

Siemens Scalance S623

Overview

- Basic Configuration
- Standard mode Firewall
- Advanced Firewall
- Password Management
- Advanced Password Management
- VPN with PreShared Key
- VPN with Certificates
- Gateway-to-Gateway VPN
- VPN with User Authentication

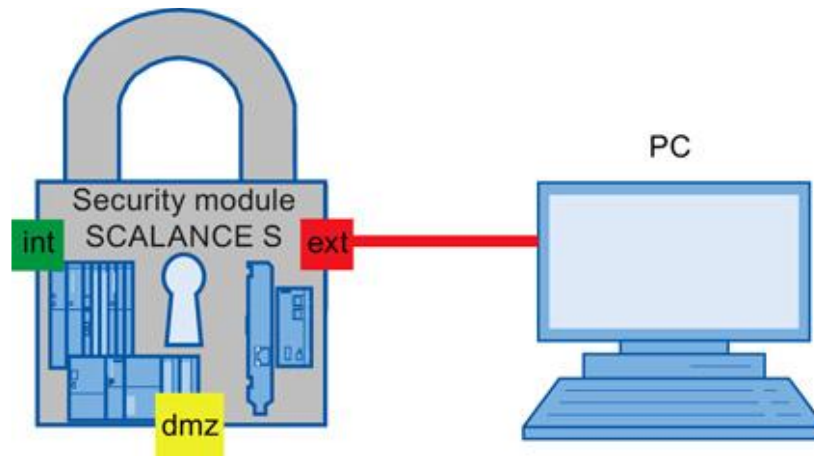
Technology Overview

- User Authentication
 - On-device
 - Connection with RADIUS server
- VPN
 - IPsec end-to-end

Necessary Software

- Siemens Security Configuration Tool
- Siemens SOFTNET Security Client
- Siemens Automation License Manager
- (Optional) Siemens Primary Setup Tool

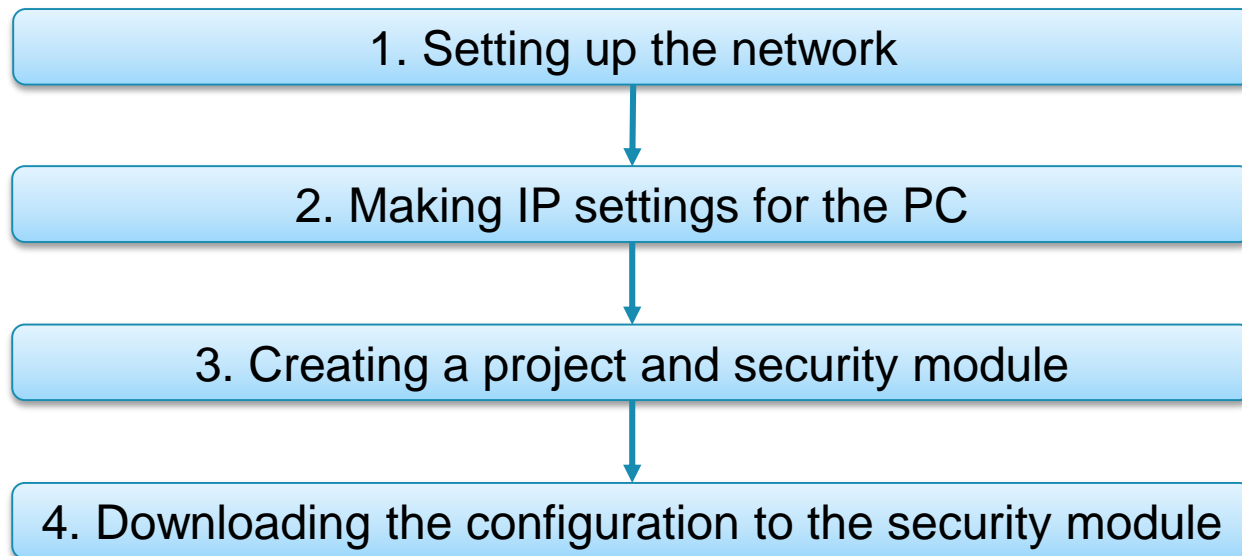
Basic Configuration



In this example we set the IP addresses of all 3 interfaces on the Scalance 623

This will demonstrate configuration steps that will be reused in every following example

Basic Configuration



Basic Configuration

1. Setting up the network

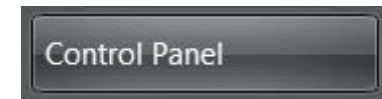
- Connecting the external interface of the Scalance to the PC
- Scalance interfaces
 - External network
Red marking = unprotected network area
 - Internal network
Green marking = network protected by Scalance
 - DMZ port
Yellow marking = unprotected or protected network

Basic Configuration

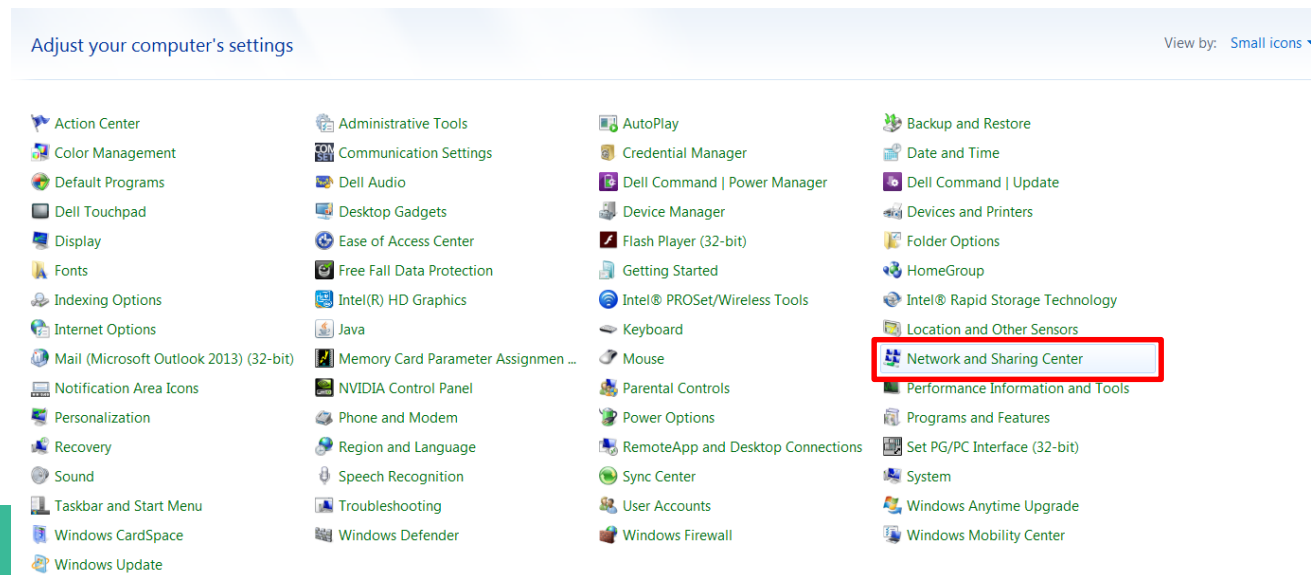
2. Making IP settings for the PC

PC	IP address	Subnet mask
PC	192.168.10.2	255.255.255.0

- Open Control Panel “Start” > “Control Panel”



- Open “Network and Sharing Center”



Basic Configuration

2. Making IP settings for the PC

PC	IP address	Subnet mask
PC	192.168.10.2	255.255.255.0

- Select “Change adapter settings”

Control Panel Home

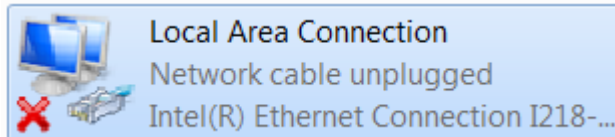
Manage wireless networks

[Change adapter settings](#)

Change advanced sharing settings

- Open the Local Area Connection Properties

Doubleclick “Local Area Connection”, then click “Properties”

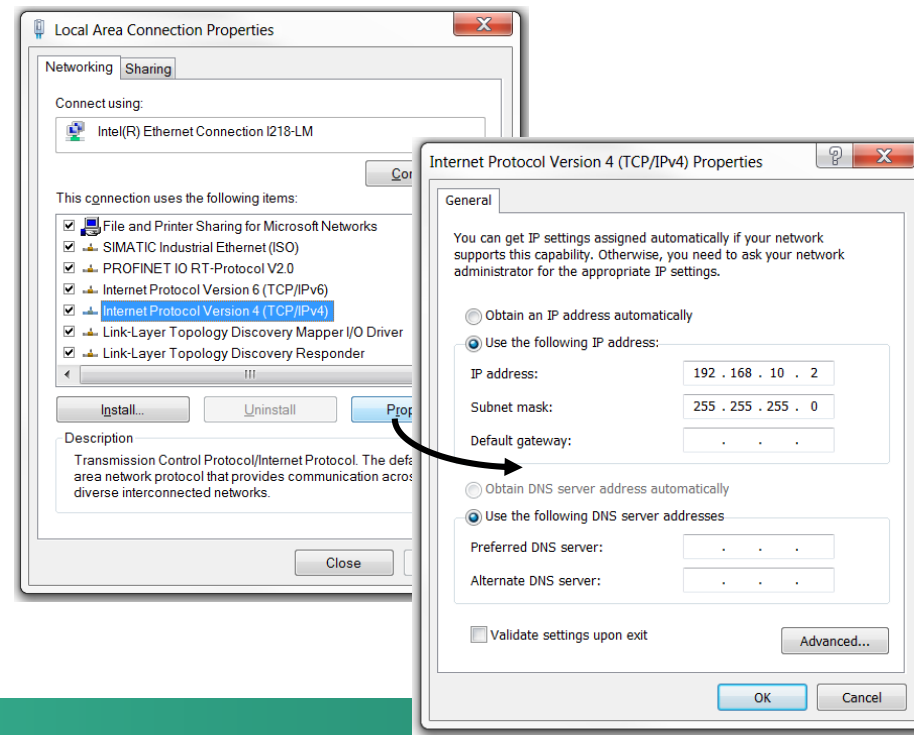


Basic Configuration

2. Making IP settings for the PC

PC	IP address	Subnet mask
PC	192.168.10.2	255.255.255.0

- Click the “Properties” button
- Select “Use the following IP”
- Enter the values from the table in the relevant boxes
- Close the dialogs with “Ok” and close Control Panel

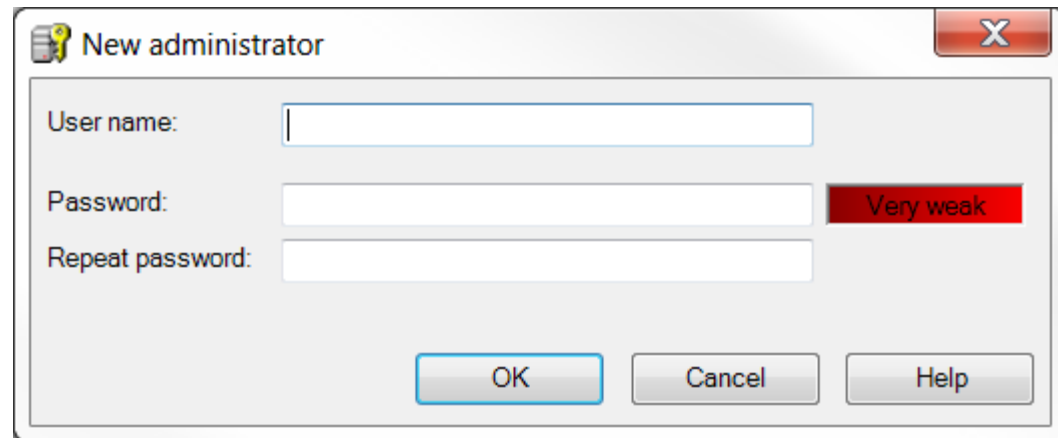


Basic Configuration

3. Creating a project and security module

- Start the Security Configuration Tool
- Select the “Project” > “New...” menu command

- Create a new user
This user is assigned the “administrator” role



The screenshot shows a dialog box titled "New administrator" with a yellow key icon. It contains three input fields: "User name:", "Password:", and "Repeat password:". To the right of the password fields is a red status bar that says "Very weak". At the bottom, there are three buttons: "OK", "Cancel", and "Help".

- Confirm with “OK”

Basic Configuration

3. Creating a project and security module

- In the “Product type”, “Module” and “Firmware release” areas, select the following options
 - Product type: Scalance S
 - Module: S623
 - Firmware release: V4

Selection of a module or software configuration

Product type

☒ SCALANCE S

☐ SOFTNET configuration
(SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

☐ S602 ☒ S623 ☐ S627-2M

☐ S612

☐ S613

Firmware release

☒ V4 ☐ V3

Configuration

Name of the module: Module1

MAC address: 00-1B-1B-BB-99-DE

IP address (ext.): 192.168.10.1 Subnet mask (ext.): 255.255.255.0

Interface routing external/internal: Routing mode

IP address (int.): 192.168.9.1 Subnet mask (int.): 255.255.255.0

Basic Configuration

3. Creating a project and security module

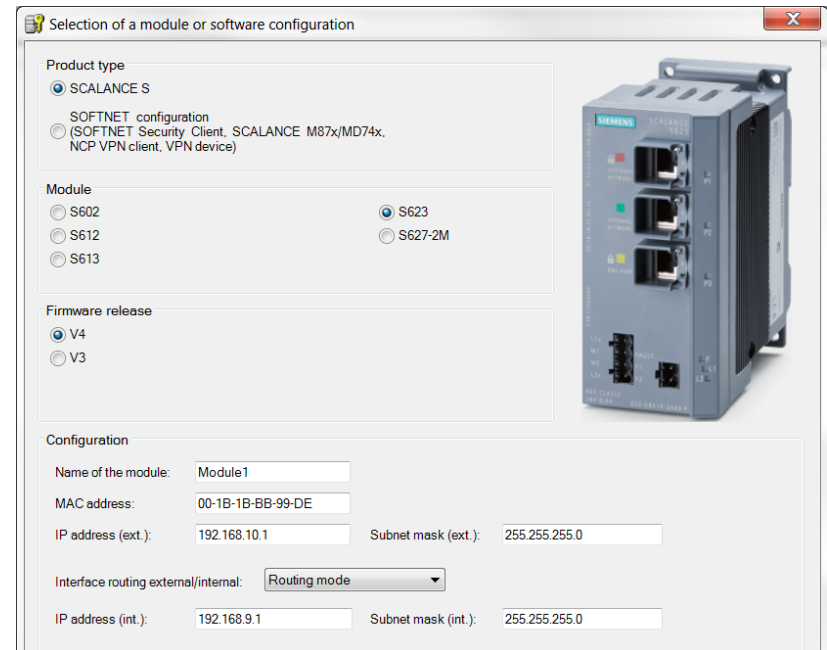
- In the “Configuration” area, enter the MAC address
The MAC address is printed on the front of the SCALANCE

The screenshot shows a software window titled 'Selection of a module or software configuration'. It contains several sections: 'Product type' with 'SCALANCE S' selected; 'Module' with 'S623' selected; 'Firmware release' with 'V4' selected; and 'Configuration' with fields for 'Name of the module' (Module1), 'MAC address' (00-1B-1B-8B-99-DE), 'IP address (ext.)' (192.168.10.1), 'Subnet mask (ext.)' (255.255.255.0), 'Interface routing external/internal' (Routing mode), and 'IP address (int.)' (192.168.9.1), 'Subnet mask (int.)' (255.255.255.0). A small image of the SCALANCE S623 module is shown on the right.

Basic Configuration

3. Creating a project and security module

- In the “Configuration” area, enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- From the drop-down list, select the “Routing Mode”
- Enter the internal IP address (192.168.9.1) and the internal subnet mask (255.255.255.0)
- Confirm with “OK”



The screenshot shows a software configuration window titled "Selection of a module or software configuration". It contains several sections for configuring a Siemens SCALANCE S module:

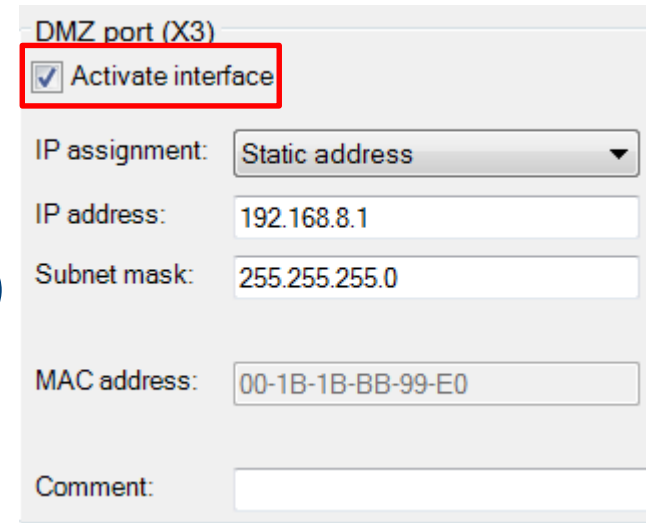
- Product type:** ☒ SCALANCE S. Below it, a radio button for "SOFTNET configuration (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)" is unselected.
- Module:** Radio buttons for S602, S612, and S613 are unselected. Radio buttons for S623 and S627-2M are selected.
- Firmware release:** Radio buttons for V4 and V3 are shown, with V4 selected.
- Configuration:**
 - Name of the module:** Module1
 - MAC address:** 00-1B-1B-BB-99-DE
 - IP address (ext.):** 192.168.10.1 **Subnet mask (ext.):** 255.255.255.0
 - Interface routing external/internal:** Routing mode (selected from a dropdown)
 - IP address (int.):** 192.168.9.1 **Subnet mask (int.):** 255.255.255.0

An image of the SCALANCE S module is shown on the right side of the window.

Basic Configuration

3. Creating a project and security module

- Select the security module created and select the “Edit” > “Properties” menu command, “Interfaces” tab
- Select the “Activate Interface” check box in the “DMZ port (X3)” area
- Enter the IP address (192.168.8.1) and the subnet mask (255.255.255.0) for the DMZ interface
- Confirm with “OK”



DMZ port (X3)

☒ Activate interface

IP assignment: Static address

IP address: 192.168.8.1

Subnet mask: 255.255.255.0

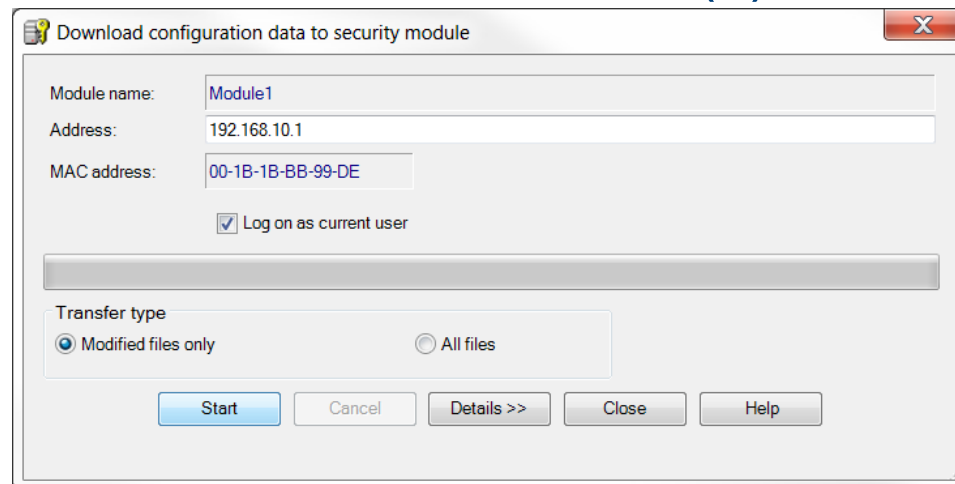
MAC address: 00-1B-1B-BB-99-E0

Comment:

Basic Configuration

4. Downloading the configuration to the security module

- Select the “Project” > “Save” menu command
- Select the security module in the content area
- Select the “Transfer” > “To module(s)...” menu command



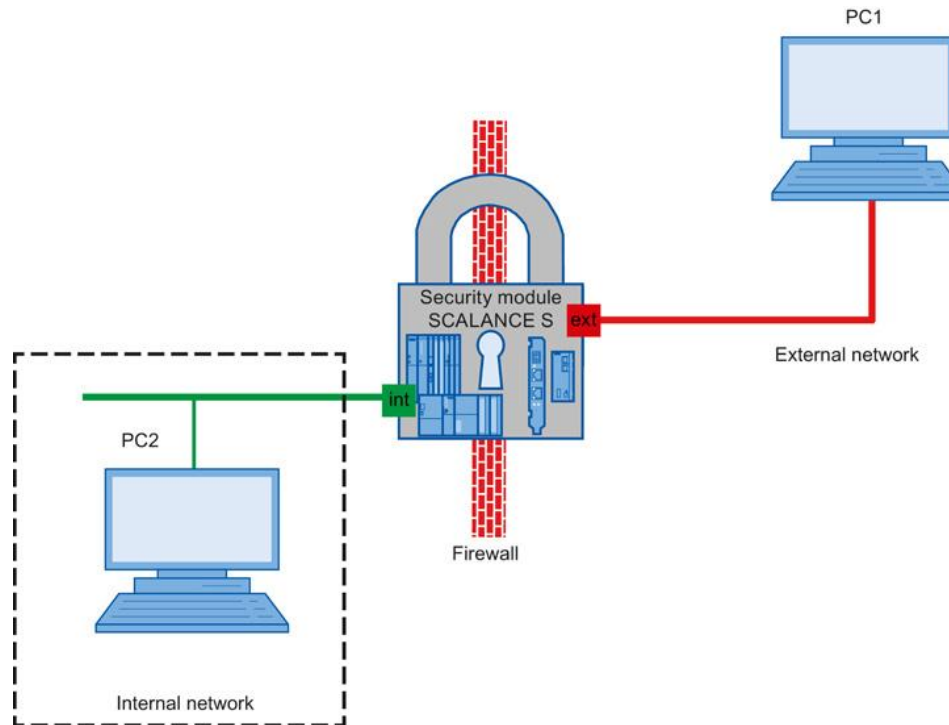
- Start the download with the “Start” button

