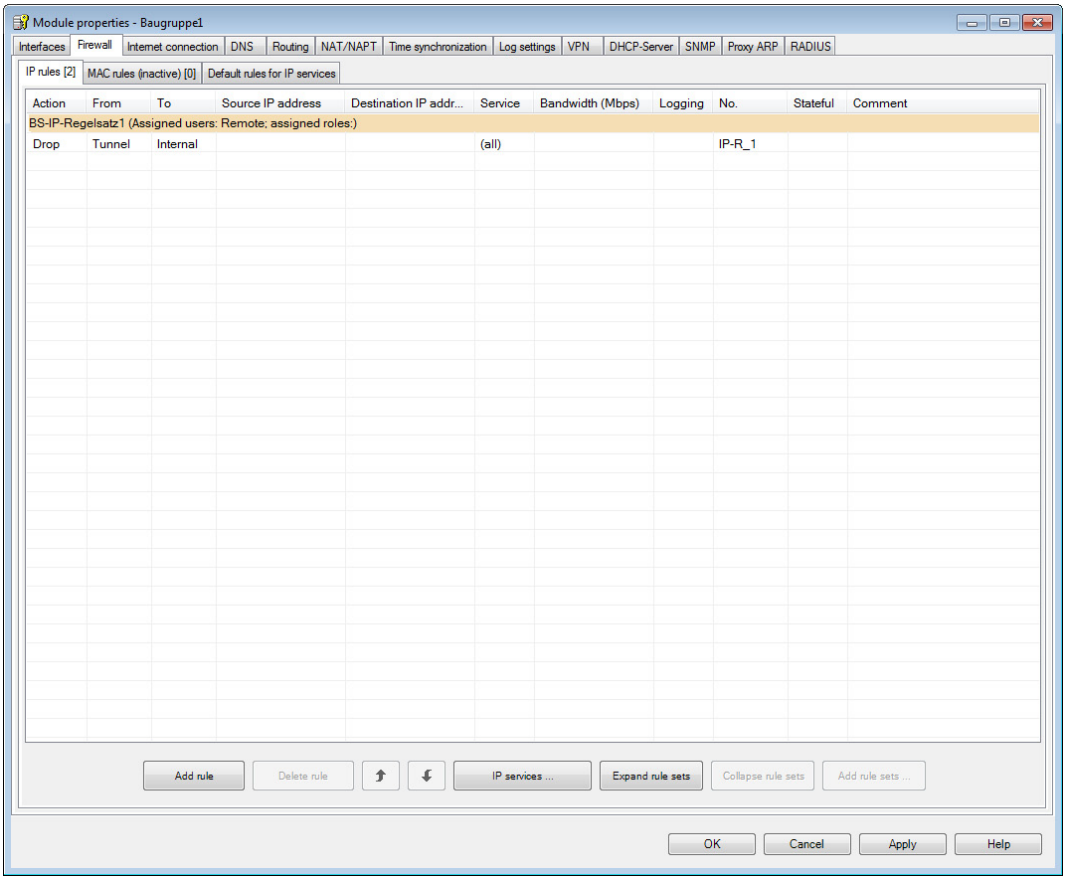


3. If you click the "Expand rule sets" button, you can view the IP rule set in detail.
4. Click the "OK" button.

Setting local firewall rules - Follow the steps below:

1. Select the security module of the type "S612 V4" in the content area.
2. Select the "Edit" > "Properties..." menu command.
3. Select the "Firewall" tab and click on the "Add rule" button.

4. Enter the rule as shown below:

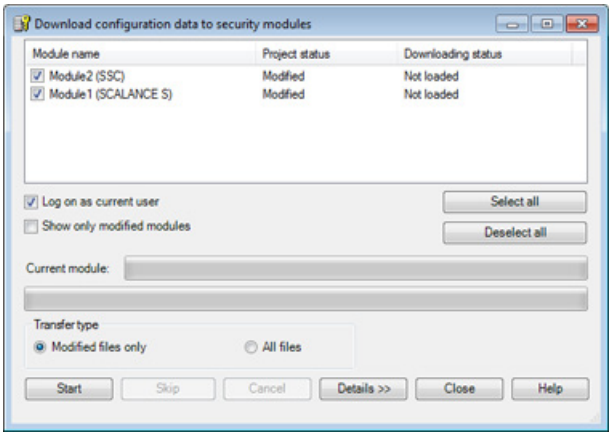


5. Confirm the dialog with "OK".

7.4.8 Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

Follow the steps below:

1. Select the "Project" > "Save" menu command.
2. Using the menu command "Transfer" > "To all modules...", open the following dialog:



3. Start the download with the "Start" button.
4. Save the configuration file in your project folder and assign a password for the private key of the certificate.

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

Result: SCALANCE S in productive operation

The security module is in productive operation. This mode is indicated by the Fault LED being lit green.

7.4.9 Setting up a tunnel with the SOFTNET Security Client

Follow the steps outlined below:

1. Start the SOFTNET Security Client on PC2.
2. Click the "Load Configuration" button, change to your project folder and load the "Projectname.SSC-PC2.dat" configuration file.
3. In the "VPN configuration" dialog, enable the "Establish VPN tunnel to the internal nodes" check box.
4. Select the network adapter from whose IP the VPN tunnel will be established.
5. Enter the password for the private key of the certificate and confirm with "Next".
6. Click the "Tunnel Overview" button.

Result: Active tunnel connection

The commissioning of the configuration is completed and the security module and the SOFTNET Security Client can now establish a communications tunnel via which PC2 from the external network can communicate securely with PC1.