Basic Configuration

4. Downloading the configuration to the security module

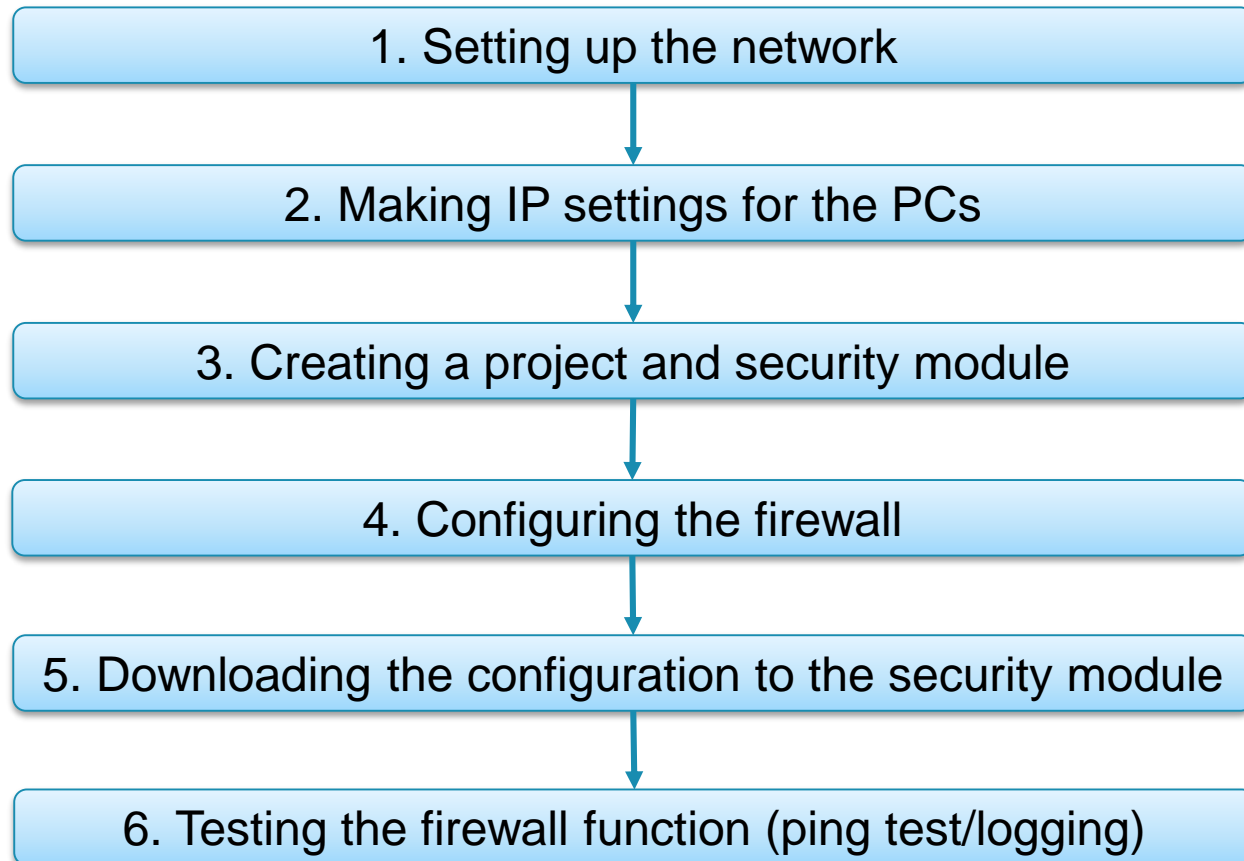
- If the download was completed successfully, the Scalance is restarted automatically and the configuration activated
- The Scalance is now in productive operation
- Configurations can be download via all interfaces
- The configured IP addresses can be modified

Standard mode Firewall



In this example, the firewall will be configured to allow IP traffic to only be initiated by the internal network

Standard mode Firewall



Standard mode Firewall

1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface

Standard mode Firewall

2. Making IP settings for the PCs

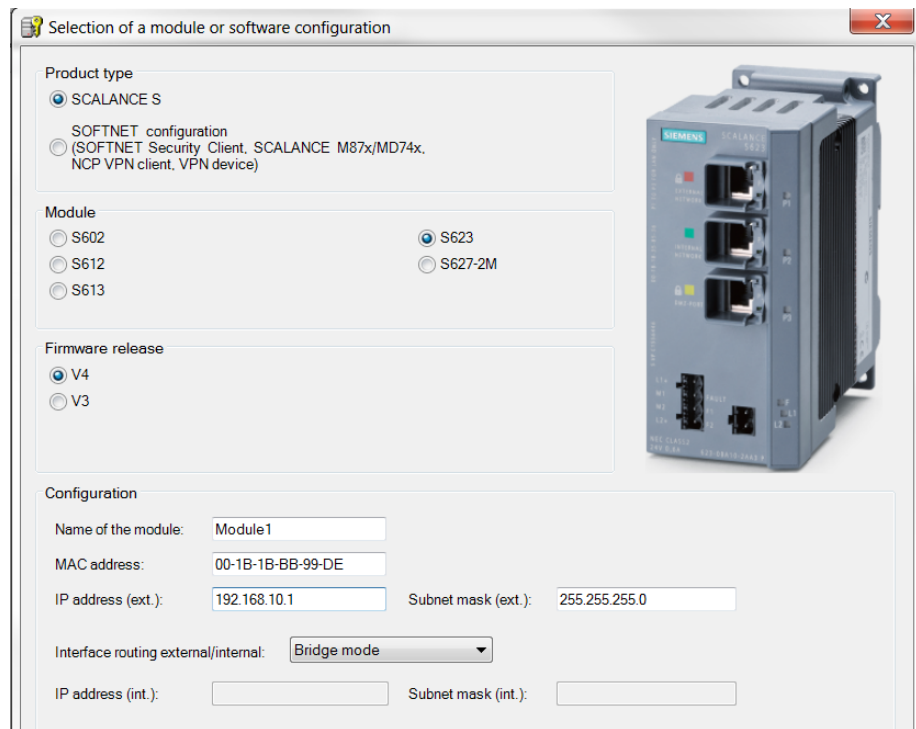
PC	IP address	Subnet mask
PC1	192.168.10.2	255.255.255.0
PC2	192.168.10.3	255.255.255.0

- Set the IP addresses of the PCs as in the table above

Standard mode Firewall

3. Creating a project and security module

- Create a new project
- In the “Configuration” area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Confirm with “OK”



The screenshot shows a software configuration window titled "Selection of a module or software configuration". It contains the following sections:

- Product type:** Radio buttons for ☒ SCALANCE S and ☐ SOFTNET configuration (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device).
- Module:** Radio buttons for ☐ S602, ☐ S612, ☐ S613, ☒ S623, and ☐ S627-2M.
- Firmware release:** Radio buttons for ☒ V4 and ☐ V3.
- Configuration:**
 - Name of the module: Module1
 - MAC address: 00-1B-1B-BB-99-DE
 - IP address (ext.): 192.168.10.1
 - Subnet mask (ext.): 255.255.255.0
 - Interface routing external/internal: Bridge mode (dropdown menu)
 - IP address (int.): (empty field)
 - Subnet mask (int.): (empty field)

An image of the SCALANCE S firewall module is shown on the right side of the window.

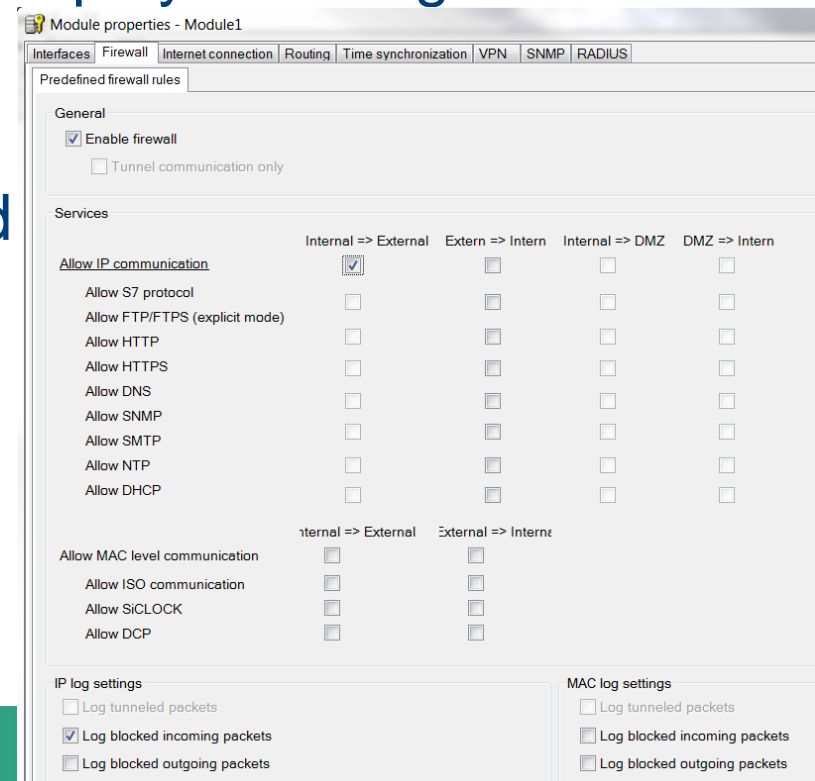
Standard mode Firewall

4. Configuring the firewall

- Select the security module in the content area
- Select the “Edit” > “Properties...” menu command
- Select the “Firewall” tab in the displayed dialog
- Activate the settings shown in the picture

Result: IP traffic is only initiated from the internal network

- Logging is selected to record data traffic
- Close with OK
- Save the project



Standard mode Firewall

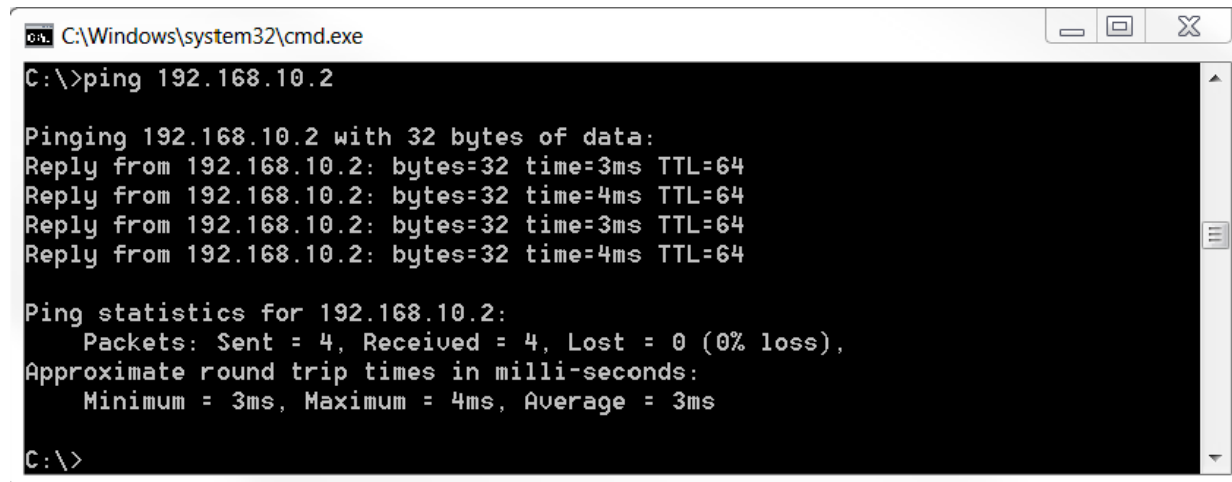
5. Downloading the configuration to the security module

- Transfer the configuration to the security module

Standard mode Firewall

6. Testing the firewall function (ping test/logging)

- Open the command prompt on PC2 “Start” > “All programs” > “Accessories” > “Command Prompt”
- Enter the ping command from PC2 to PC1
“ping 192.168.10.2”



```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=3ms TTL=64
Reply from 192.168.10.2: bytes=32 time=4ms TTL=64
Reply from 192.168.10.2: bytes=32 time=3ms TTL=64
Reply from 192.168.10.2: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms

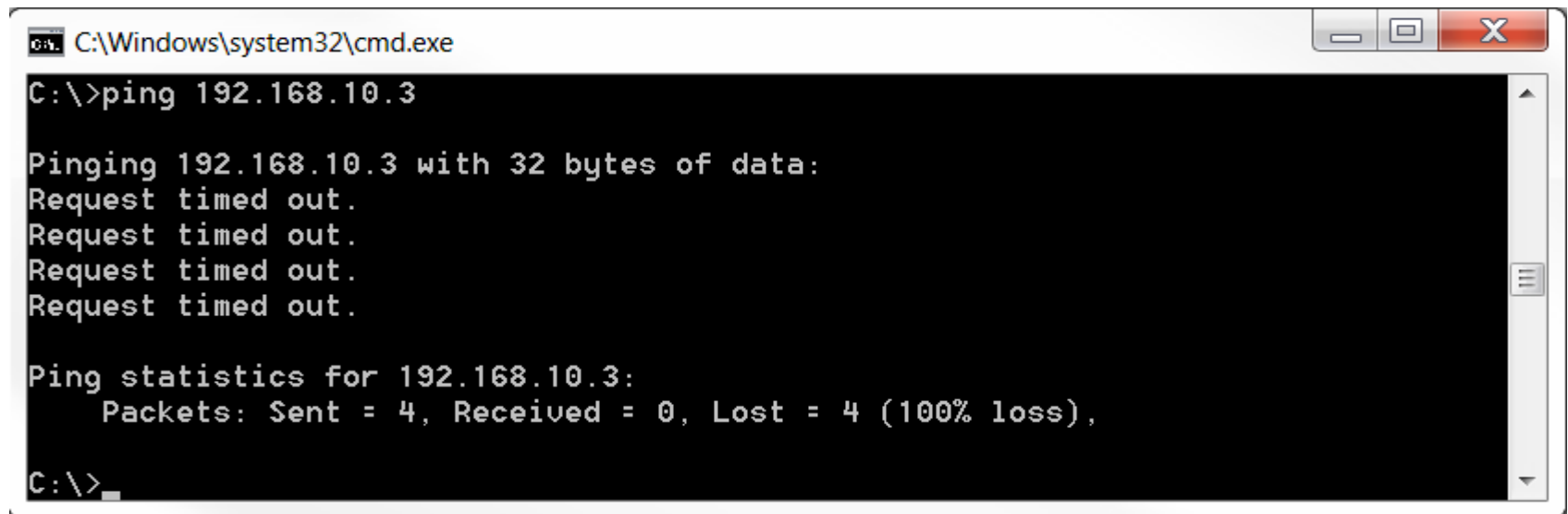
C:\>
```

- All packets reach PC1

Standard mode Firewall

6. Testing the firewall function (ping test/logging)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC2
“ping 192.168.10.3”



A screenshot of a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The window has standard Windows window controls (minimize, maximize, close) in the top right corner. The command prompt shows the following text:

```
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

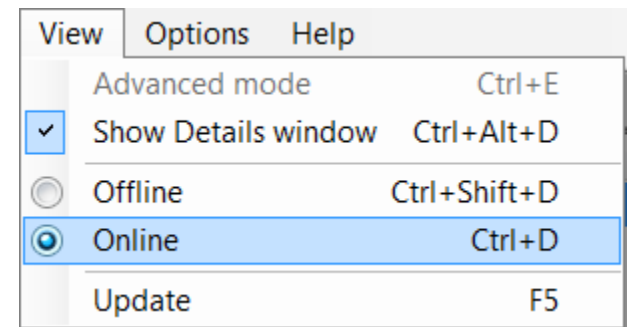
C:\>
```

- All packets are blocked at Scalance

Standard mode Firewall

6. Testing the firewall function (ping test/logging)

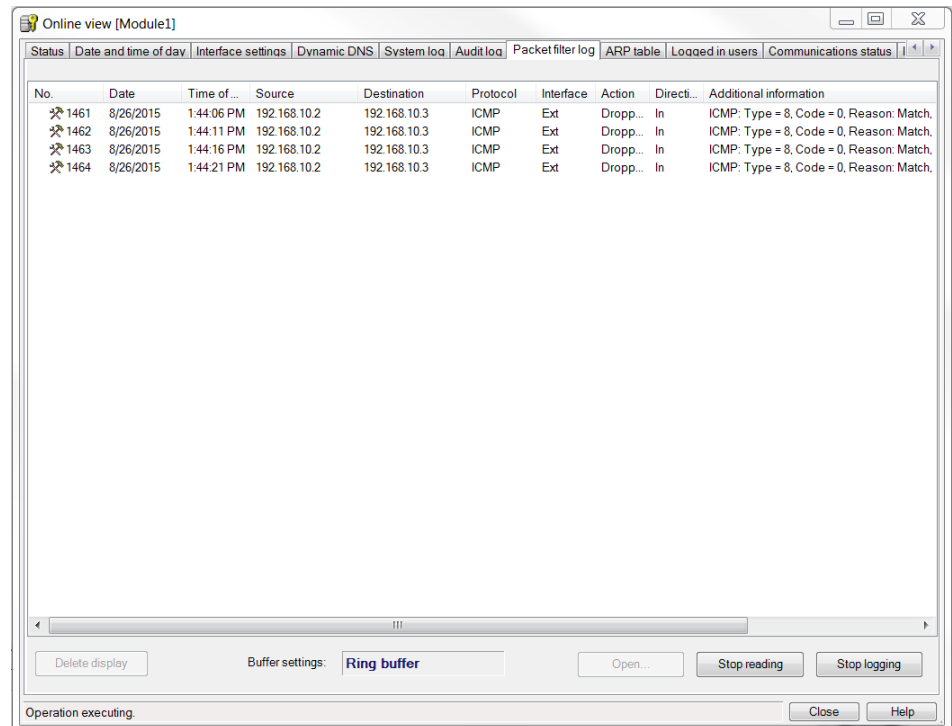
- In the SCT change to online mode by selecting the menu option “View” > “Online”
- Select “Edit” > “View Diagnostics”
- Select the “Packet filter log” tab



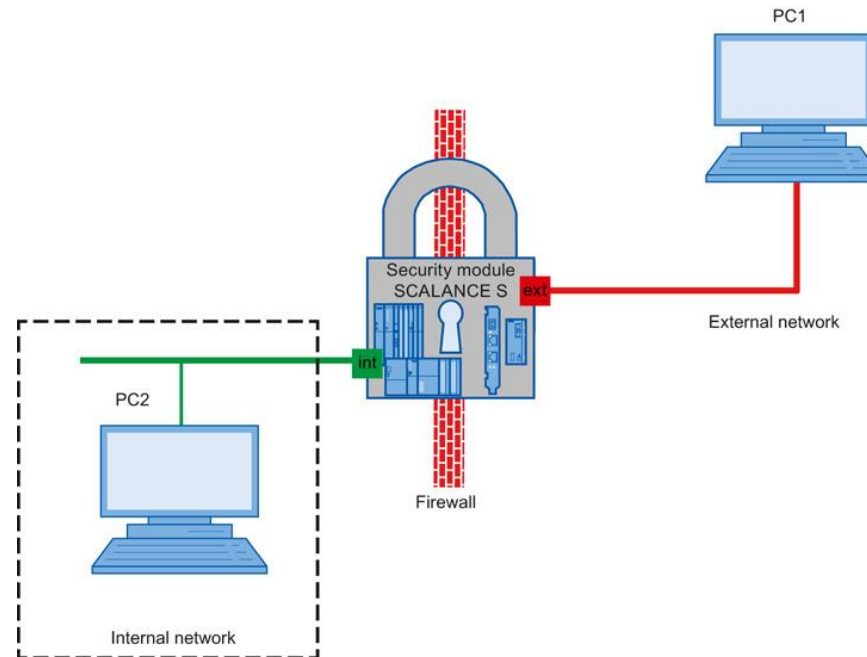
Standard mode Firewall

6. Testing the firewall function (ping test/logging)

- Click the “Start reading” button
- Acknowledge with “OK”
- Log entries are read and displayed here

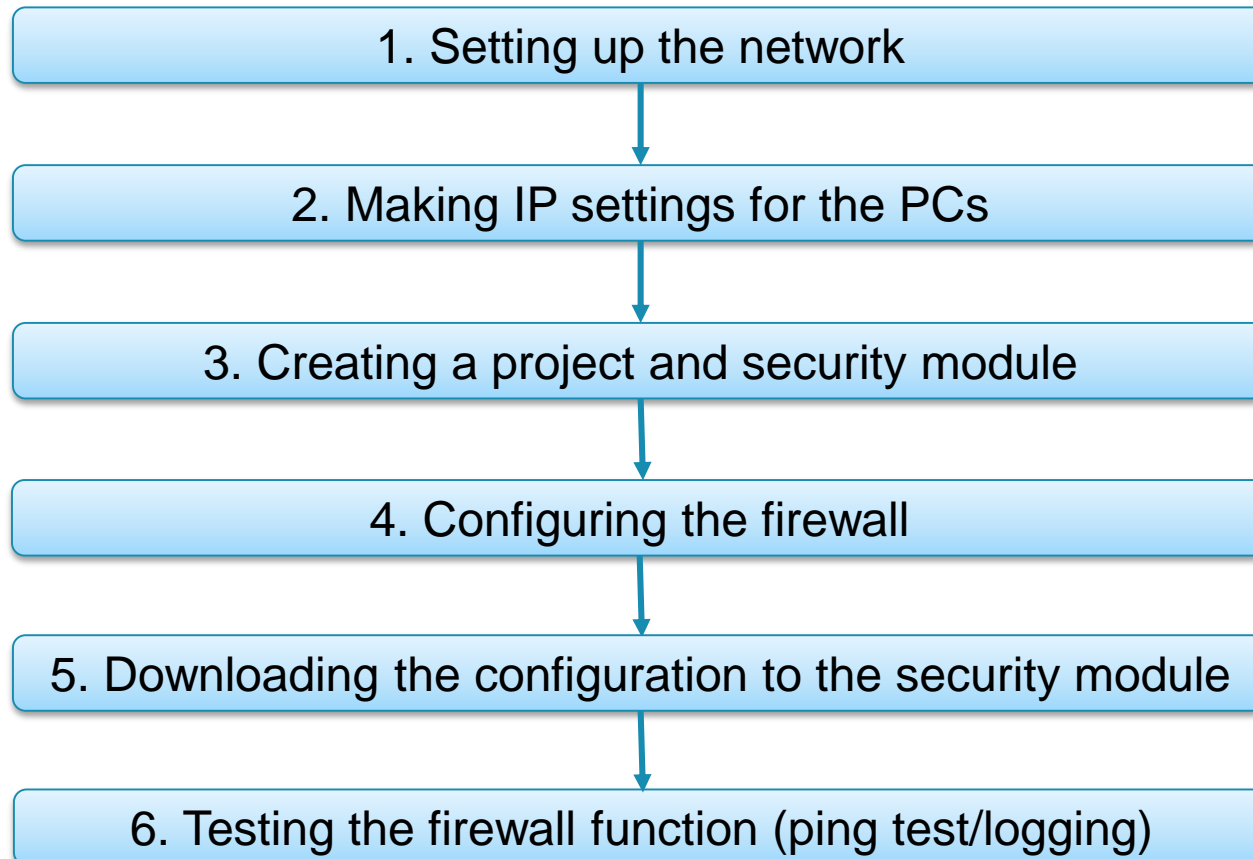


Advanced Firewall



In this example, the firewall is configured to allow IP traffic from PC2 to PC1. The packets are forwarded to the outside with an IP address translated to the IP address of the security module and a dynamically assigned port number. Only replies to these packets can enter the internal network