The tunnel between the SOFTNET Security Client and the security module was established. This status is indicated by the blue symbol and the green circle.

7.4.10 Testing the firewall function (ping test)

How can you test the configured function?

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

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

Note

Firewall in Windows

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

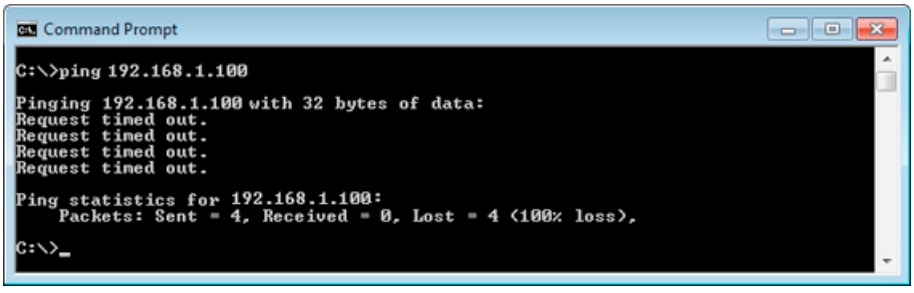
Testing

Now test the function of the firewall configuration as follows:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to PC1 (IP address 192.168.1.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.1.100" at the cursor position.

   You will then receive the following message (no reply from PC1):



Result

The IP packets from PC2 cannot reach PC1 because the data traffic from the VPN tunnel to the internal network is not allowed.

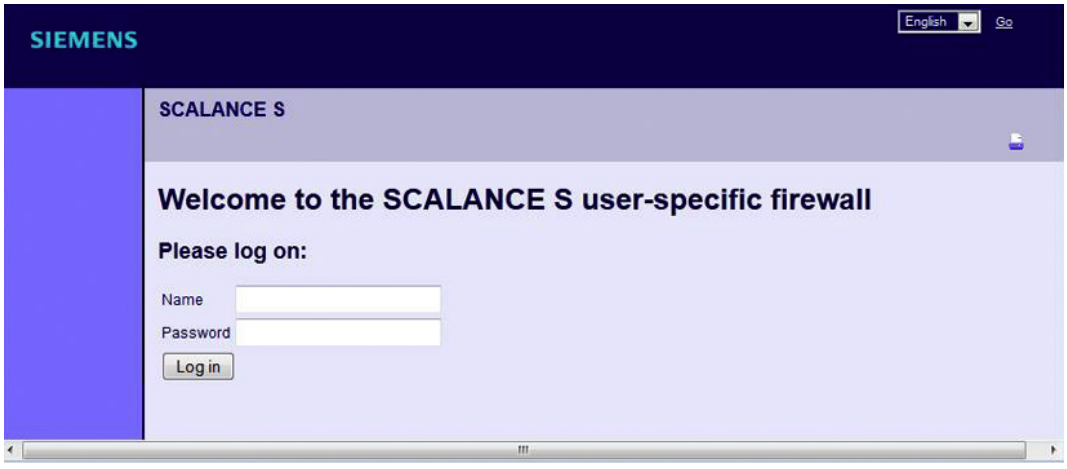
This is shown in the "Ping statistics" 192.168.1.100 as follows:

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

7.4.11 Logging in on the Web page

Logging on via Web page

1. In a Web browser of PC2, enter the address "https://192.168.2.1".
2. In the following window, enter the user name "Remote" and the corresponding password and click the "Log in" button.



3. The defined IP rule set is enabled for the "Remote" user. Access from PC2 in the external network to PC1 in the internal network is allowed.

7.4.12 Testing the firewall function (ping test)

How can you test the configured function?

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

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

Note

Firewall in Windows

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

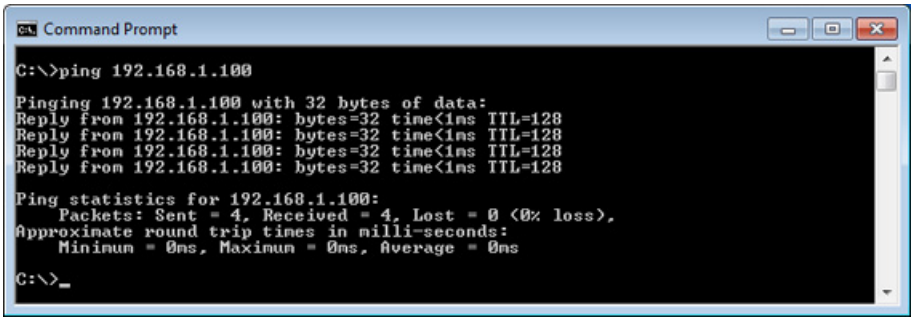
Testing

Now test the function of the firewall configuration as follows:

1. On PC2, call up the menu command "Start" >"All Programs" > "Accessories" > "Command Prompt".
2. Enter the ping command from PC2 to PC1 (IP address 192.168.1.100)

   In the command line of the "Command Prompt" window, enter the command "ping 192.168.1.100" at the cursor position.

   You will then receive the following message (positive reply from PC1):



Result

If the IP packets have reached PC1, the "Ping statistics" for 192.168.1.100 display the following:

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

Due to the configuration of the user-specific IP rule set, the ping packets could reach the internal network via the VPN tunnel. The PC in the internal network has responded to the packets. Due to the "stateful inspection" function of the firewall, the reply packets arriving from the internal network are automatically allowed into the external network.