Advanced Firewall



Advanced Firewall

1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface

Advanced Firewall

2. Making IP settings for the PCs

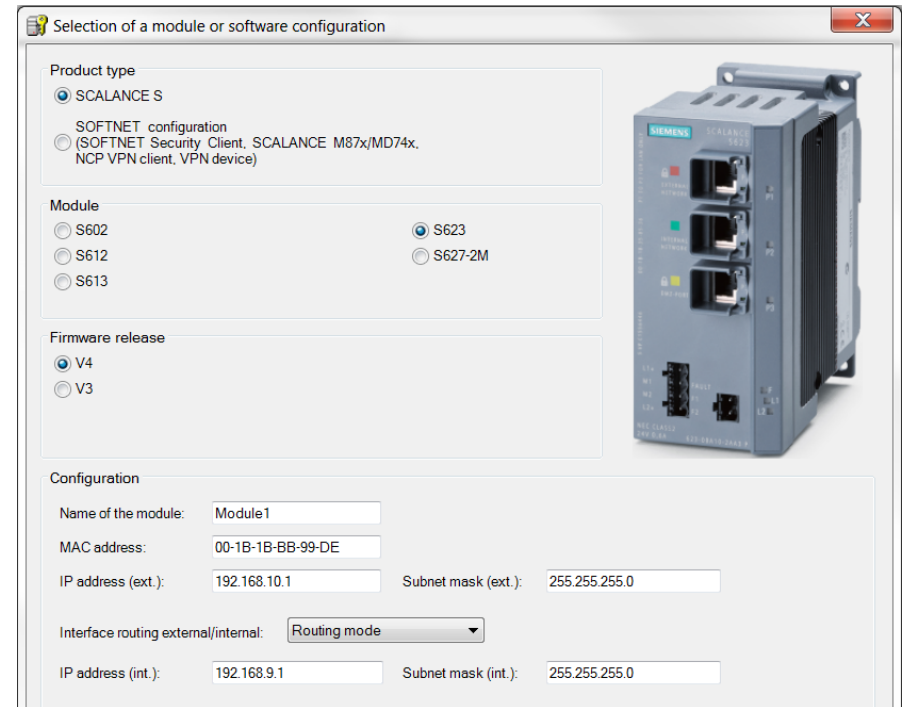
PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.9.2	255.255.255.0	192.168.9.1

- Set the IP addresses of the PCs as in the table above

Advanced Firewall

3. Creating a project and security module

- Create a new project
- In the “Configuration” area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the “Routing mode”
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with “OK”



Selection of a module or software configuration

Product type

- ☒ SCALANCE S
- ☐ SOFTNET configuration (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

- ☐ S602
- ☐ S612
- ☐ S613
- ☒ S623
- ☐ S627-2M

Firmware release

- ☒ V4
- ☐ V3

Configuration

Name of the module: Module1

MAC address: 00-1B-1B-BB-99-DE

IP address (ext.): 192.168.10.1 Subnet mask (ext.): 255.255.255.0

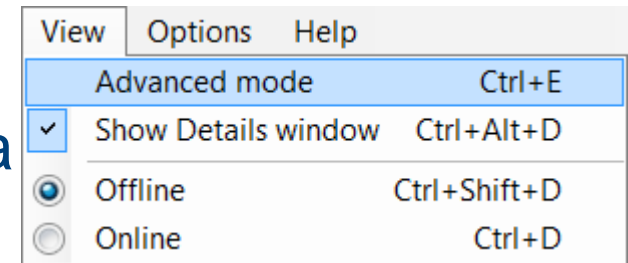
Interface routing external/internal: Routing mode

IP address (int.): 192.168.9.1 Subnet mask (int.): 255.255.255.0

Advanced Firewall

4. Configuring the firewall

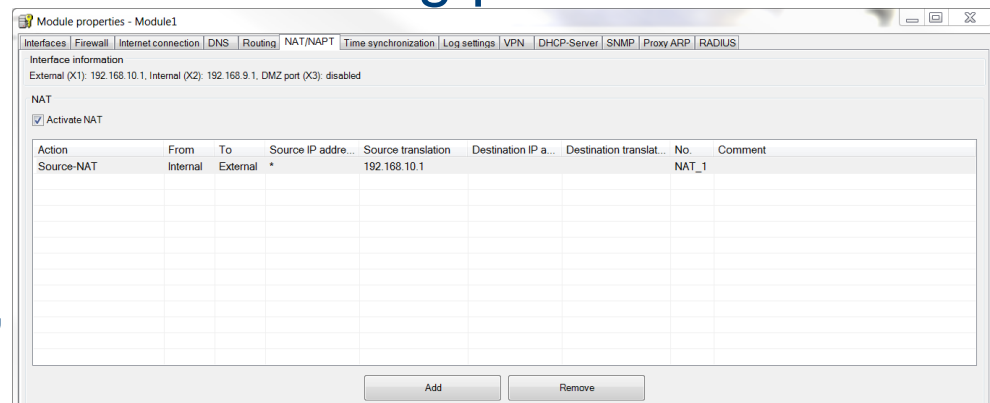
- Change the configuration view to advance mode with the menu command “View” > “Advanced Mode”
- Select the module in the content area
- Select the “Edit” > “Properties...” menu command
- Go to the “NAT/NAPT” tab



Advanced Firewall

4. Configuring the firewall

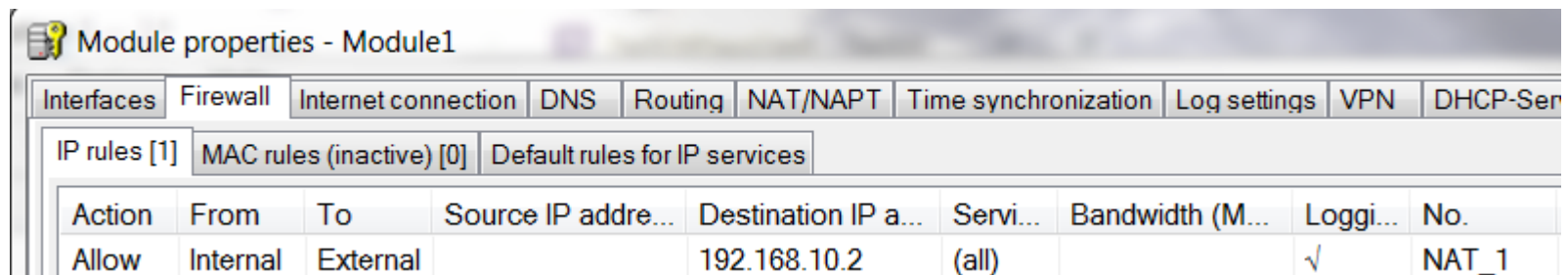
- Select the “Activate NAT” checkbox
- Click the “Add” button in the “NAT” input area
- Configure the NAT rule with the following parameters
 - Action: “Source NAT”
 - From: “Internal”
 - To: “External”
 - Source IP address: “*”
 - Source translation: “192.168.10.1”
- Confirm with “Apply”



Advanced Firewall

4. Configuring the firewall

- Select the “Firewall” tab
- Expand the firewall rule created by SCT with the following
 - Destination IP address: 192.168.10.2
- Select the “Logging” check box



- Confirm with “OK”

Advanced Firewall

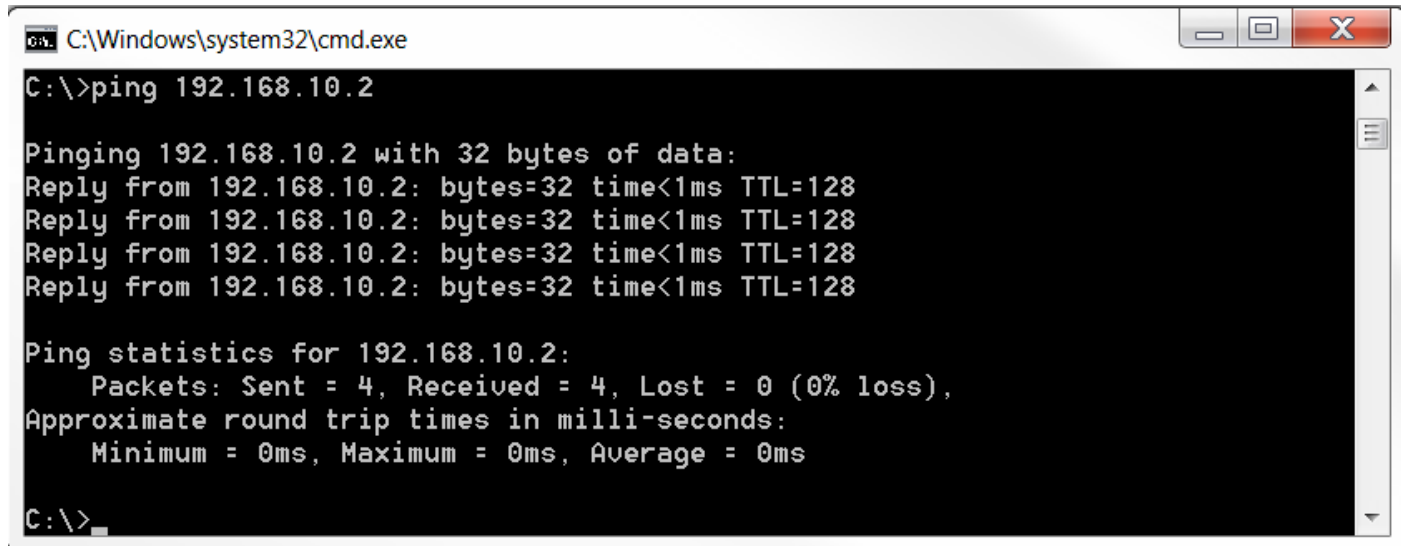
5. Downloading the configuration to the security module

- Transfer the configuration to the security module

Advanced Firewall

6. Testing the firewall function (ping test/logging)

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC1
“ping 192.168.10.2”



```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

- All packets reach PC1

Advanced Firewall

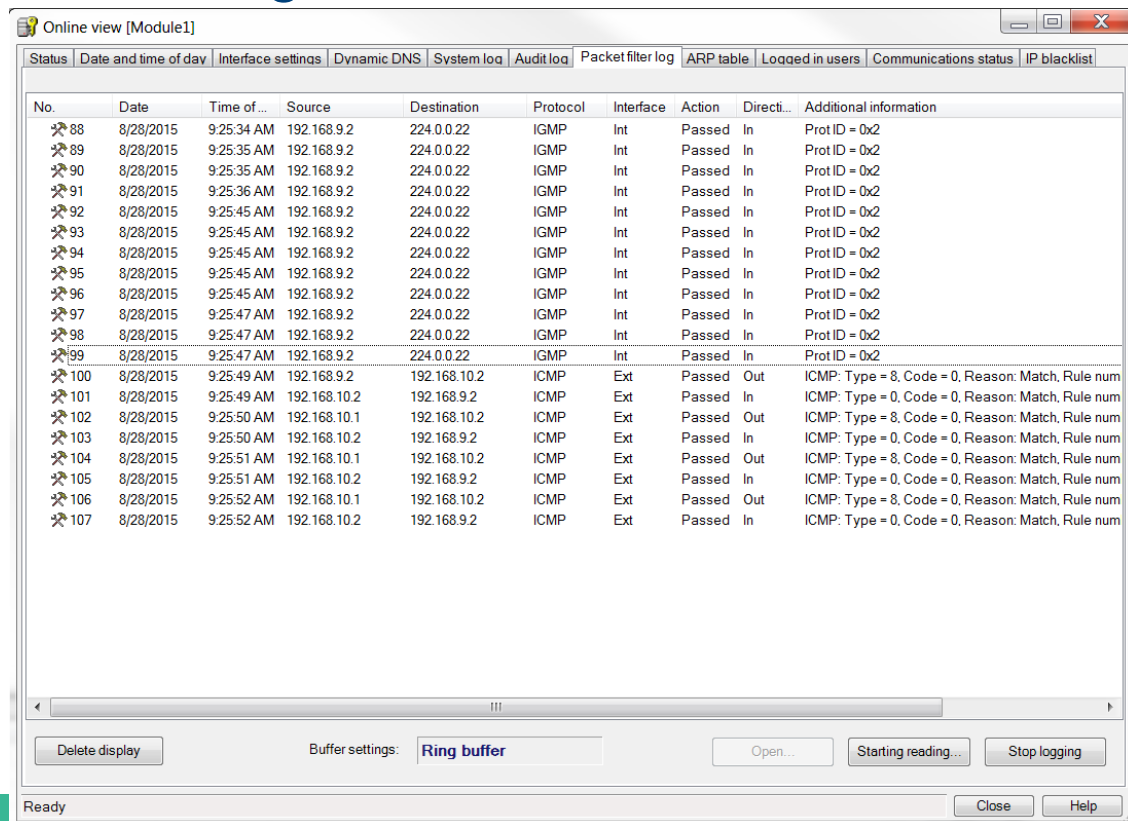
6. Testing the firewall function (ping test/logging)

- Change to online mode in the SCT with the “View” > “Online” menu command
- Select the module in the content area and the menu command “Edit” > “Online diagnostics”
- Go to the “Packet filter log” tab

Advanced Firewall

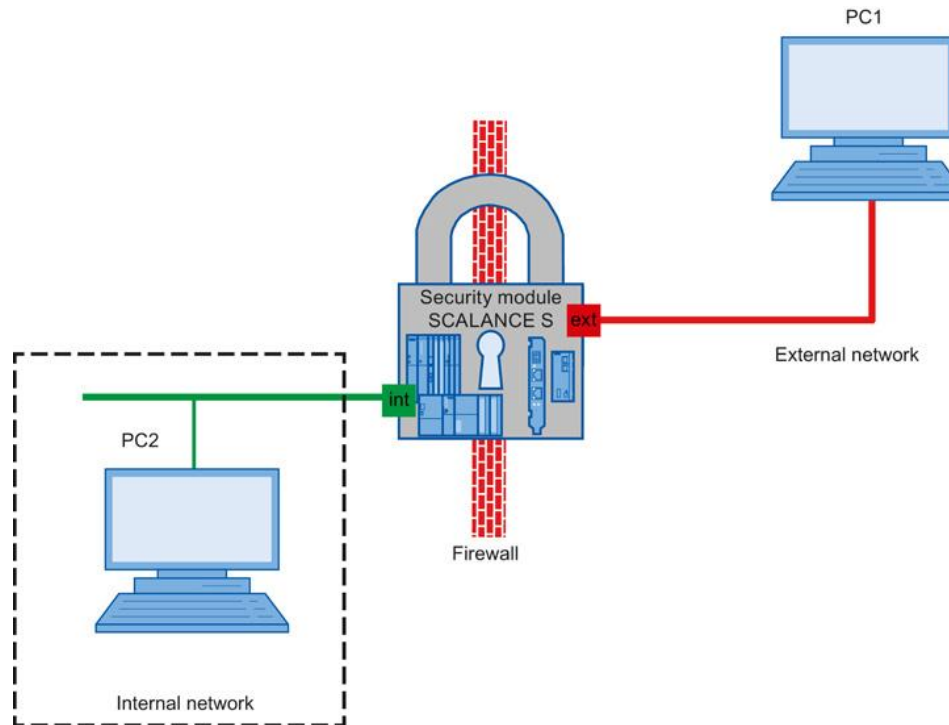
6. Testing the firewall function (ping test/logging)

- Click “Start reading...”
- Confirm the dialog with “OK”



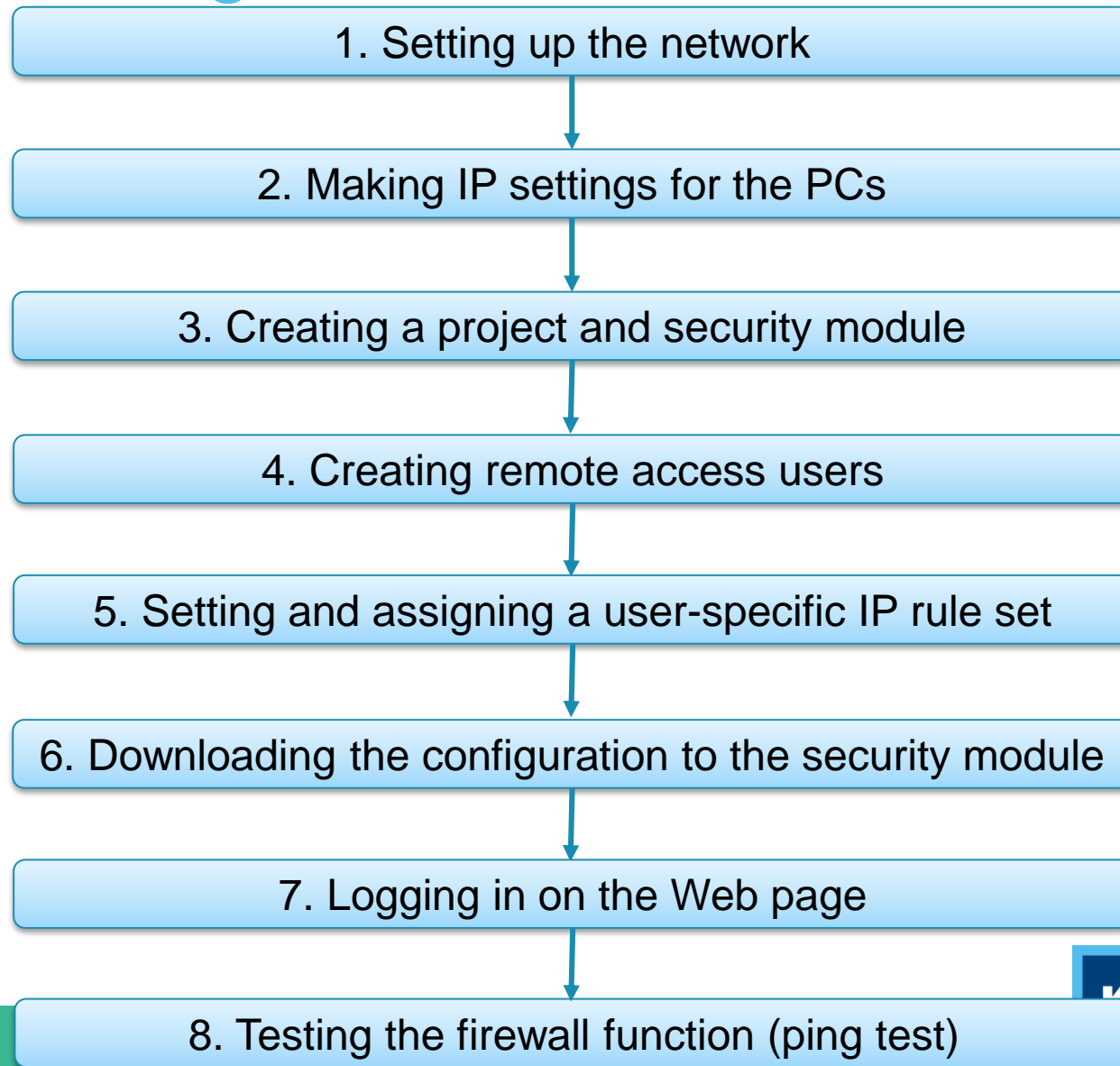
No.	Date	Time of ...	Source	Destination	Protocol	Interface	Action	Directi...	Additional information
88	8/28/2015	9:25:34 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
89	8/28/2015	9:25:35 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
90	8/28/2015	9:25:35 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
91	8/28/2015	9:25:36 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
92	8/28/2015	9:25:45 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
93	8/28/2015	9:25:45 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
94	8/28/2015	9:25:45 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
95	8/28/2015	9:25:45 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
96	8/28/2015	9:25:45 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
97	8/28/2015	9:25:47 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
98	8/28/2015	9:25:47 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
99	8/28/2015	9:25:47 AM	192.168.9.2	224.0.0.22	IGMP	Int	Passed	In	Prot ID = 0x2
100	8/28/2015	9:25:49 AM	192.168.9.2	192.168.10.2	ICMP	Ext	Passed	Out	ICMP: Type = 8, Code = 0, Reason: Match, Rule num
101	8/28/2015	9:25:49 AM	192.168.10.2	192.168.9.2	ICMP	Ext	Passed	In	ICMP: Type = 0, Code = 0, Reason: Match, Rule num
102	8/28/2015	9:25:50 AM	192.168.10.1	192.168.10.2	ICMP	Ext	Passed	Out	ICMP: Type = 8, Code = 0, Reason: Match, Rule num
103	8/28/2015	9:25:50 AM	192.168.10.2	192.168.9.2	ICMP	Ext	Passed	In	ICMP: Type = 0, Code = 0, Reason: Match, Rule num
104	8/28/2015	9:25:51 AM	192.168.10.1	192.168.10.2	ICMP	Ext	Passed	Out	ICMP: Type = 8, Code = 0, Reason: Match, Rule num
105	8/28/2015	9:25:51 AM	192.168.10.2	192.168.9.2	ICMP	Ext	Passed	In	ICMP: Type = 0, Code = 0, Reason: Match, Rule num
106	8/28/2015	9:25:52 AM	192.168.10.1	192.168.10.2	ICMP	Ext	Passed	Out	ICMP: Type = 8, Code = 0, Reason: Match, Rule num
107	8/28/2015	9:25:52 AM	192.168.10.2	192.168.9.2	ICMP	Ext	Passed	In	ICMP: Type = 0, Code = 0, Reason: Match, Rule num

User Management



In this example, only a specific user is allowed to access PC2 in the internal network from PC1 in the external network. For other users, access is blocked

User Management



User Management

1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface

User Management

2. Making IP settings for the PCs

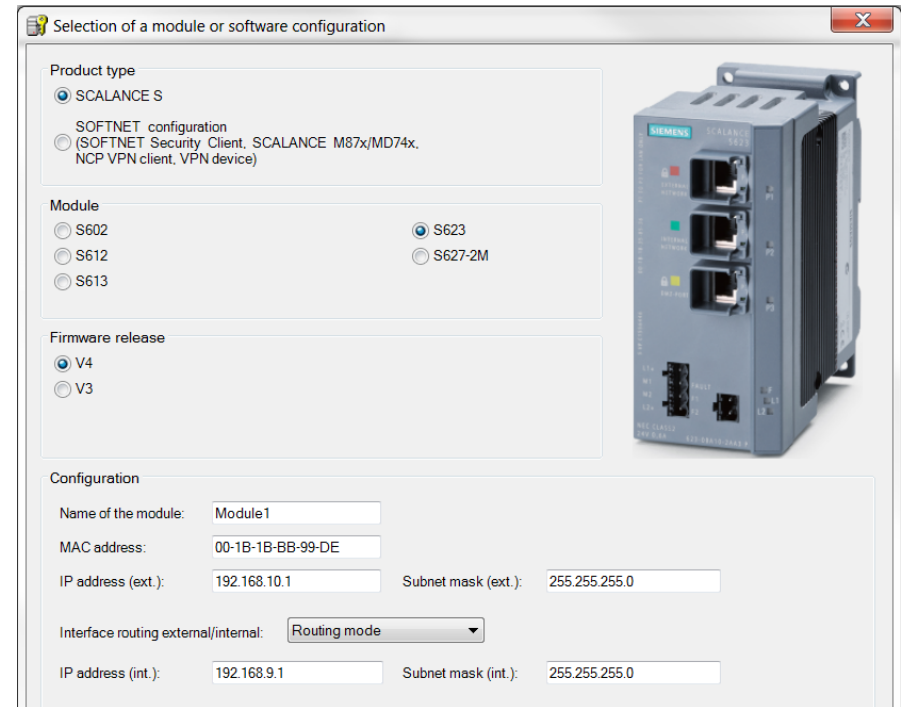
PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.9.2	255.255.255.0	192.168.9.1

- Set the IP addresses of the PCs as in the table above

User Management

3. Creating a project and security module

- Create a new project
- In the “Configuration” area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the “Routing mode”
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with “OK”



Selection of a module or software configuration

Product type

☒ SCALANCE S

SOFTNET configuration
☐ (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

☐ S602 ☒ S623 ☐ S627-2M

☐ S612

☐ S613

Firmware release

☒ V4 ☐ V3

Configuration

Name of the module: Module1

MAC address: 00-1B-1B-BB-99-DE

IP address (ext.): 192.168.10.1 Subnet mask (ext.): 255.255.255.0

Interface routing external/internal: Routing mode

IP address (int.): 192.168.9.1 Subnet mask (int.): 255.255.255.0

User Management

4. Creating remote access users

- Select the “Options” > “User management...” menu command
- Click the “Add...” button in the “User” tab
- Create a new user with the settings in the figure
- Confirm with “OK”

Create new user

User data

User name: Remote

Authentication method: Password

Password: Very weak

Repeat password:

Comment:

Settings for user-specific IP rule sets

Maximum time of the session: 30 Minutes

Role

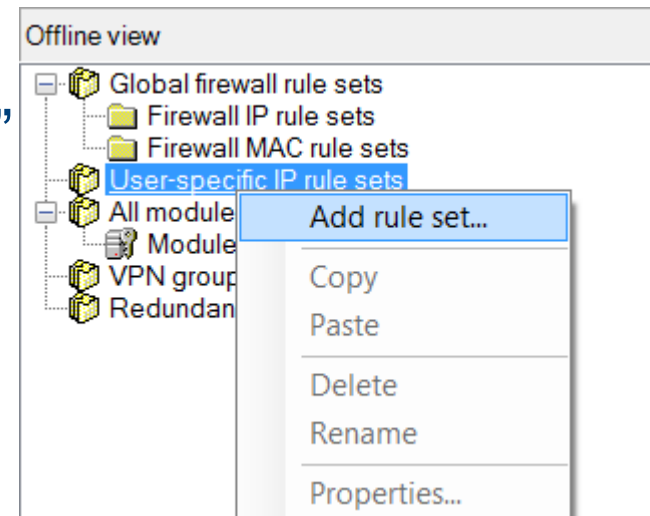
Assigned role: remote access

OK Cancel Help

User Management

5. Setting and assigning a user-specific IP rule set

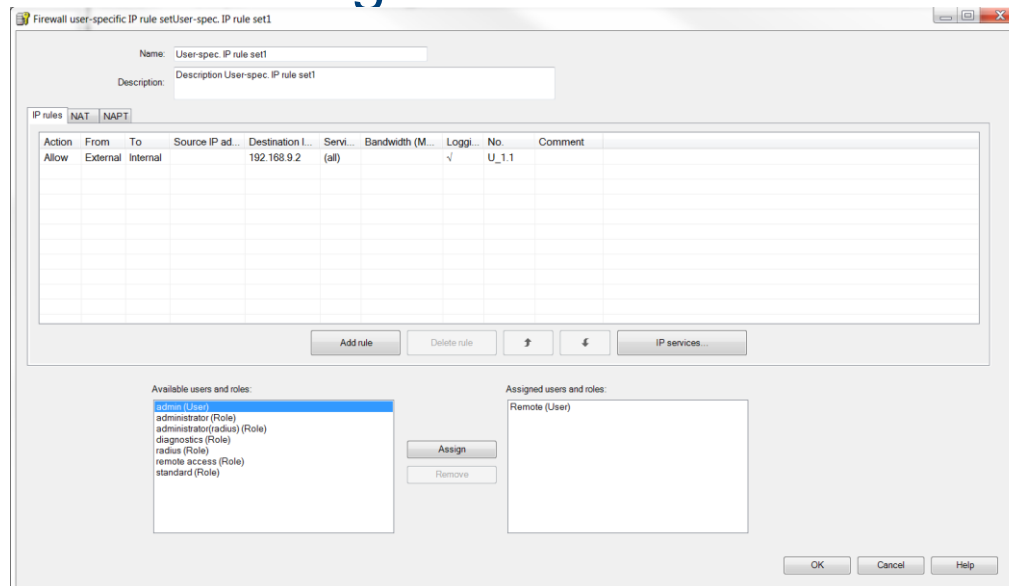
- Change the configuration to advanced mode via “View” > “Advanced Mode”
- Select the “User-specific IP rule sets” object in the navigation panel
- Select the “Add rule set...” entry in the shortcut menu



User Management

5. Setting and assigning a user-specific IP rule set

- Enter a rule in the dialog as shown below



- From the “Available users and roles” list, select the “Remote (user)” entry and click the “Assign” button
- Confirm with “OK”

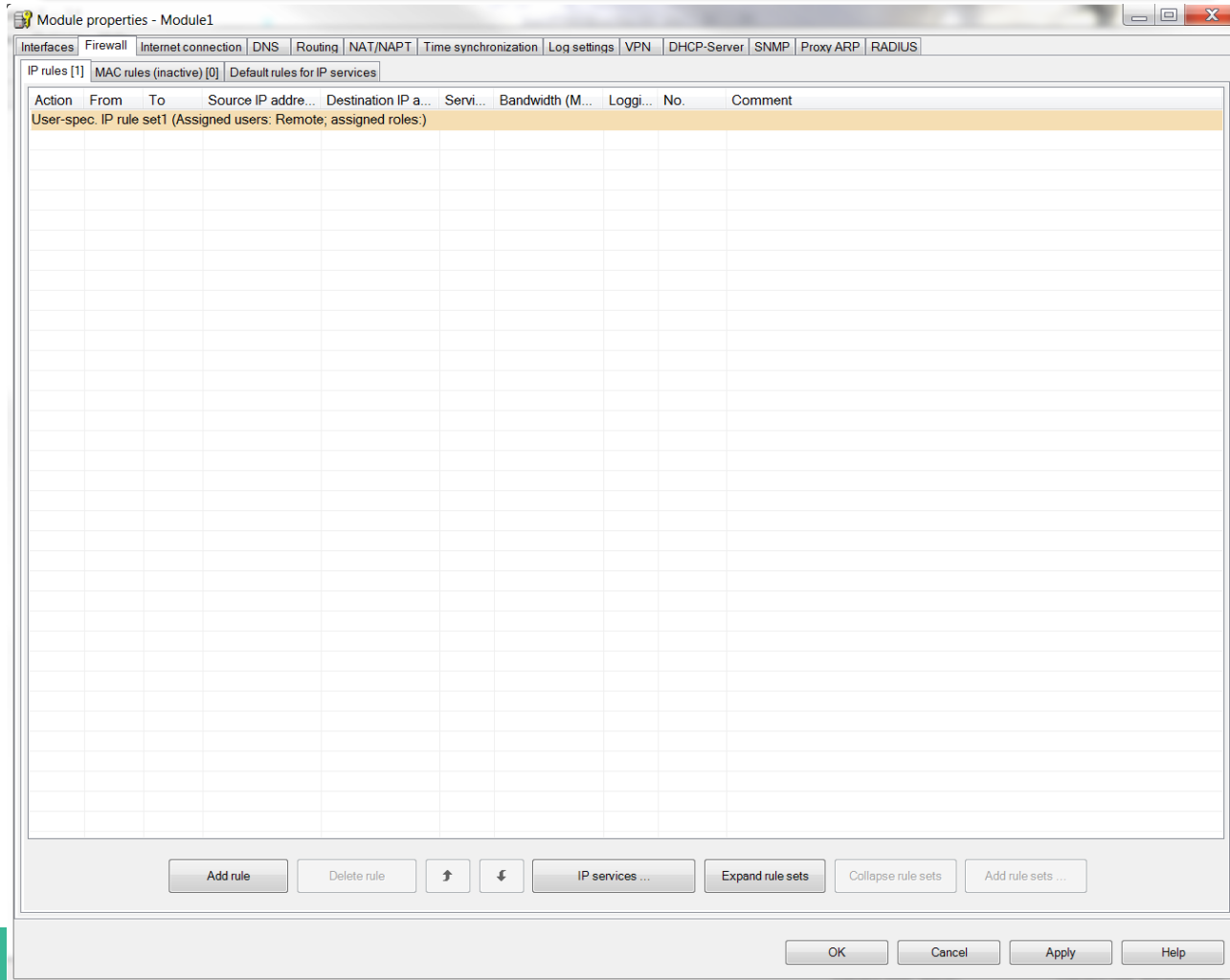
User Management

5. Setting and assigning a user-specific IP rule set

- Select the security module in the navigation panel and drag it to the newly created user-specific IP rule set
- The assignment can be checked by opening the module properties and selecting the “Firewall” tab

User Management

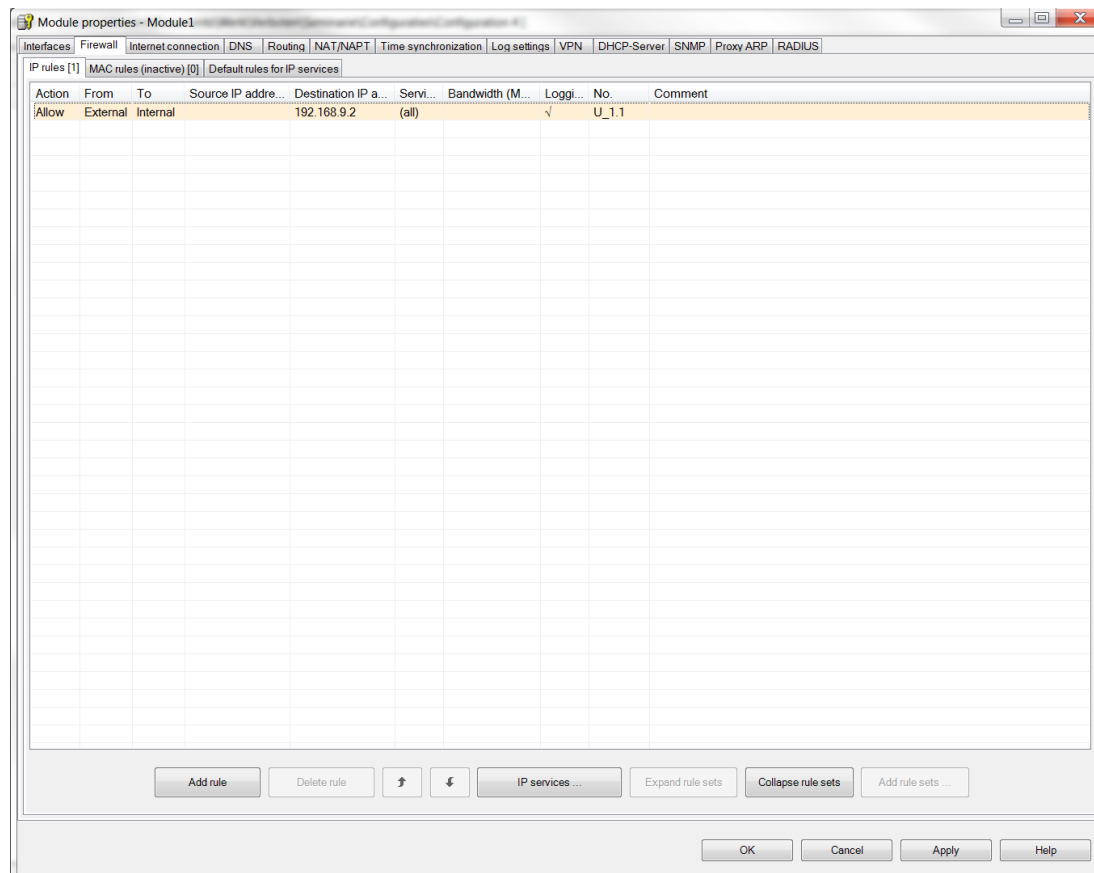
5. Setting and assigning a user-specific IP rule set



User Management

5. Setting and assigning a user-specific IP rule set

- “Expand rule set” shows the user-specific rule in detail



User Management

6. Downloading the configuration to the security module

- Transfer the configuration to the security module

User Management

7. Logging in on the Web page

- In the Web browser of PC1, enter the address “https://192.168.10.1”



The screenshot shows the login interface for the SCALANCE S user-specific firewall. The page has a dark blue header with the 'SIEMENS' logo on the left and a language dropdown set to 'English' on the right. Below the header, the page title 'SCALANCE S' is displayed. The main content area has a light blue background and contains the text 'Welcome to the SCALANCE S user-specific firewall'. Below this, it says 'Please log on:'. There are two input fields: 'Name' and 'Password'. A 'Log in' button is located below the password field.

SIEMENS

English Go

SCALANCE S

Welcome to the SCALANCE S user-specific firewall

Please log on:

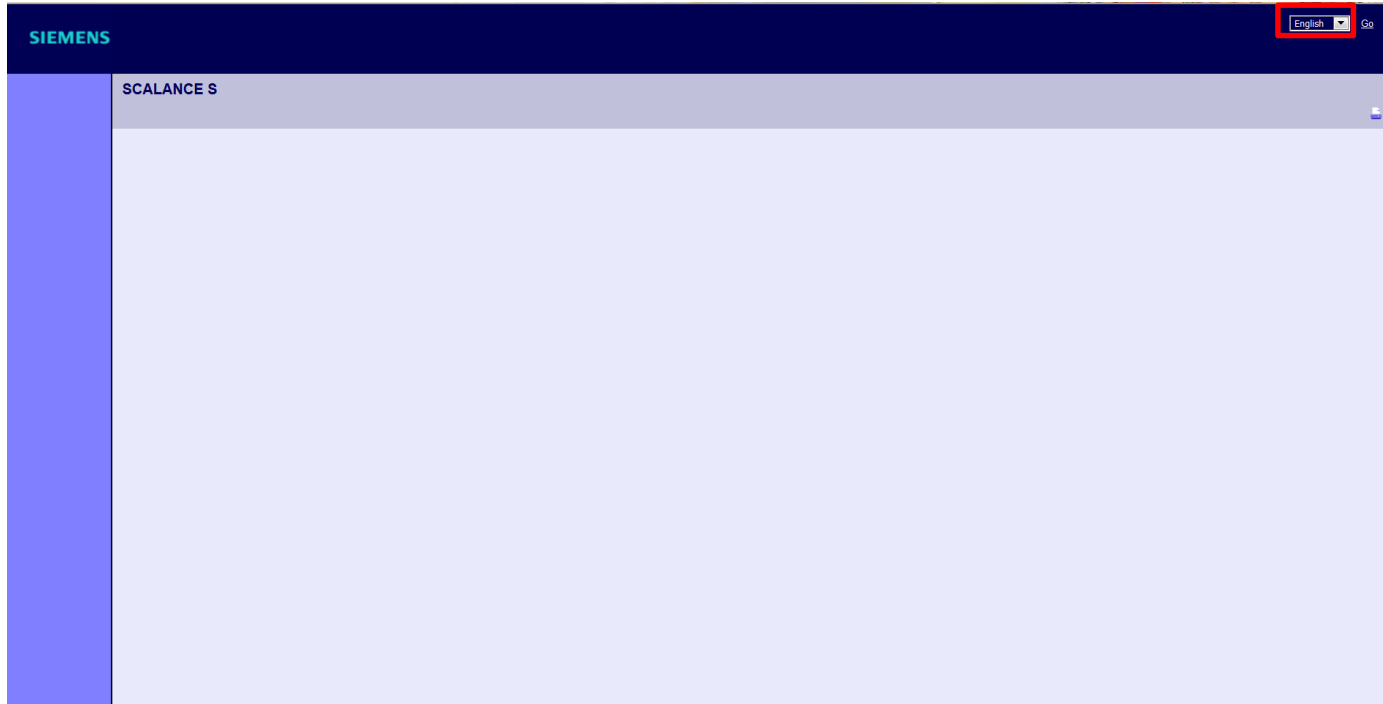
Name

Password

User Management

7. Logging in on the Web page

- If the web page does not show the login fields, try changing the language in the upper right corner



User Management

7. Logging in on the Web page

- Enter the user name “Remote” and corresponding password and click the “Log in” button



The screenshot shows the login interface for the SCALANCE S user-specific firewall. The page has a dark blue header with the 'SIEMENS' logo on the left and a language dropdown set to 'English' on the right. Below the header, the page title 'SCALANCE S' is displayed. The main content area has a light blue background and contains the text 'Welcome to the SCALANCE S user-specific firewall'. Below this, it says 'Please log on:'. There are two input fields: 'Name' with the value 'Remote' and 'Password' with masked characters. A 'Log in' button is positioned below the password field.

SIEMENS

English Go

SCALANCE S

Welcome to the SCALANCE S user-specific firewall

Please log on:

Name Remote

Password

Log in

User Management

7. Logging in on the Web page

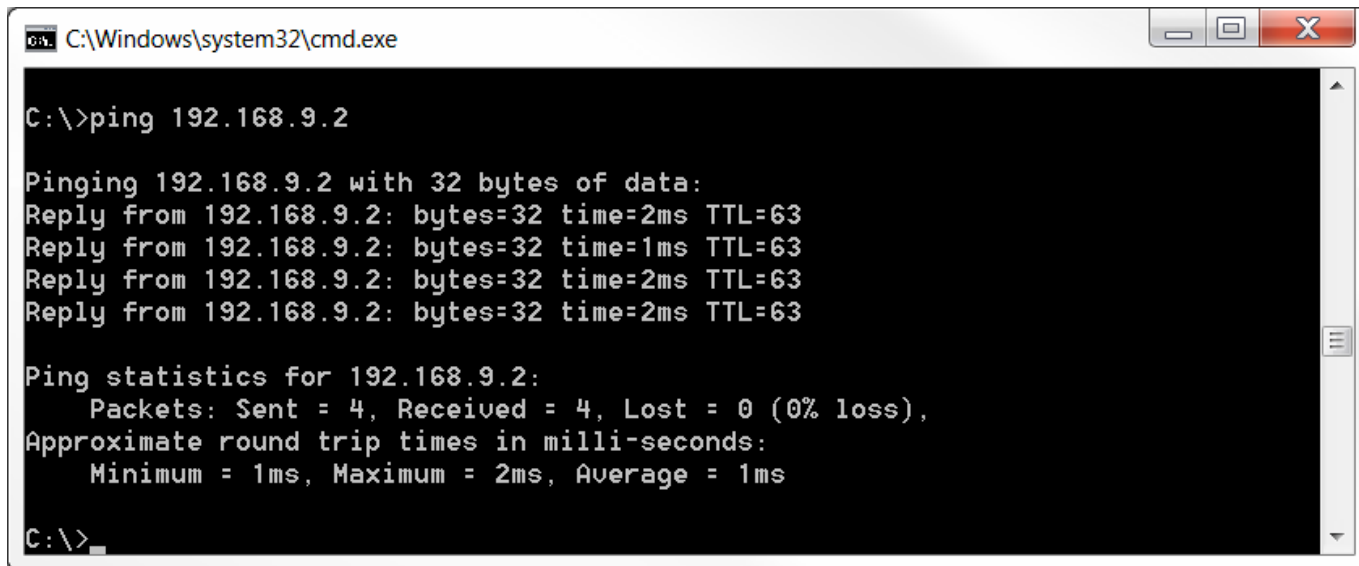
- The defined IP rule set is enabled for the “Remote” user.



User Management

8. Testing the firewall function (ping test)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC2
“ping 192.168.9.2”



```
C:\Windows\system32\cmd.exe

C:\>ping 192.168.9.2

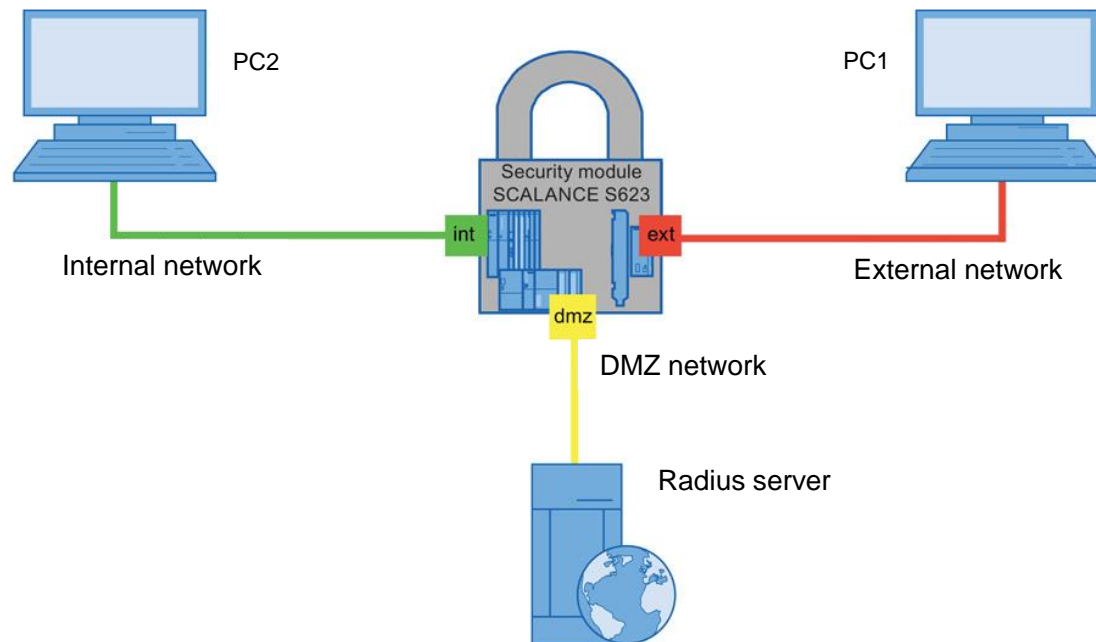
Pinging 192.168.9.2 with 32 bytes of data:
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Reply from 192.168.9.2: bytes=32 time=1ms TTL=63
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

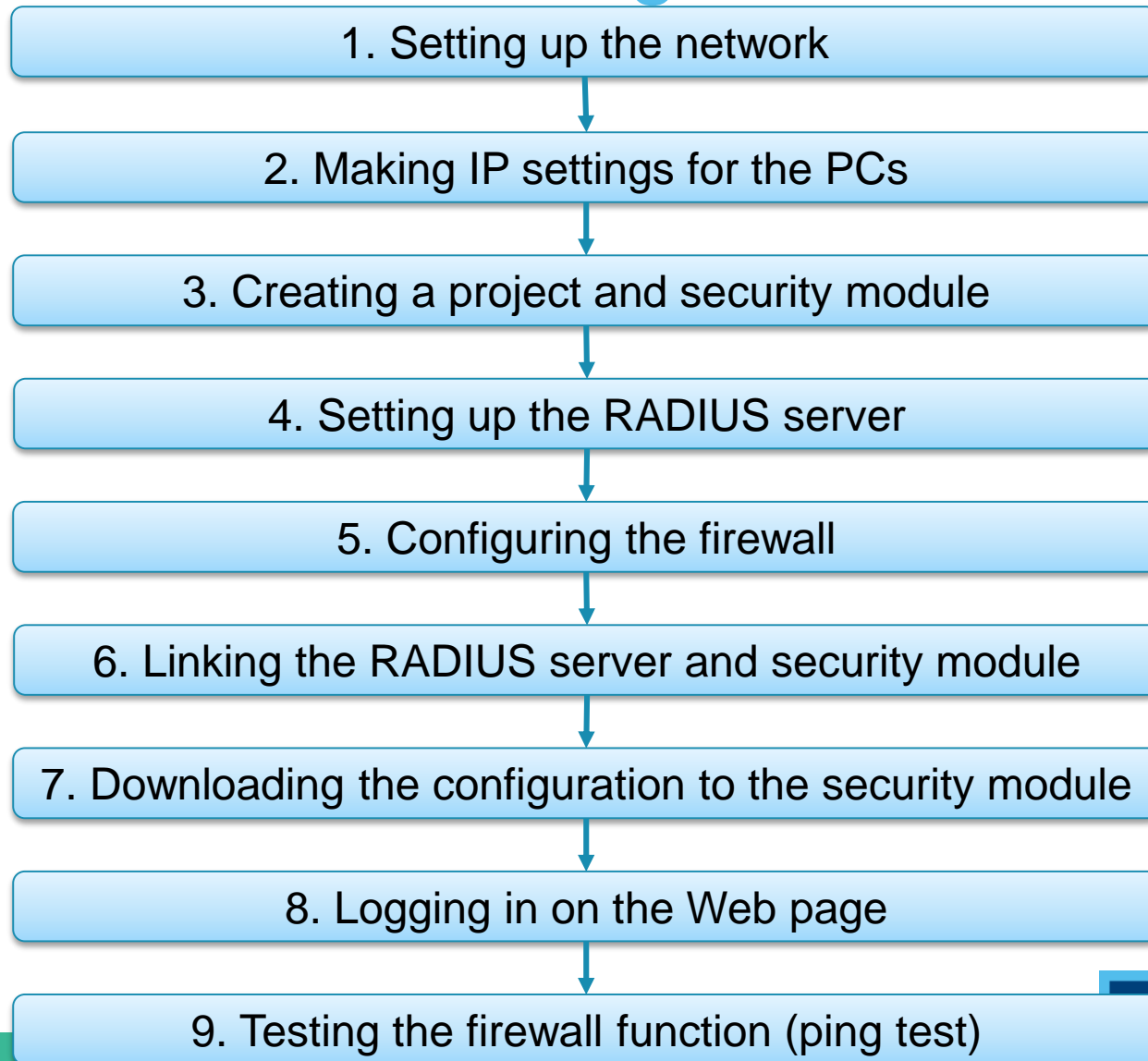
- All packets reach PC2

Advanced User Management



In this example, a RADIUS server is set up to manage user accounts. Only users that can authenticate to the RADIUS server can access the internal network from the external network

Advanced User Management



Advanced User Management

1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface
- Connect the Linux PC that will be used as RADIUS server to the DMZ interface

Advanced User Management

2. Making IP settings for the PCs

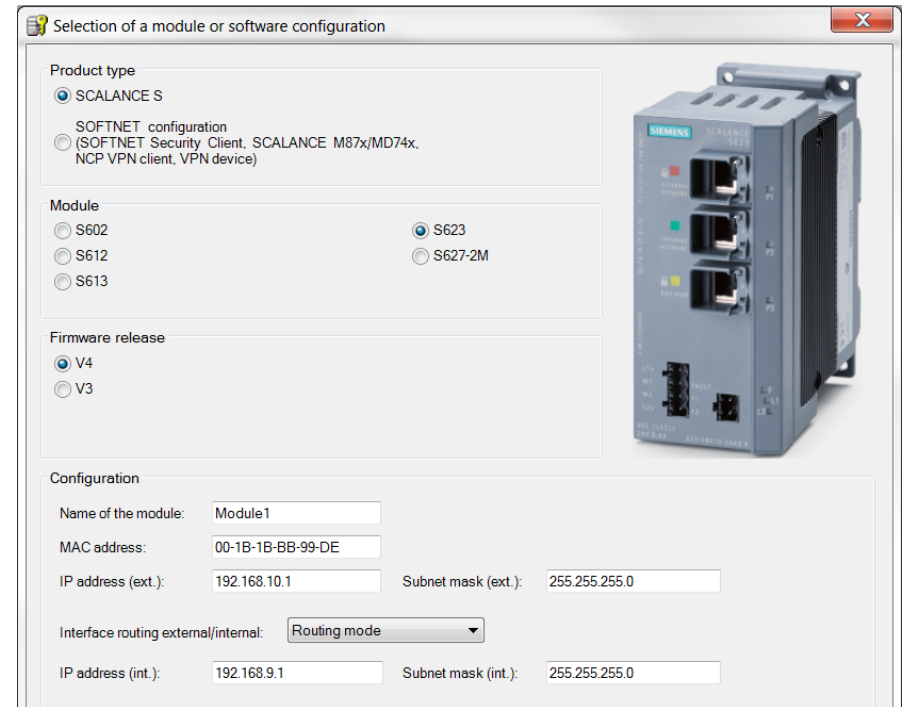
PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.9.2	255.255.255.0	192.168.9.1
RADIUS	192.168.8.2	255.255.255.0	192.168.8.1

- Set the IP addresses of the PCs as in the table above
- The IP address of the Linux PC is preset to the correct value

Advanced User Management

3. Creating a project and security module

- Create a new project
- In the “Configuration” area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the “Routing mode”
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with “OK”



The screenshot shows a software configuration window titled "Selection of a module or software configuration". It contains several sections for configuring a Siemens SCALANCE S module:

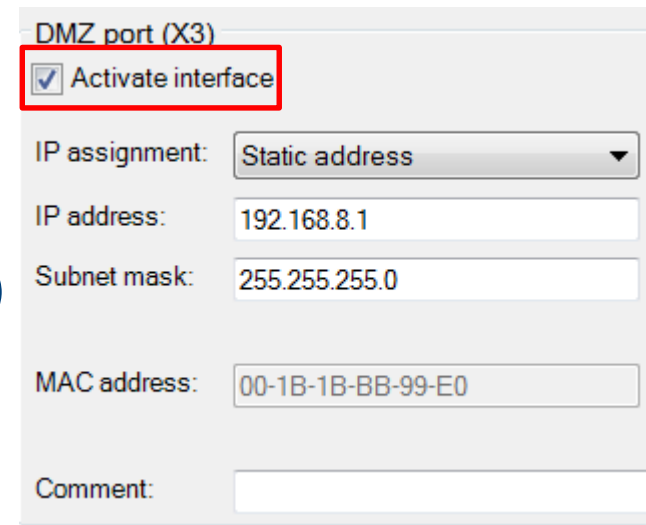
- Product type:** ☒ SCALANCE S (SOFTNET configuration) and ☐ (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device).
- Module:** ☐ S602, ☒ S623, ☐ S612, ☐ S613, and ☐ S627-2M.
- Firmware release:** ☒ V4 and ☐ V3.
- Configuration:**
 - Name of the module: Module1
 - MAC address: 00-1B-1B-BB-99-DE
 - IP address (ext.): 192.168.10.1 Subnet mask (ext.): 255.255.255.0
 - Interface routing external/internal: Routing mode (dropdown menu)
 - IP address (int.): 192.168.9.1 Subnet mask (int.): 255.255.255.0

An image of the SCALANCE S module is shown on the right side of the window.

Advanced User Management

3. Creating a project and security module

- Select the security module created and select the “Edit” > “Properties” menu command, “Interfaces” tab
- Select the “Activate Interface” check box in the “DMZ port (X3)” area
- Enter the IP address (192.168.8.1) and the subnet mask (255.255.255.0) for the DMZ interface
- Confirm with “OK”



DMZ port (X3)

☒ Activate interface

IP assignment: Static address

IP address: 192.168.8.1

Subnet mask: 255.255.255.0

MAC address: 00-1B-1B-BB-99-E0

Comment:

Advanced User Management

4. Setting up the RADIUS server

- On the Linux PC open the Web browser and go to “<http://freeradius.org/download.html>”
- Download version 3.0.9 of the RADIUS server

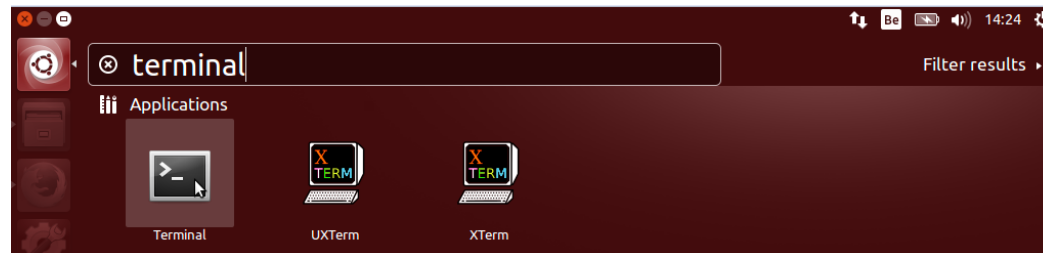
Downloads

3.0.x Series - Stable

Version 3.0.9: tar.gz (PGP Signature)

Version 3.0.9: tar.bz2 (PGP Signature)

- Open the Terminal
Open the Dash and type “terminal”



Advanced User Management

4. Setting up the RADIUS server

- Go to the “Downloads” map (“cd Downloads”)

```
vincent@vincent-VirtualBox:~$ cd Downloads  
vincent@vincent-VirtualBox:~/Downloads$
```

- Unpack the RADIUS server (“tar zxvf freeradius-server-3.0.9.tar.gz”)
- Enter the newly made map (“cd freeradius-server-3.0.9”)

Advanced User Management

4. Setting up the RADIUS server

- Install the server with the following commands
“./configure”
“make”
“sudo make install”

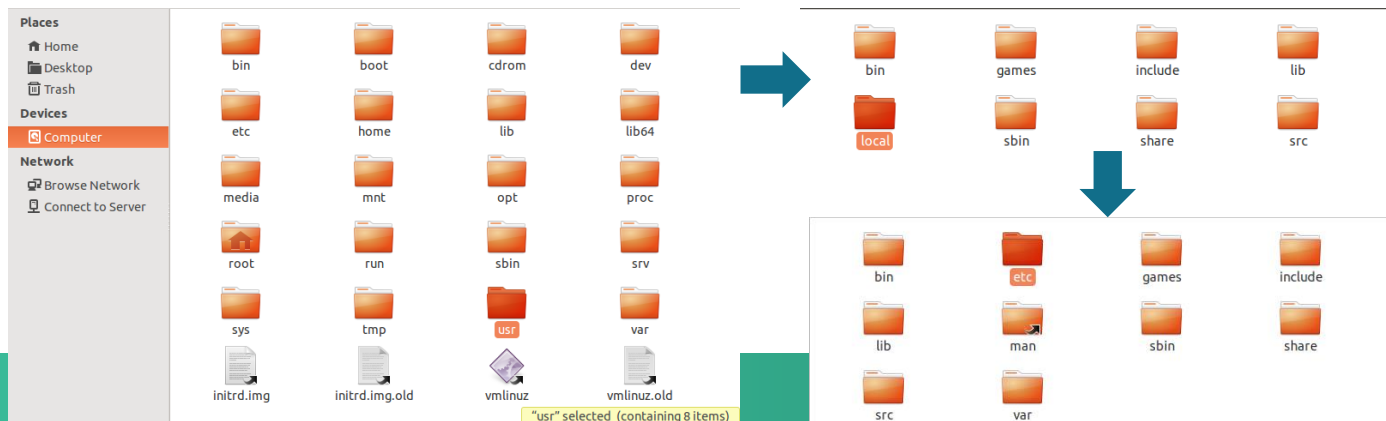
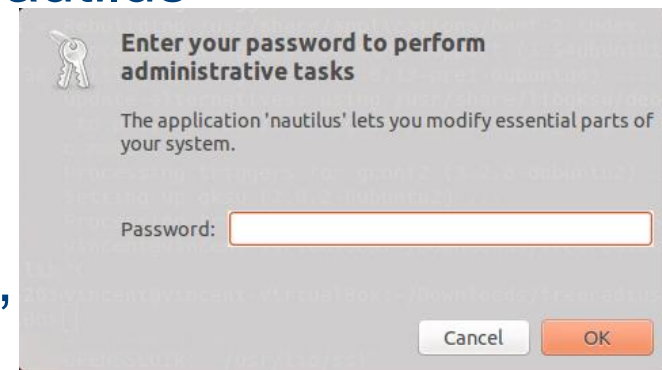
```
vincent@vincent-VirtualBox:~/Downloads/freeradius-server-3.0.9$ sudo make instal  
l  
[sudo] password for vincent:
```

The password is **TBD**

Advanced User Management

4. Setting up the RADIUS server

- The next step is to configure the clients of the server
- Open the file explorer with “gksudo nautilus”
Enter the sudo password in the following prompt
- Using Nautilus browse to “Computer”
> “usr” > “local” > “etc” > “raddb”



Advanced User Management

4. Setting up the RADIUS server

- Open “clients.conf” and add a new client as in the image

```
#Scalance client for demo
client scalance {
    ipaddr = 192.168.8.1
    secret = SiemensSecret
}
```

- Save and close the window
- Open “users” and add the following users

```
radius Cleartext-Password := "password"
radius2 Cleartext-Password := "password2"
```

- Save and close the window

Advanced User Management

4. Setting up the RADIUS server

- With the server installed and configured, run “sudo radiusd -X” to start the server in debug mode

```
Refusing to start with libssl version OpenSSL 1.0.1f 6 Jan 2014 0x1000106f (1.0.1f release) (in range 1.0.1 dev - 1.0.1f release)
Security advisory CVE-2014-0160 (Heartbleed)
For more information see http://heartbleed.com
Once you have verified libssl has been correctly patched, set security.allow_vulnerable_openssl = 'CVE-2014-0160'
```

- If this error shows up, check the OpenSSL version with “openssl version -a”

This command should show the following date:

‘built on: Thu Jun 11’

```
vincent@vincent-VirtualBox:~$ openssl version -a
OpenSSL 1.0.1f 6 Jan 2014
built on: Thu Jun 11 15:28:12 UTC 2015
```

Advanced User Management

4. Setting up the RADIUS server

- If this date is not shown update the library with the following command
“sudo apt-get update”
“sudo apt-get upgrade”
- If OpenSSL is correctly updated, open “radius.conf” and change the “allow_vulnerable_openssl” parameter to yes

`allow_vulnerable_openssl = no` ➡ `allow_vulnerable_openssl = yes`

- Save and close the window
- Try starting the server again with “sudo radiusd -X”

Advanced User Management

5. Configuring the firewall

- Enter “Advanced mode” in the Security Configuration Tool
- Use the menu command “Options” > “User Management”
- Create a new user with the following settings
- Confirm with “OK”

The screenshot shows the 'Edit users' dialog box with the following settings:

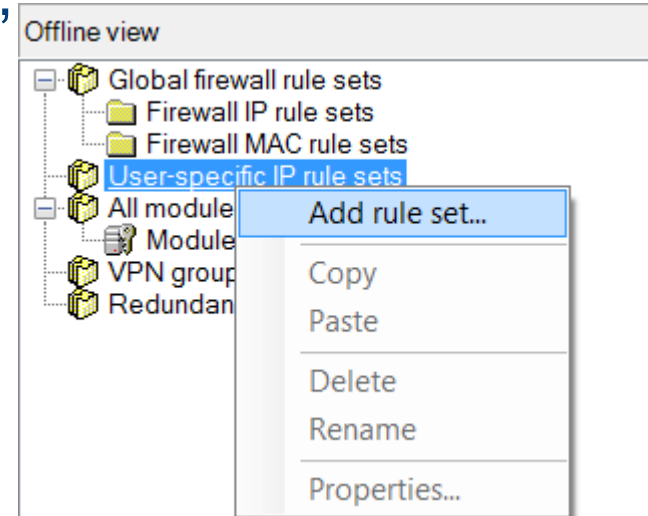
- User data:**
 - User name: radius
 - Authentication method: RADIUS
 - Password: (empty)
 - Repeat password: (empty)
 - Comment: (empty)
- Settings for user-specific IP rule sets:**
 - Maximum time of the session: 30 Minutes
- Role:**
 - Assigned role: radius

Buttons: OK, Cancel, Help

Advanced User Management

5. Configuring the firewall

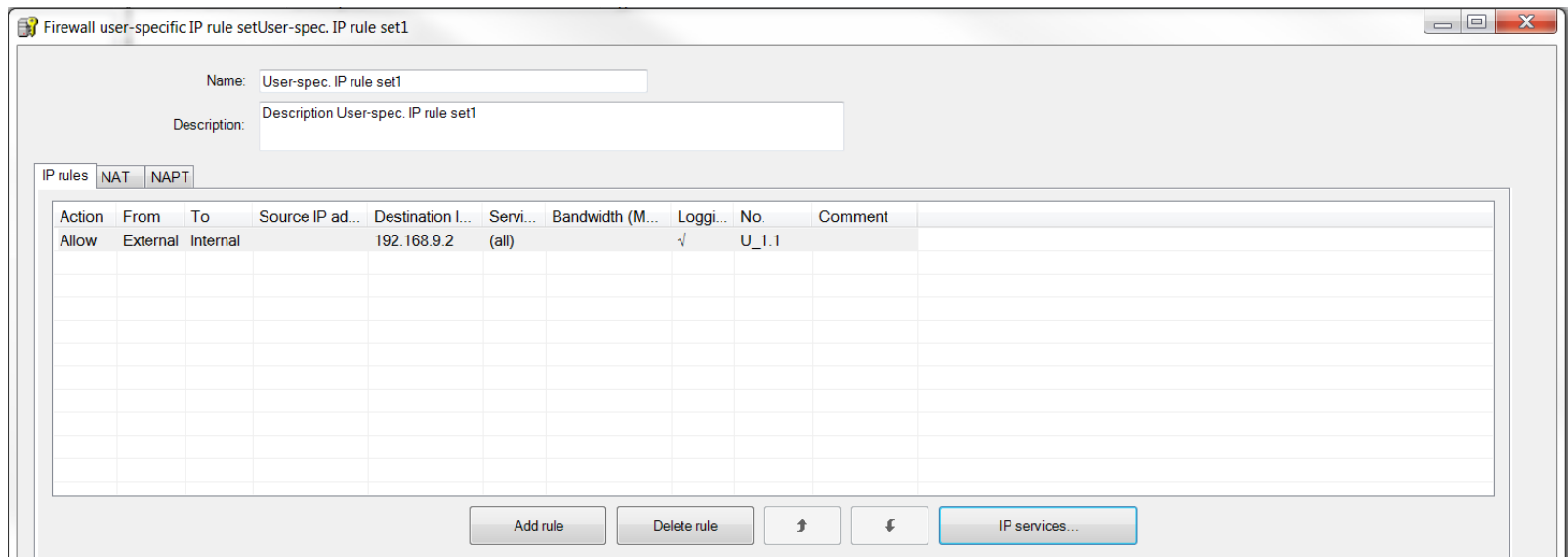
- Select the “User-specific IP rule sets” in the navigation window
- Select the “Add rule set...” option in the shortcut menu



Advanced User Management

5. Configuring the firewall

- Enter a rule in the dialog as shown below



Advanced User Management

5. Configuring the firewall

- From the “Available users and roles” list, select the “radius (user)” entry and click the “Assign” button, then select the “radius (role)” entry and click “Assign”

Available users and roles:		Assigned users and roles:
admin (User) administrator (Role) administrator(radius) (Role) diagnostics (Role) remote access (Role) standard (Role)	Assign Remove	radius (Role) radius (User)

- Confirm with “OK”

Advanced User Management

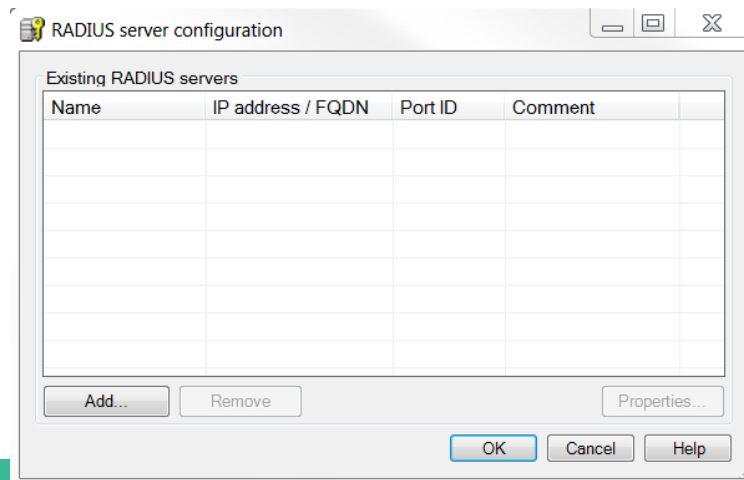
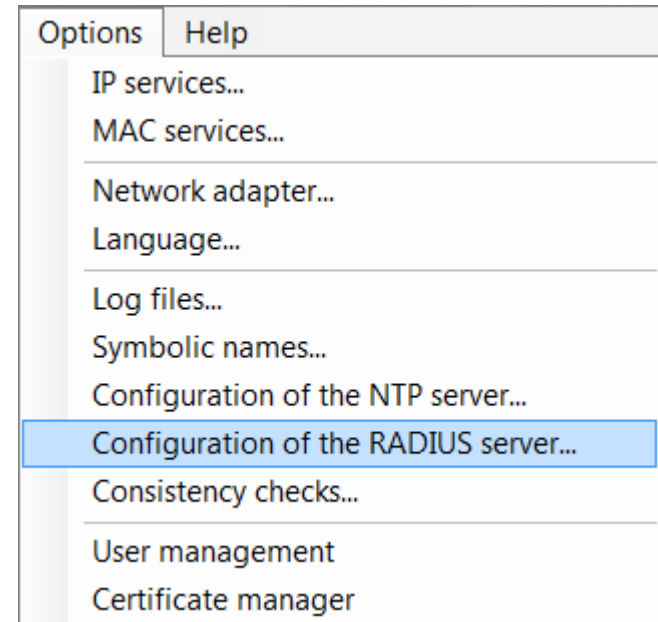
5. Configuring the firewall

- Select the security module in the navigation panel and drag it to the newly created user-specific IP rule set
- The assignment can be checked by opening the module properties and selecting the “Firewall” tab

Advanced User Management

6. Linking the RADIUS server and security module

- Select the menu option “Options” > “Configuration of the RADIUS server...”
- Click the “Add...” button in the dialog

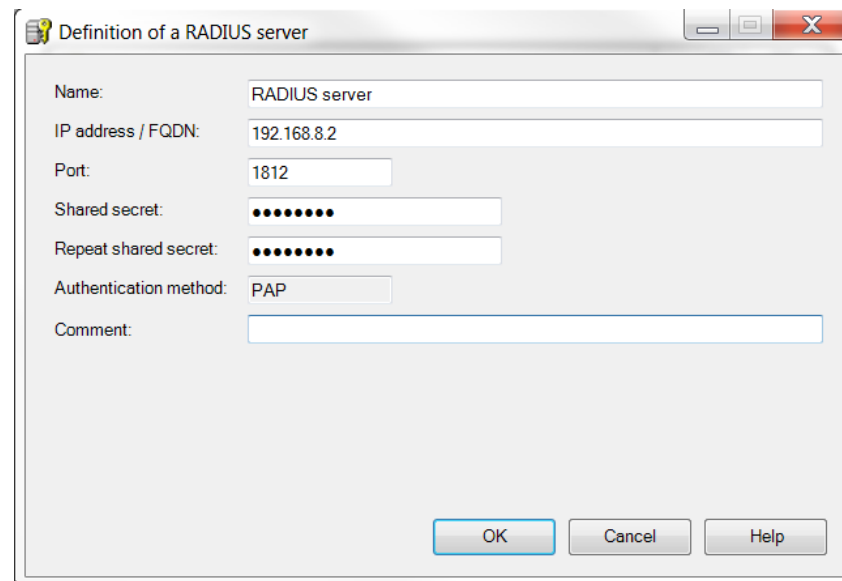


Advanced User Management

6. Linking the RADIUS server and security module

- Define the server with the following values
 - IP address/FQDN: 192.186.8.2
 - Shared secret: SiemensSecret
 - Repeat shared secret: SiemensSecret

- Confirm with “OK”

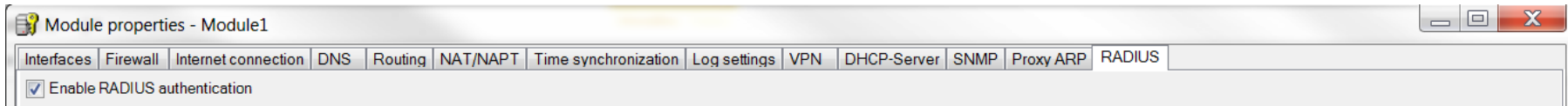


The screenshot shows a Windows-style dialog box titled "Definition of a RADIUS server". It contains several input fields and buttons. The fields are: "Name:" with the value "RADIUS server", "IP address / FQDN:" with the value "192.168.8.2", "Port:" with the value "1812", "Shared secret:" with a masked value ".....", "Repeat shared secret:" with a masked value ".....", "Authentication method:" with the value "PAP", and "Comment:" which is empty. At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

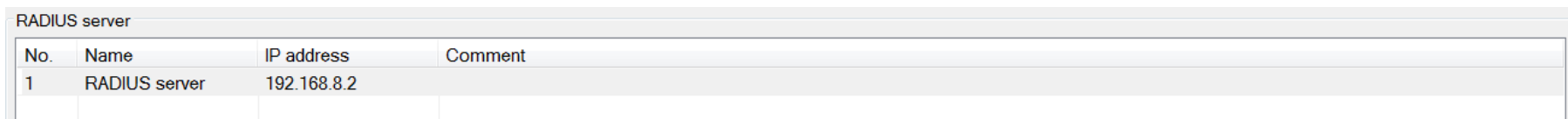
Advanced User Management

6. Linking the RADIUS server and security module

- Open the SCALANCE S module properties and go to the “RADIUS” tab



- Check the “Enable RADIUS authentication” box
- Click the “Add” button
This adds the newly configured RADIUS server

A screenshot of a table titled 'RADIUS server'. The table has four columns: 'No.', 'Name', 'IP address', and 'Comment'. There is one row of data with the following values: '1' in the 'No.' column, 'RADIUS server' in the 'Name' column, '192.168.8.2' in the 'IP address' column, and an empty cell in the 'Comment' column.

No.	Name	IP address	Comment
1	RADIUS server	192.168.8.2	

Advanced User Management

6. Linking the RADIUS server and security module

- In the “RADIUS setting” area, check the “Allow RADIUS authentication of non-configured users” box

RADIUS settings

RADIUS timeout: Seconds

RADIUS retries:

☒ Allow RADIUS authentication of non-configured users

☐ Filter ID is required for authentication

- Confirm with “OK”

Advanced User Management

7. Downloading the configuration to the security module

- Transfer the configuration to the SCALANCE S module

Advanced User Management

8. Logging in on the Web page

- In the Web browser of PC1, enter the address “https://192.168.10.1”



The screenshot shows the login interface for the SCALANCE S user-specific firewall. The page has a dark blue header with the 'SIEMENS' logo on the left and a language dropdown set to 'English' on the right. Below the header, the page title 'SCALANCE S' is displayed. The main content area is light blue and contains the text 'Welcome to the SCALANCE S user-specific firewall'. Below this, it says 'Please log on:'. There are two input fields: 'Name' and 'Password'. A 'Log in' button is located below the password field.

SIEMENS English Go

SCALANCE S

Welcome to the SCALANCE S user-specific firewall

Please log on:

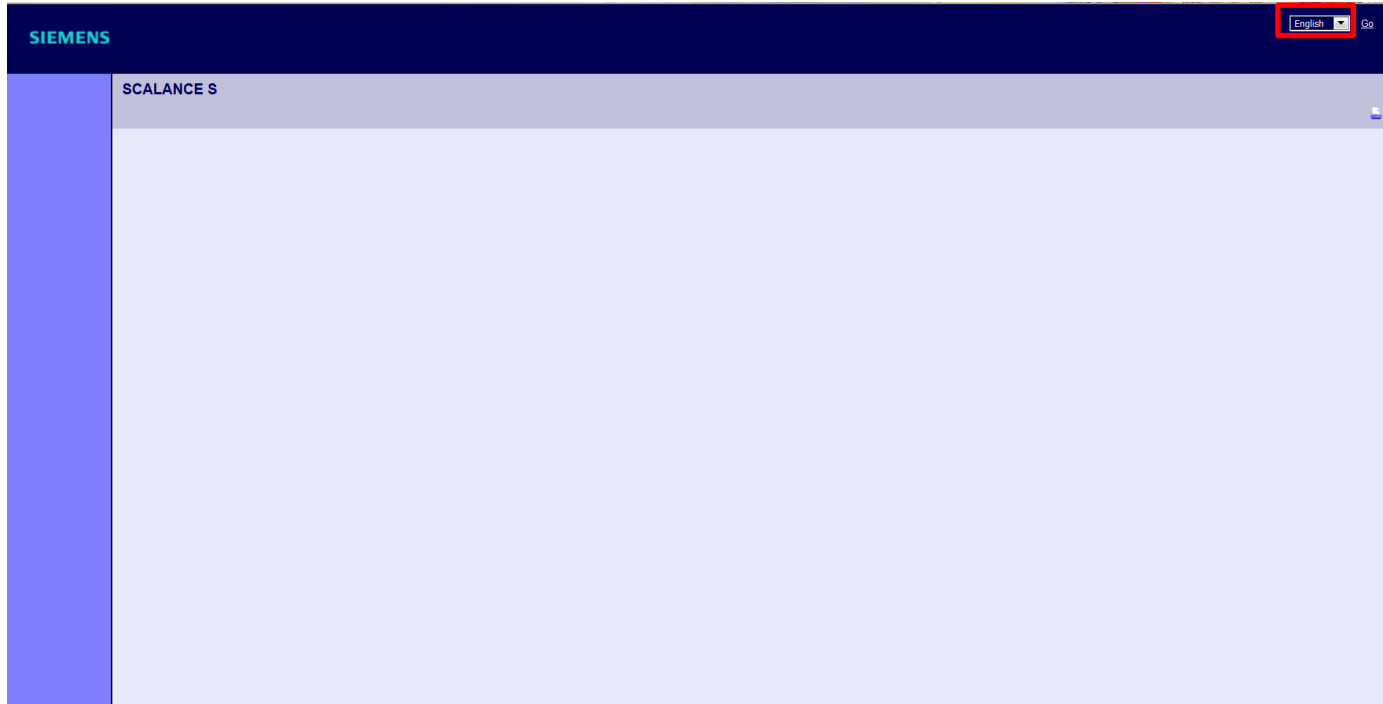
Name

Password

Advanced User Management

8. Logging in on the Web page

- If the web page does not show the login fields, try changing the language in the upper right corner



Advanced User Management

8. Logging in on the Web page

- Enter the user name “radius” and corresponding password and click the “Log in” button



The screenshot shows the Siemens SCALANCE S user-specific firewall login page. The page has a dark blue header with the Siemens logo on the left and a language dropdown menu set to 'English' on the right. Below the header, the page title 'SCALANCE S' is displayed. The main content area has a light blue background and contains the text 'Welcome to the SCALANCE S user-specific firewall'. Below this, it says 'Please log on:'. There are two input fields: 'Name' with the value 'radius' and 'Password' with a masked password of eight dots. A 'Log in' button is located below the password field.

SIEMENS

English Go

SCALANCE S

Welcome to the SCALANCE S user-specific firewall

Please log on:

Name radius

Password ••••••••

Log in

Advanced User Management

8. Logging in on the Web page

- The defined IP rule set is enabled for the “radius” user.



Advanced User Management

8. Logging in on the Web page

- Now click the “Log out” button
- Enter the user name “radius2” and corresponding password and click the “Log in” button



The screenshot shows the Siemens SCALANCE S user-specific firewall login page. The page has a dark blue header with the Siemens logo on the left and a language dropdown set to 'English' on the right. Below the header, the page title 'SCALANCE S' is displayed. The main content area is light blue and contains the text 'Welcome to the SCALANCE S user-specific firewall'. Below this, it says 'Please log on:'. There are two input fields: 'Name' with the value 'radius2' and 'Password' with masked characters. A 'Log in' button is located below the password field.

SIEMENS

English Go

SCALANCE S

Welcome to the SCALANCE S user-specific firewall

Please log on:

Name radius2

Password

Log in

Advanced User Management

8. Logging in on the Web page

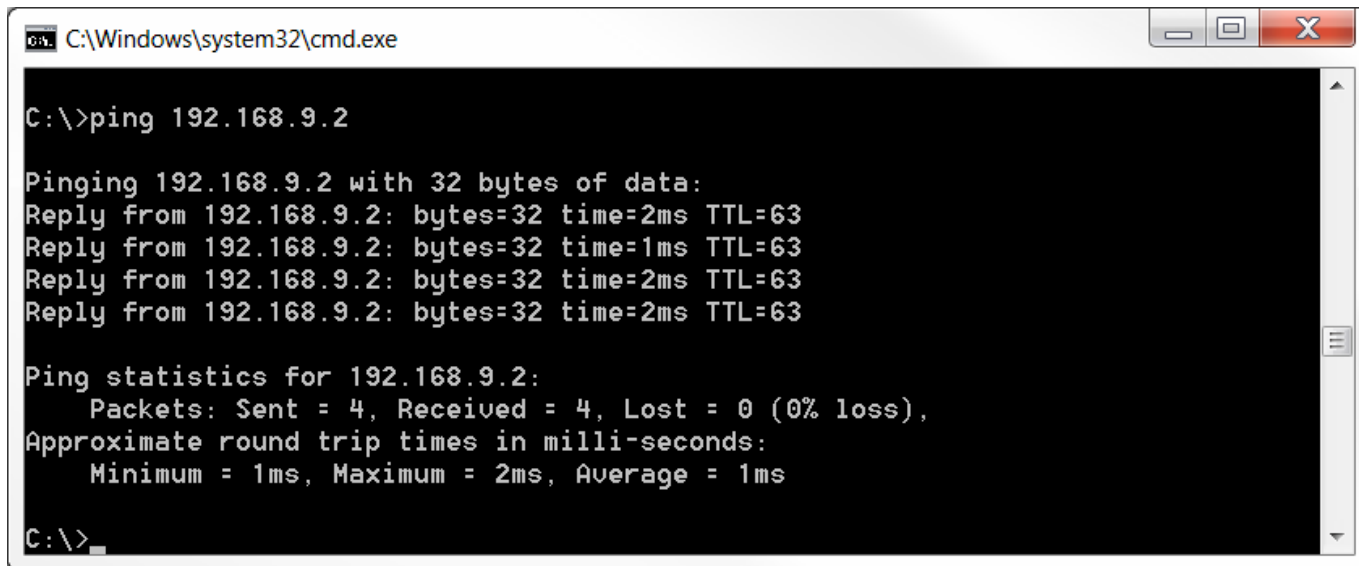
- The defined IP rule set for the “radius” role is enabled
→ Users that are not defined on the module can log in



Advanced User Management

9. Testing the firewall function (ping test)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC2
“ping 192.168.9.2”



```
C:\Windows\system32\cmd.exe

C:\>ping 192.168.9.2

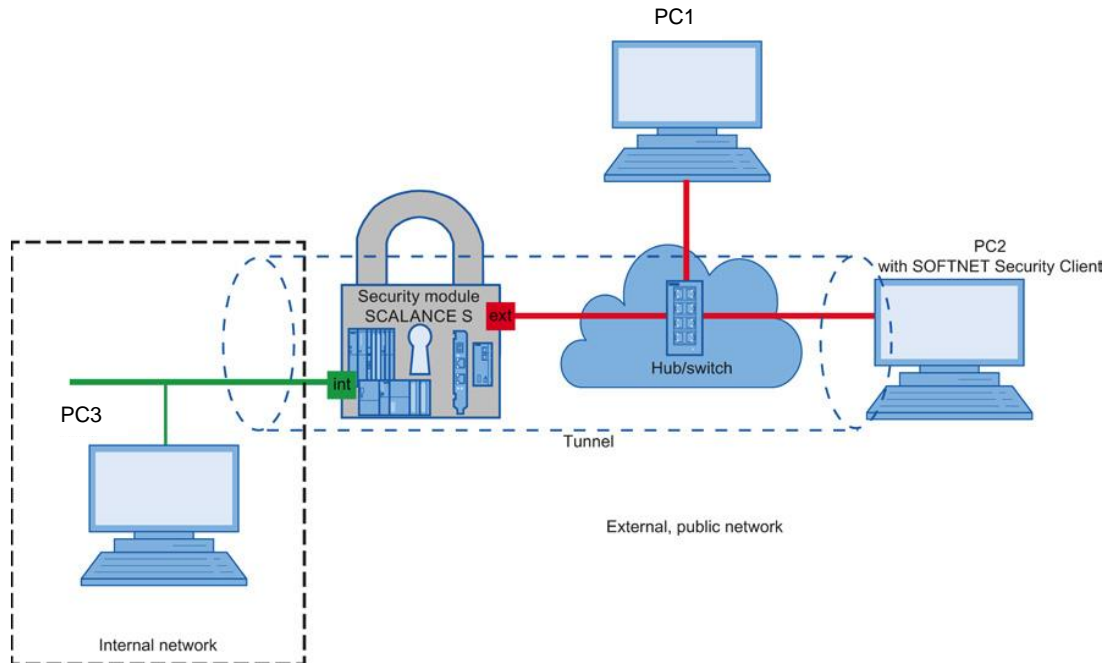
Pinging 192.168.9.2 with 32 bytes of data:
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Reply from 192.168.9.2: bytes=32 time=1ms TTL=63
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

- All packets reach PC2

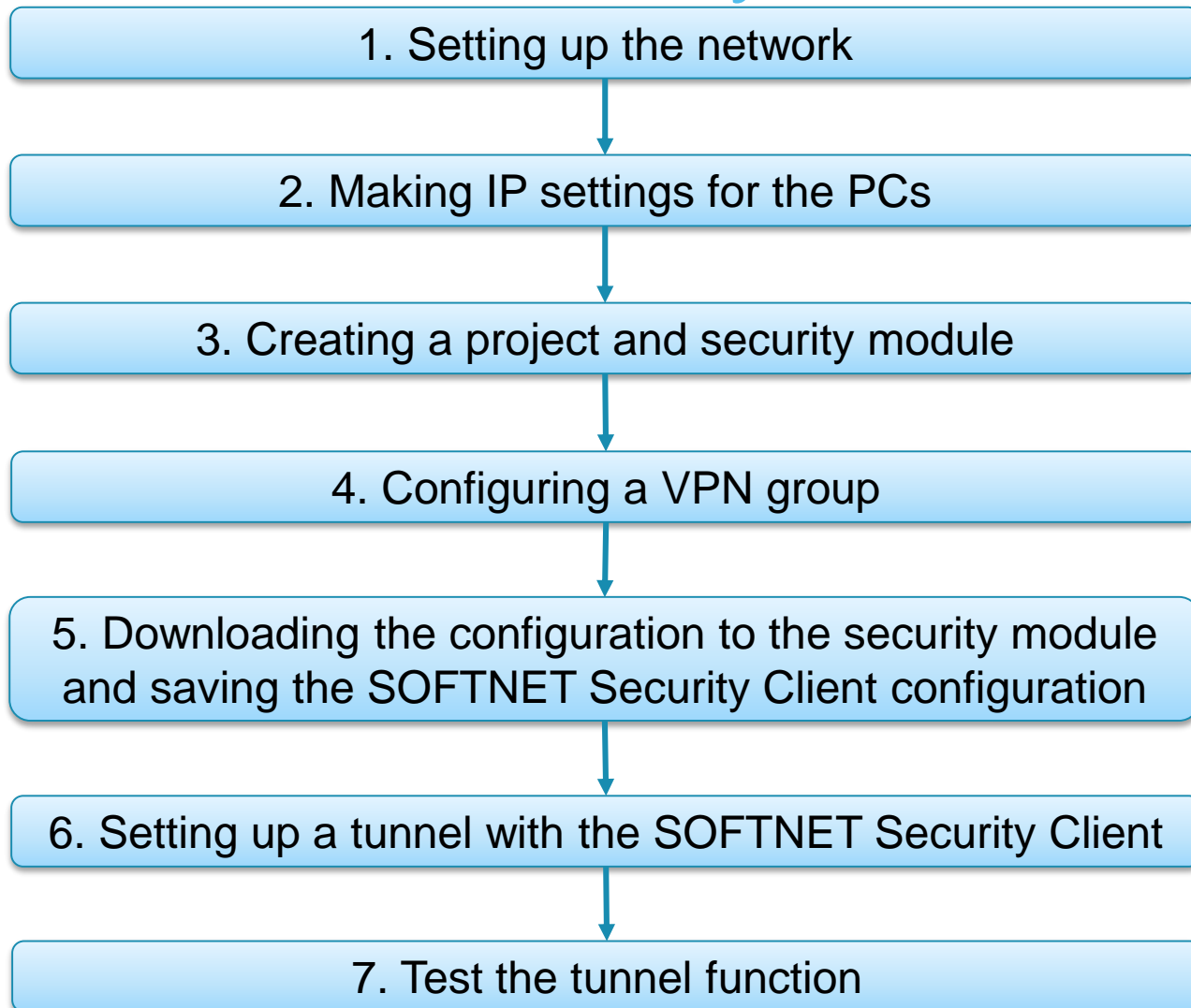
VPN with Preshared Key



In this example, a VPN tunnel is configured between a security module and the SOFTNET Security Client

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

VPN with Preshared Key



VPN with Preshared Key

1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the switch to the external network interface
- Connect the PC with the Security Configuration Tool (PC1) and the PC with the SOFTNET Security Client (PC2) to the switch
- Connect PC3 to the internal network interface

VPN with Preshared Key

2. Making IP settings for the PCs

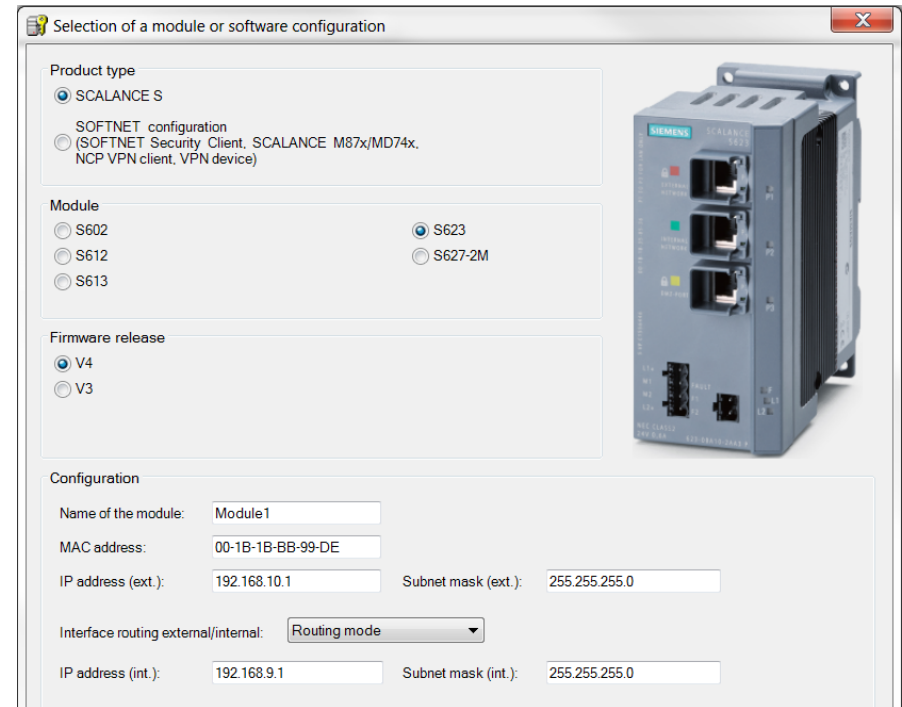
PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.10.3	255.255.255.0	192.168.10.1
PC3	192.168.9.2	255.255.255.0	192.168.9.1

- Set the IP addresses of the PCs as in the table above

VPN with Preshared Key

3. Creating a project and security module

- Create a new project
- In the “Configuration” area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the “Routing mode”
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with “OK”



Selection of a module or software configuration

Product type

- ☒ SCALANCE S
- ☐ SOFTNET configuration (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

- ☐ S602
- ☐ S612
- ☐ S613
- ☒ S623
- ☐ S627-2M

Firmware release

- ☒ V4
- ☐ V3

Configuration

Name of the module: Module1

MAC address: 00-1B-1B-BB-99-DE

IP address (ext.): 192.168.10.1 Subnet mask (ext.): 255.255.255.0

Interface routing external/internal: Routing mode

IP address (int.): 192.168.9.1 Subnet mask (int.): 255.255.255.0

VPN with Preshared Key

3. Creating a project and security module

- Use the “Insert” > “Module” menu command with the following parameters
 - Product type: SOFTNET configuration
 - Module: SOFTNET Security Client
 - Firmware release: V4
- Confirm with “OK”

Selection of a module or software configuration

Product type

- ☐ SCALANCE S
- ☒ SOFTNET configuration
(SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

- ☒ SOFTNET Security Client
- ☐ SCALANCE M87x/MD74x
- ☐ NCP VPN client for Android
- ☐ VPN device

Firmware release

- ☒ V4
- ☐ V3
- ☐ 2005
- ☐ 2008

Configuration

Name of the module:

MAC address:

IP address (ext.): Subnet mask (ext.):

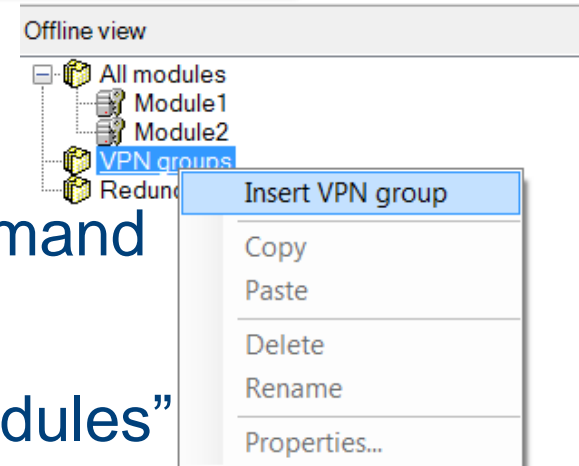
Interface routing external/internal:

IP address (int.): Subnet mask (int.):

VPN with Preshared Key

4. Configuring a VPN group

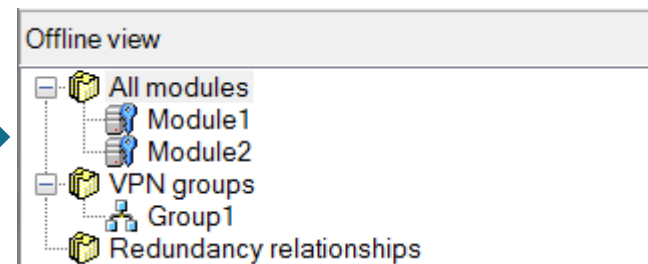
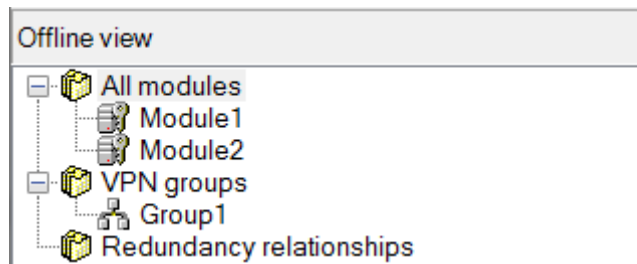
- Select “VPN groups” in the navigation
- Select the “Insert” > “Group” menu command
- In the navigation panel, click the “All modules” entry
- Drag the Scalance S Module to the VPN group “Group1” in the navigation panel
The module is now assigned to the VPN group
The color of the key symbol changes to blue



VPN with Preshared Key

4. Configuring a VPN group

- Drag the SOFTNET Security Client module to the VPN group “Group1” in the navigation panel
The module is now assigned to the VPN group
The color of the key symbol changes to blue

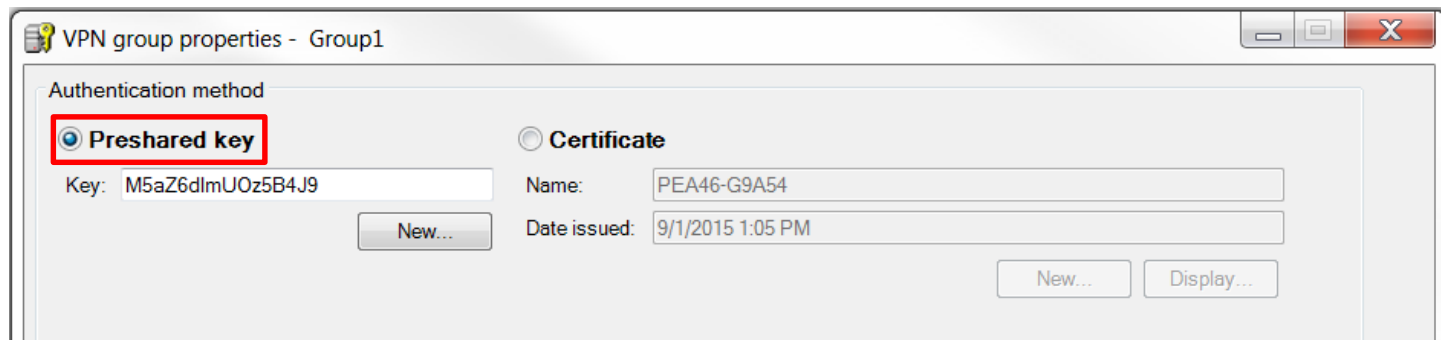


- Activate “Advanced Mode”

VPN with Preshared Key

4. Configuring a VPN group

- Select the VPN group “Group1” in the Navigation windows and select the menu command “Edit” > “Properties”
- Select the “Preshared key” option in the “Authentication method” area

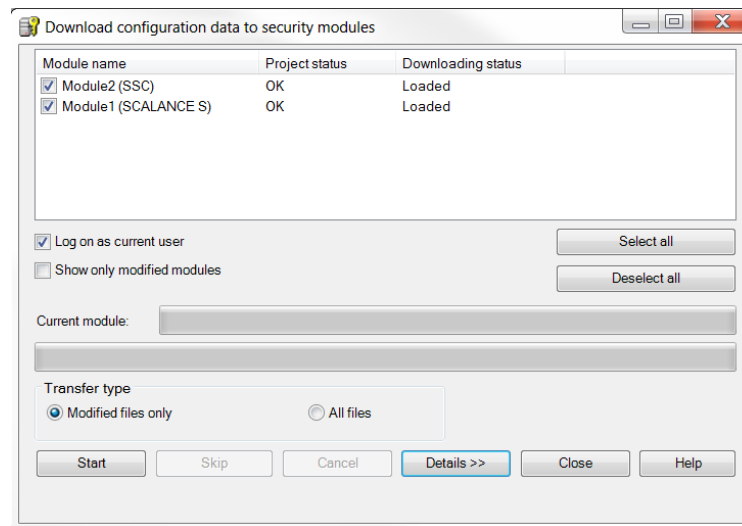


- Confirm with “OK”

VPN with Preshared Key

5. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the project
- Use the menu command “Transfer” > “To all modules...”



- Start the download with the “Start” button

VPN with Preshared Key

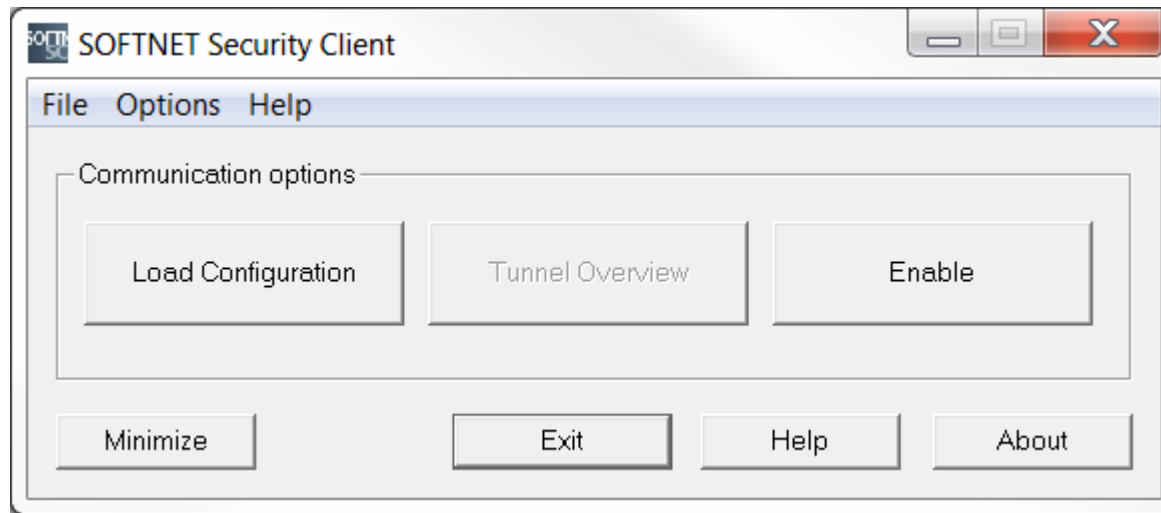
5. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the configuration file “projectname.Module2.dat” in your project folder
- Confirm the popup with “OK”

VPN with Preshared Key

6. Setting up a tunnel with the SOFTNET Security Client

- Open the SOFTNET Security Client on PC2

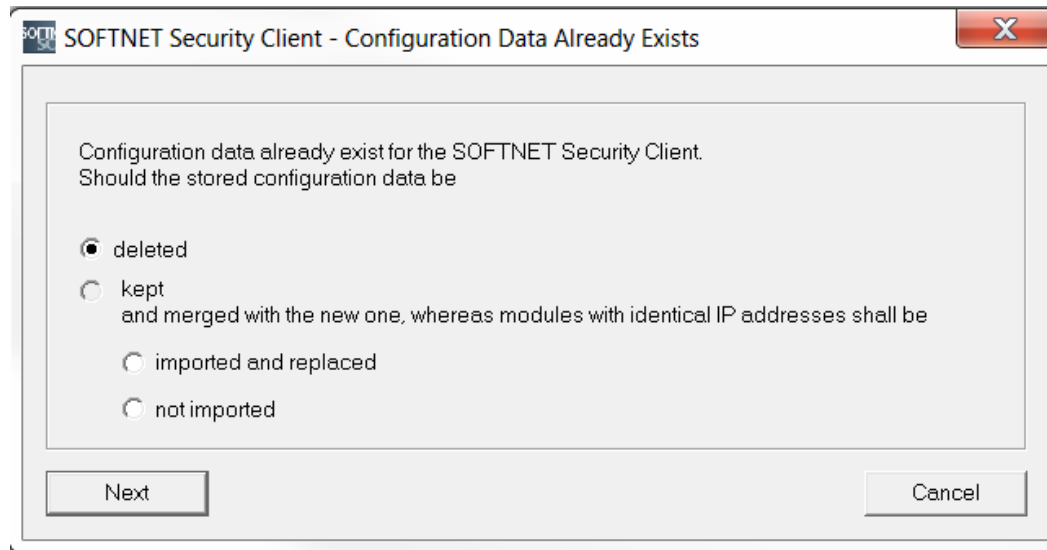


- Select “Load Configuration” and browse to where “projectname.Module2.dat” has been saved
- Open the configuration with the “Open” button

VPN with Preshared Key

6. Setting up a tunnel with the SOFTNET Security Client

- Loading a new configuration will delete any previous configurations

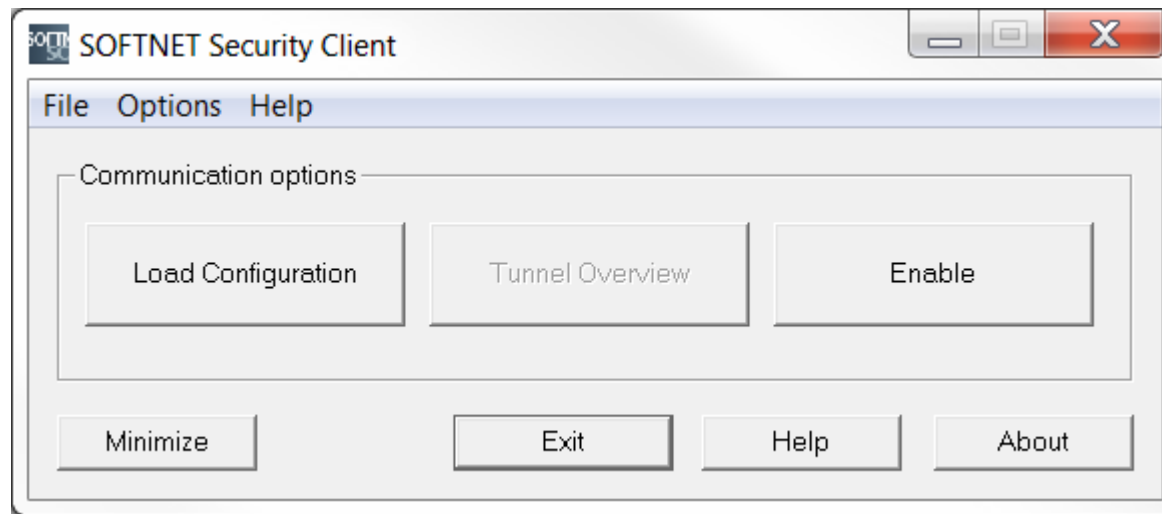


- When the dialog above pops up, select “deleted” and confirm with “Next”

VPN with Preshared Key

6. Setting up a tunnel with the SOFTNET Security Client

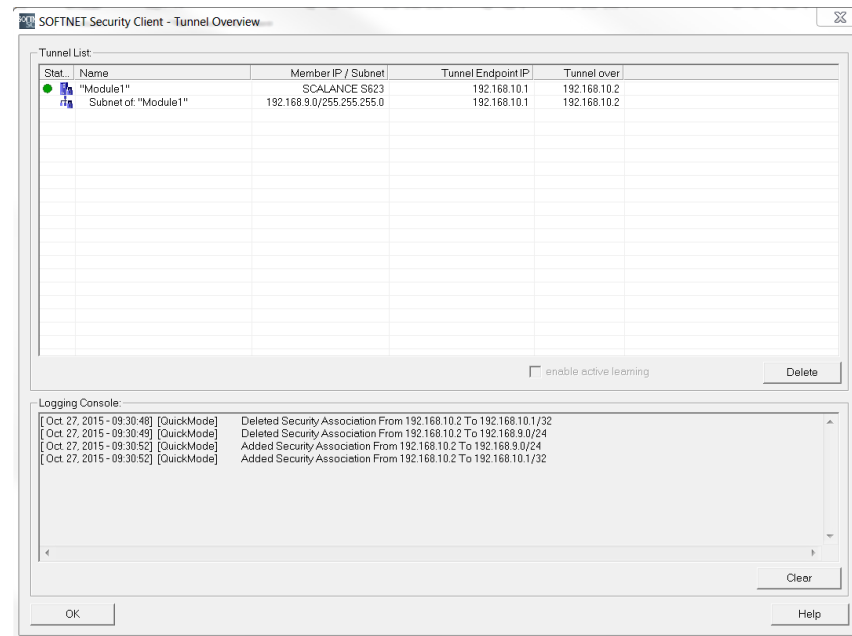
- The VPN tunnel can now be opened by clicking the “Enable” button



VPN with Preshared Key

6. Setting up a tunnel with the SOFTNET Security Client

- “Tunnel Overview” shows the status of the tunnel

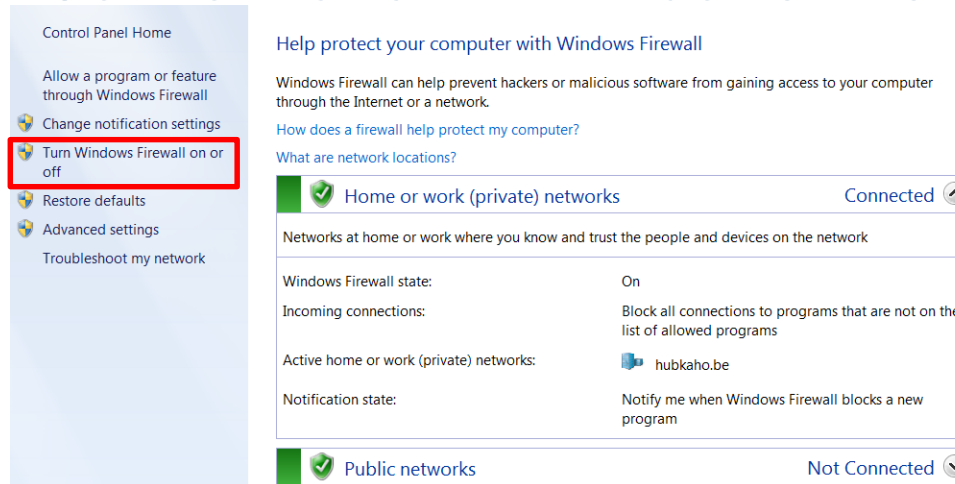


- The green circle shows that the tunnel has been established

VPN with Preshared Key

6. Setting up a tunnel with the SOFTNET Security Client

- If the tunnel does not get set up, check whether the Windows Firewall has been enabled
- Open the “Control Panel” > “Windows Firewall”

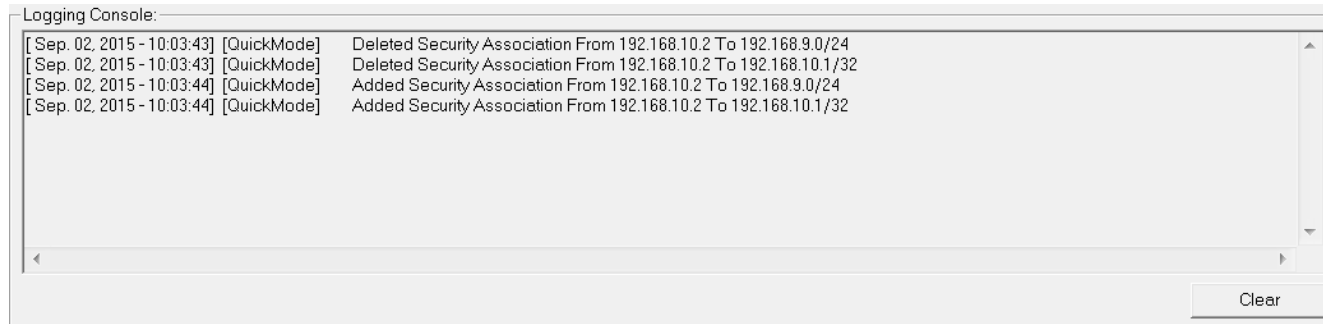


- If the firewall is not enabled, click “Turn Windows Firewall on or off” and enable it

VPN with Preshared Key

6. Setting up a tunnel with the SOFTNET Security Client

- In the Logging Console, the sequence of executed connection attempts is displayed

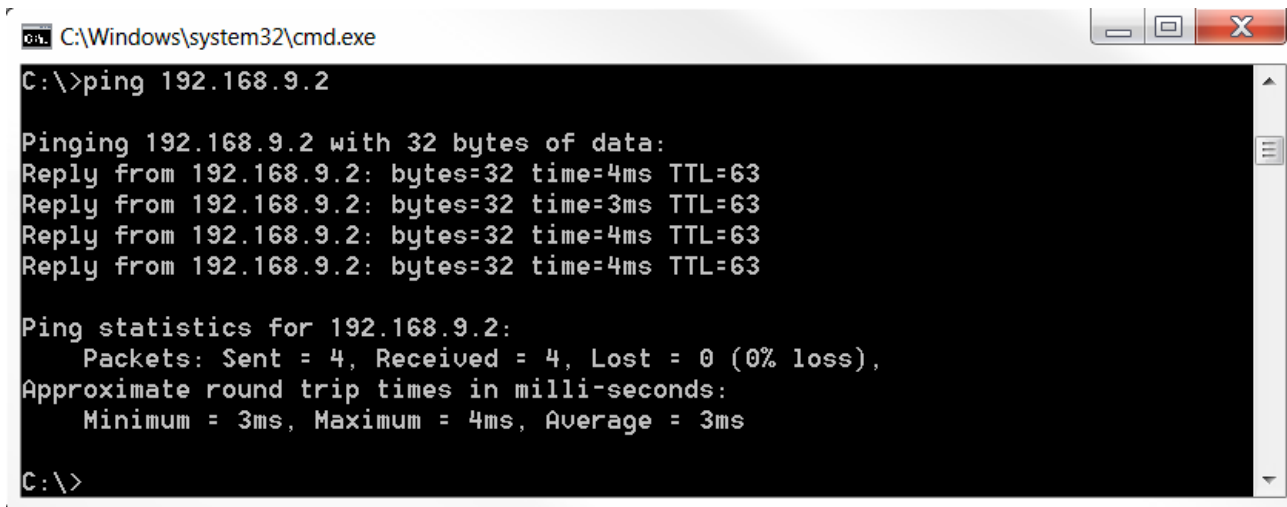


- The SCALANCE S module and the SOFTNET Security Client have established a communication tunnel

VPN with Preshared Key

7. Test the tunnel function

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC3
“ping 192.168.9.2”



```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.9.2

Pinging 192.168.9.2 with 32 bytes of data:
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63
Reply from 192.168.9.2: bytes=32 time=3ms TTL=63
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms

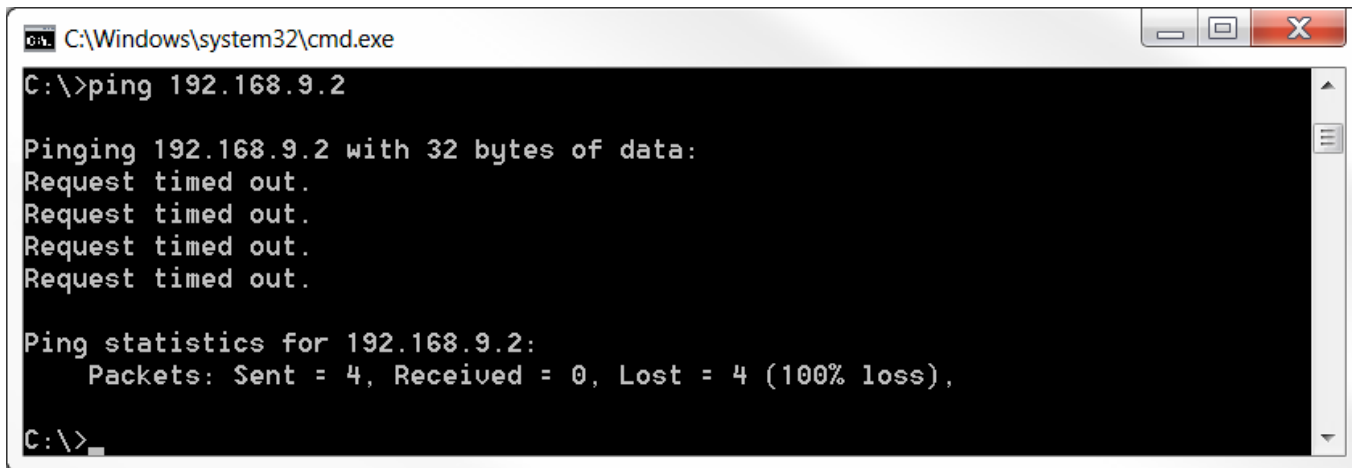
C:\>
```

- All packets reach PC3 through the tunnel

VPN with Preshared Key

7. Test the tunnel function

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC3
“ping 192.168.9.2”



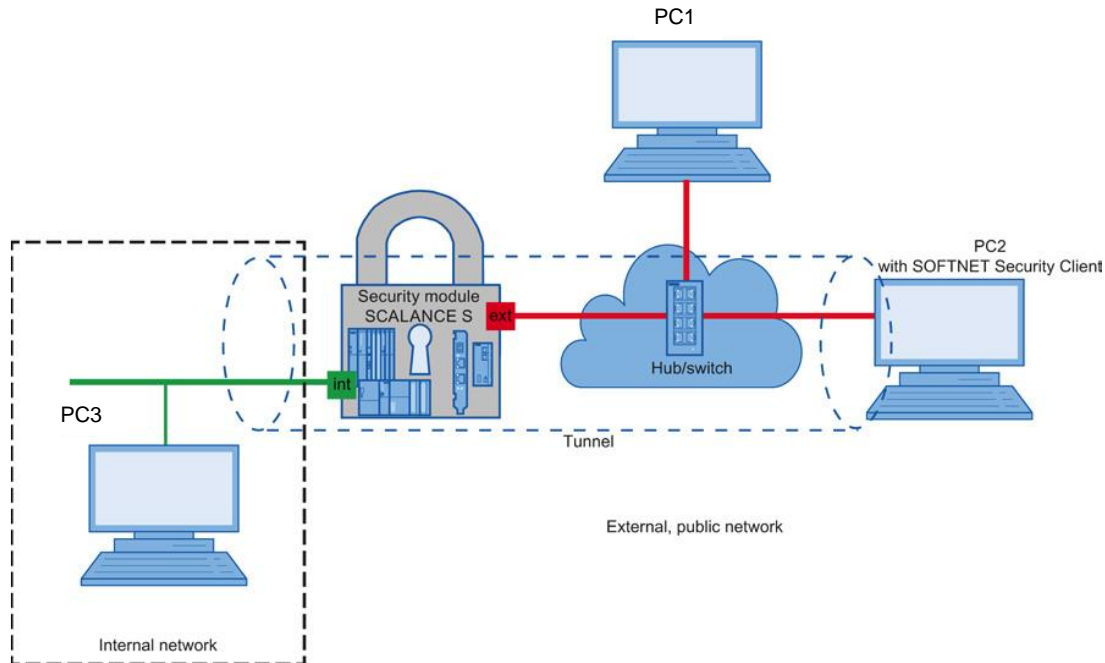
```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.9.2

Pinging 192.168.9.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

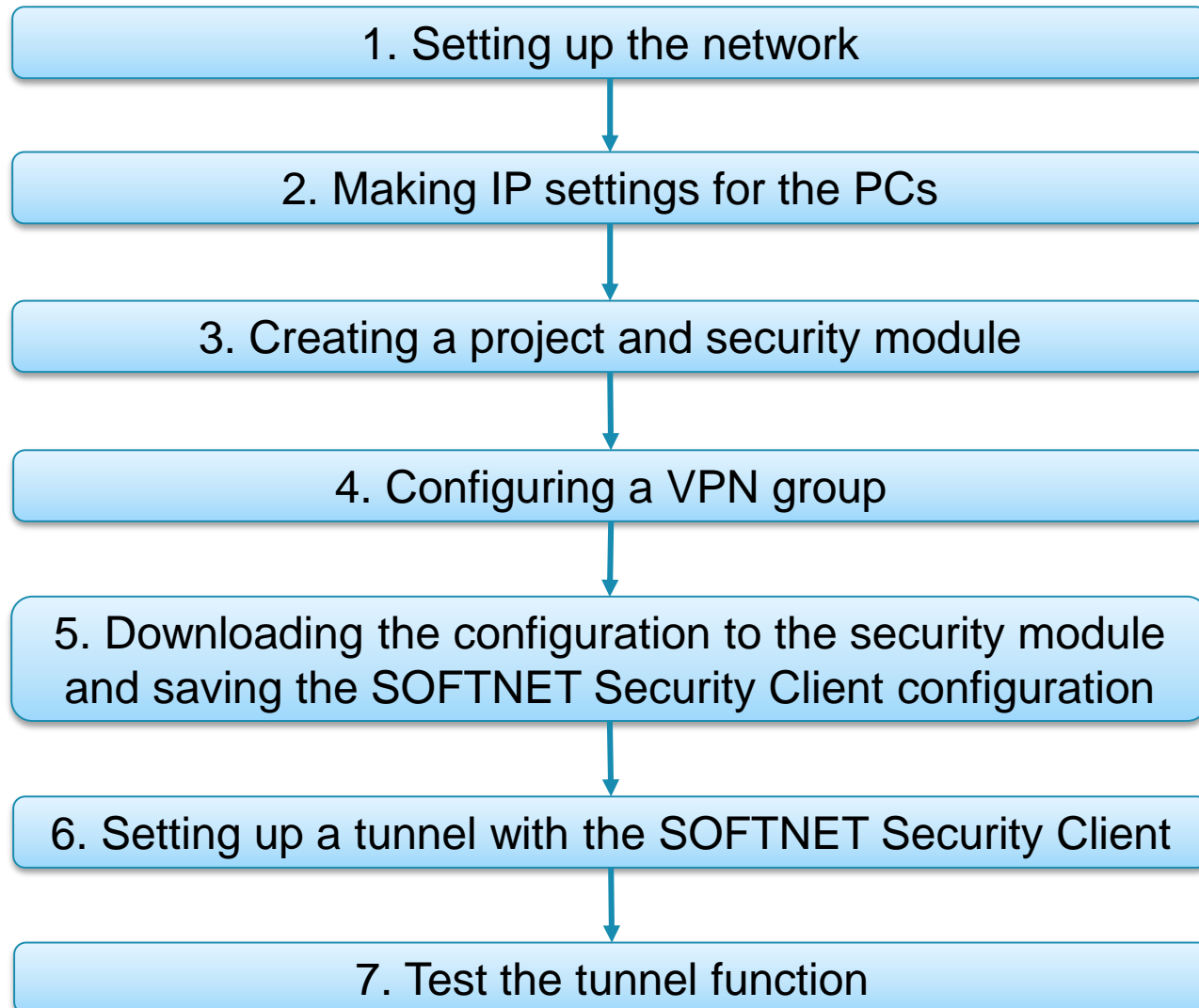
- The packets cannot reach PC3 since there is no tunnel communication between these two devices

VPN with Certificates



In this example, a VPN tunnel is configured between a security module and the SOFTNET Security Client
The endpoints authenticate using certificates

VPN with Certificates



VPN with Certificates

1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the switch to the external network interface
- Connect the PC with the Security Configuration Tool (PC1) and the PC with the SOFTNET Security Client (PC2) to the switch
- Connect PC3 to the internal network interface

VPN with Certificates

2. Making IP settings for the PCs

PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.10.3	255.255.255.0	192.168.10.1
PC3	192.168.9.2	255.255.255.0	192.168.9.1

- Set the IP addresses of the PCs as in the table above

VPN with Certificates

3. Creating a project and security module

- Create a new project
- In the “Configuration” area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the “Routing mode”
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with “OK”

Selection of a module or software configuration

Product type

☒ SCALANCE S

SOFTNET configuration
☐ (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

☐ S602 ☒ S623
☐ S612 ☐ S627-2M
☐ S613

Firmware release

☒ V4
☐ V3

Configuration

Name of the module: Module1

MAC address: 00-1B-1B-BB-99-DE

IP address (ext.): 192.168.10.1 Subnet mask (ext.): 255.255.255.0

Interface routing external/internal: Routing mode

IP address (int.): 192.168.9.1 Subnet mask (int.): 255.255.255.0

VPN with Certificates

3. Creating a project and security module

- Use the “Insert” > “Module” menu command with the following parameters
 - Product type: SOFTNET configuration
 - Module: SOFTNET Security Client
 - Firmware release: V4
- Confirm with “OK”

Selection of a module or software configuration

Product type

- ☐ SCALANCE S
- ☒ SOFTNET configuration
(SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

- ☒ SOFTNET Security Client
- ☐ SCALANCE M87x/MD74x
- ☐ NCP VPN client for Android
- ☐ VPN device

Firmware release

- ☒ V4
- ☐ V3
- ☐ 2005
- ☐ 2008

Configuration

Name of the module:

MAC address:

IP address (ext.): Subnet mask (ext.):

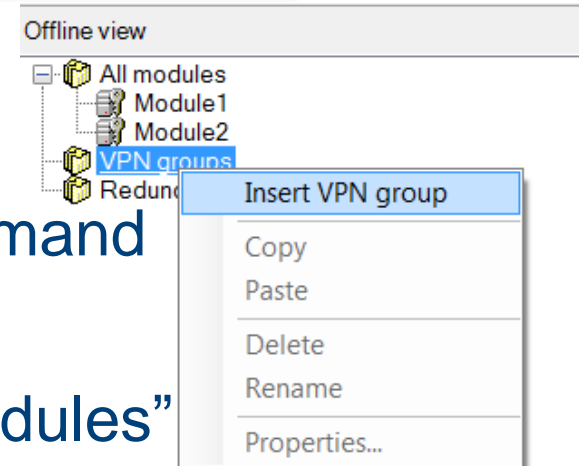
Interface routing external/internal:

IP address (int.): Subnet mask (int.):

VPN with Certificates

4. Configuring a VPN group

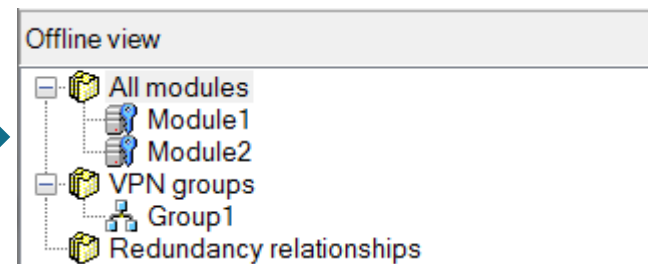
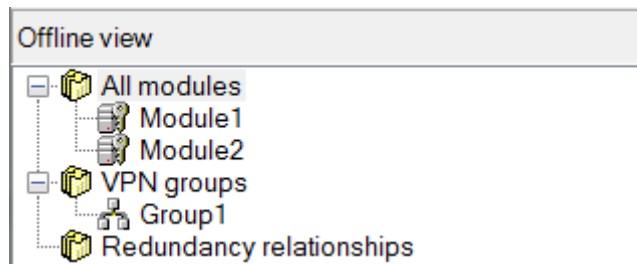
- Select “VPN groups” in the navigation
- Select the “Insert” > “Group” menu command
- In the navigation panel, click the “All modules” entry
- Drag the Scalance S Module to the VPN group “Group1” in the navigation panel
The module is now assigned to the VPN group
The color of the key symbol changes to blue



VPN with Certificates

4. Configuring a VPN group

- Drag the SOFTNET Security Client module to the VPN group “Group1” in the navigation panel
The module is now assigned to the VPN group
The color of the key symbol changes to blue

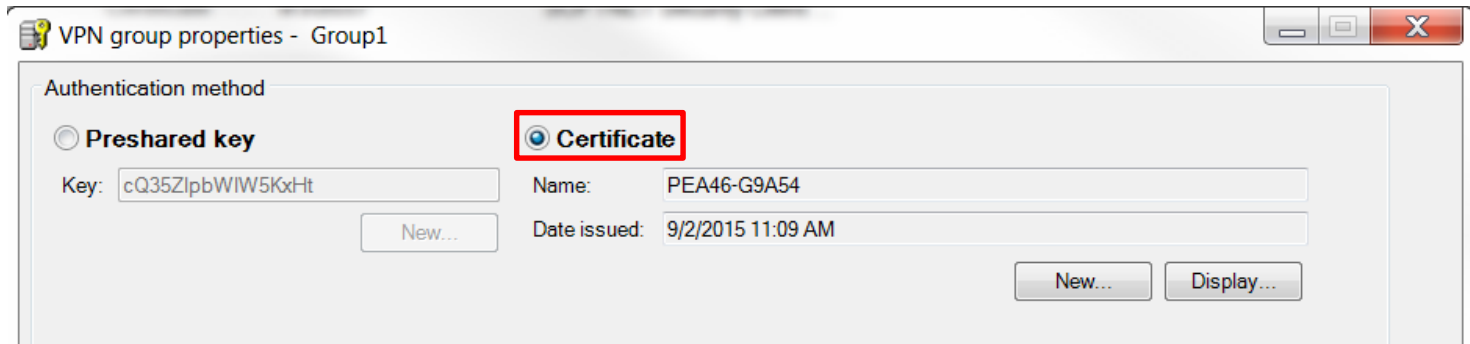


- Activate “Advanced Mode”

VPN with Certificates

4. Configuring a VPN group

- Select the VPN group “Group1” in the Navigation windows and select the menu command “Edit” > “Properties”
- Select the “Certificate” option in the “Authentication method” area

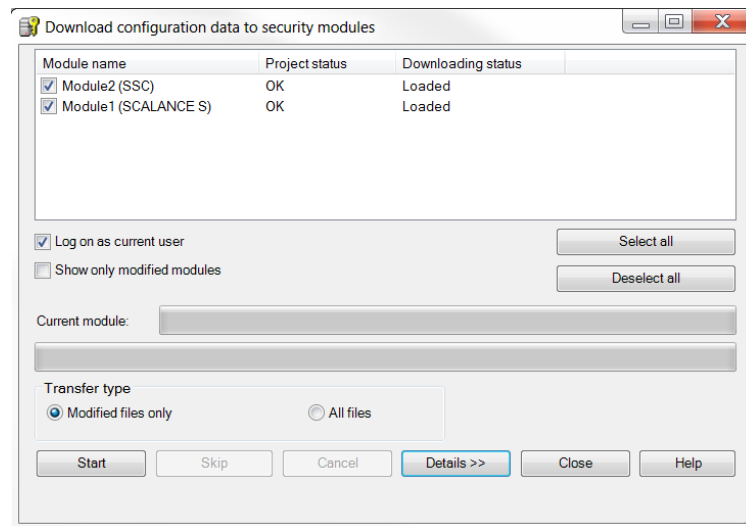


- Confirm with “OK”

VPN with Certificates

5. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the project
- Use the menu command “Transfer” > “To all modules...”



- Start the download with the “Start” button

VPN with Certificates

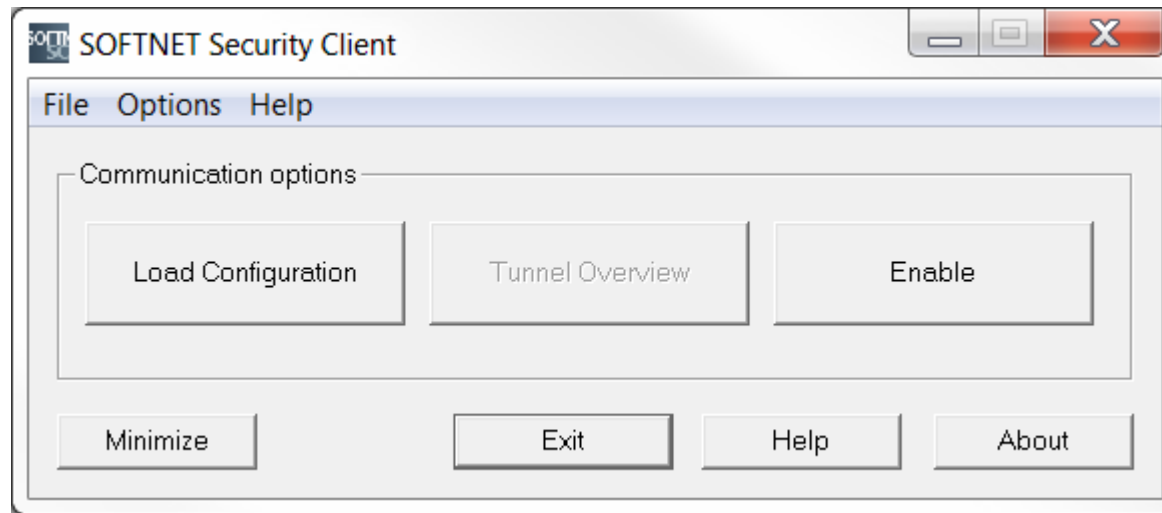
5. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the configuration file “projectname.Module2.dat” in your project folder
- Assign a password to the certificate
- Confirm the popup with “OK”

VPN with Certificates

6. Setting up a tunnel with the SOFTNET Security Client

- Open the SOFTNET Security Client on PC2

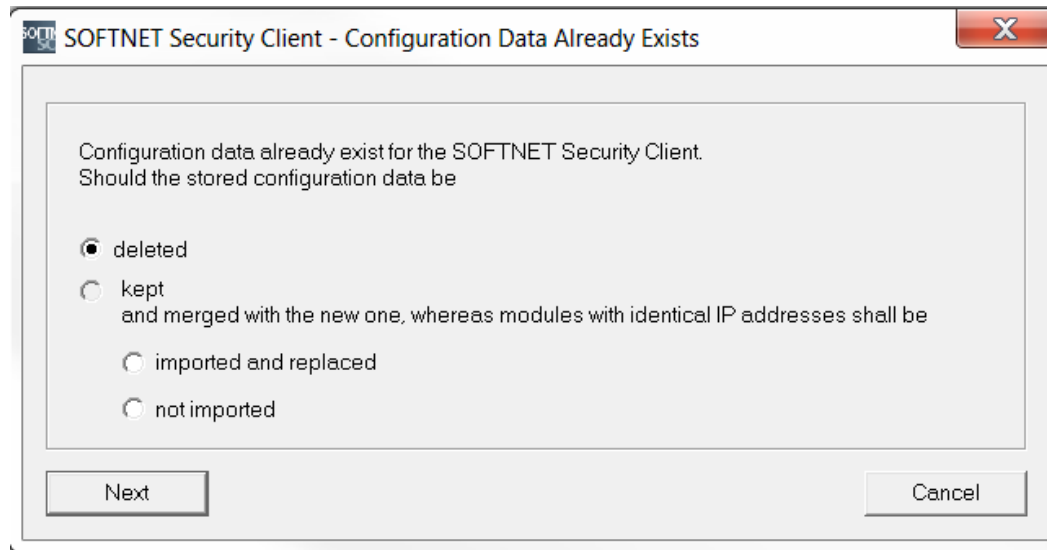


- Select “Load Configuration” and browse to where “projectname.Module2.dat” has been saved
- Open the configuration with the “Open” button

VPN with Certificates

6. Setting up a tunnel with the SOFTNET Security Client

- Loading a new configuration will delete any previous configurations

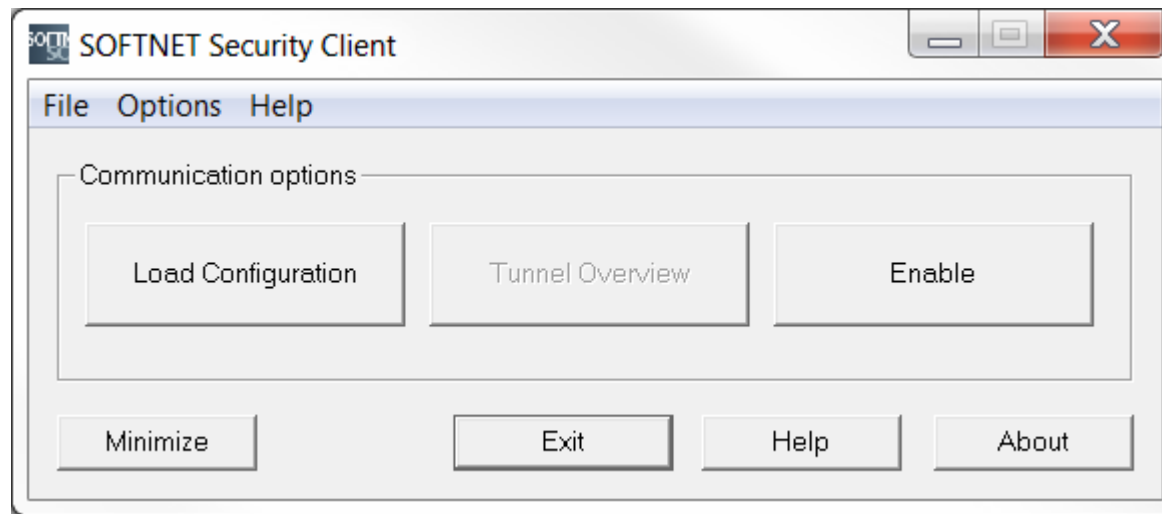


- When the dialog above pops up, select “deleted” and confirm with “Next”

VPN with Certificates

6. Setting up a tunnel with the SOFTNET Security Client

- The VPN tunnel can now be opened by clicking the “Enable” button

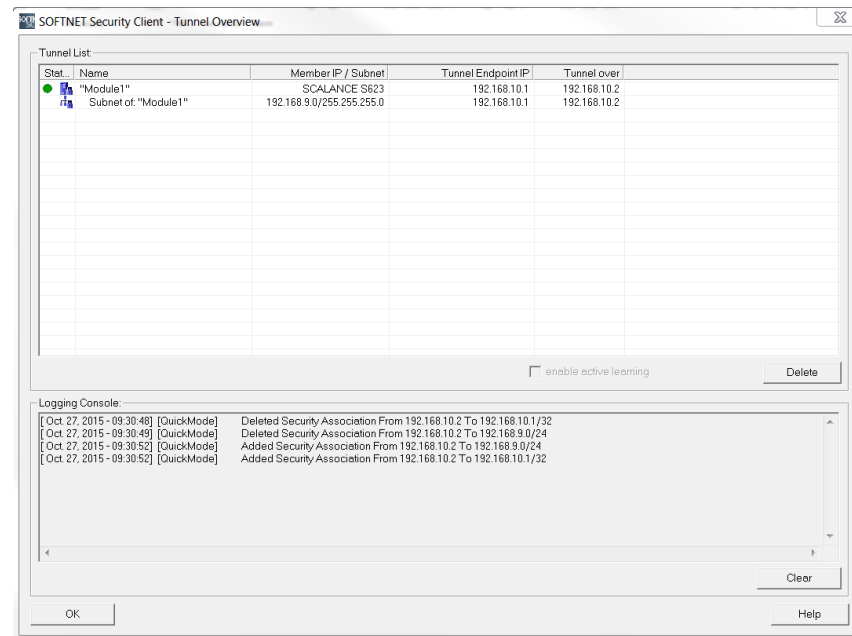


- Enter the certificate password in the dialog

VPN with Certificates

6. Setting up a tunnel with the SOFTNET Security Client

- “Tunnel Overview” shows the status of the tunnel

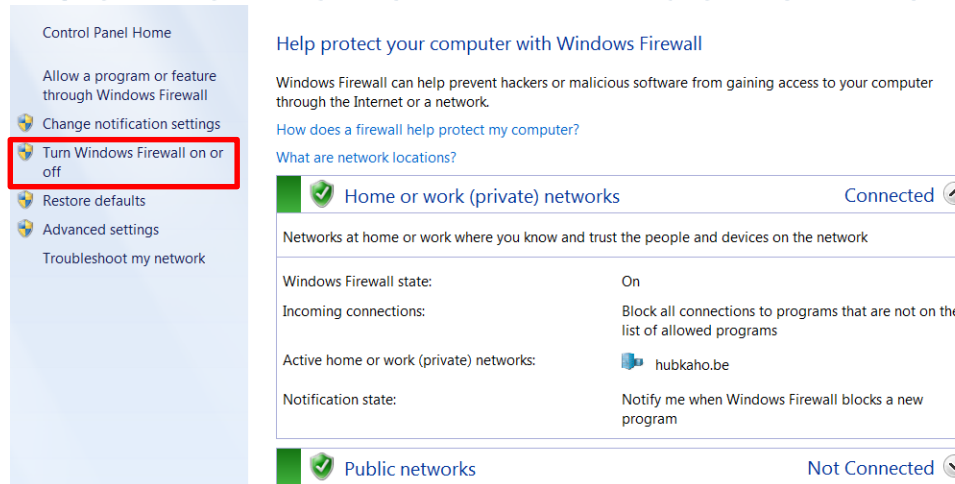


- The green circle shows that the tunnel has been established

VPN with Certificates

6. Setting up a tunnel with the SOFTNET Security Client

- If the tunnel does not get set up, check whether the Windows Firewall has been enabled
- Open the “Control Panel” > “Windows Firewall”

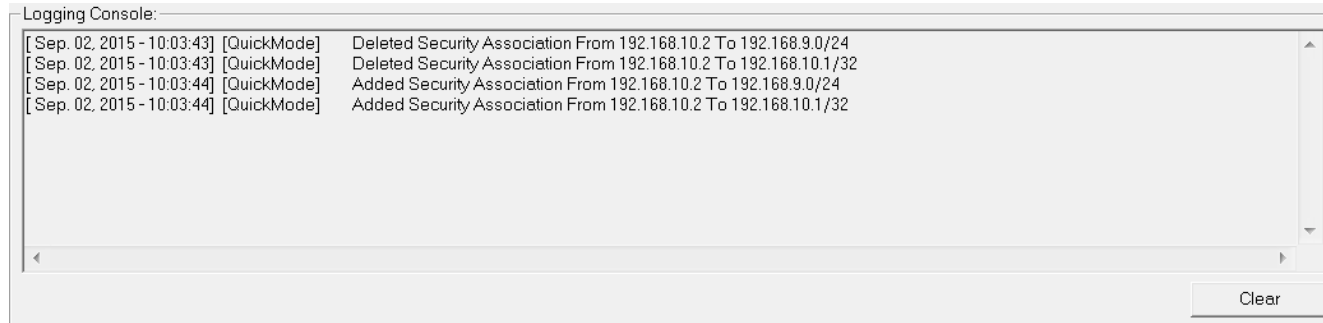


- If the firewall is not enabled, click “Turn Windows Firewall on or off” and enable it

VPN with Certificates

6. Setting up a tunnel with the SOFTNET Security Client

- In the Logging Console, the sequence of executed connection attempts is displayed

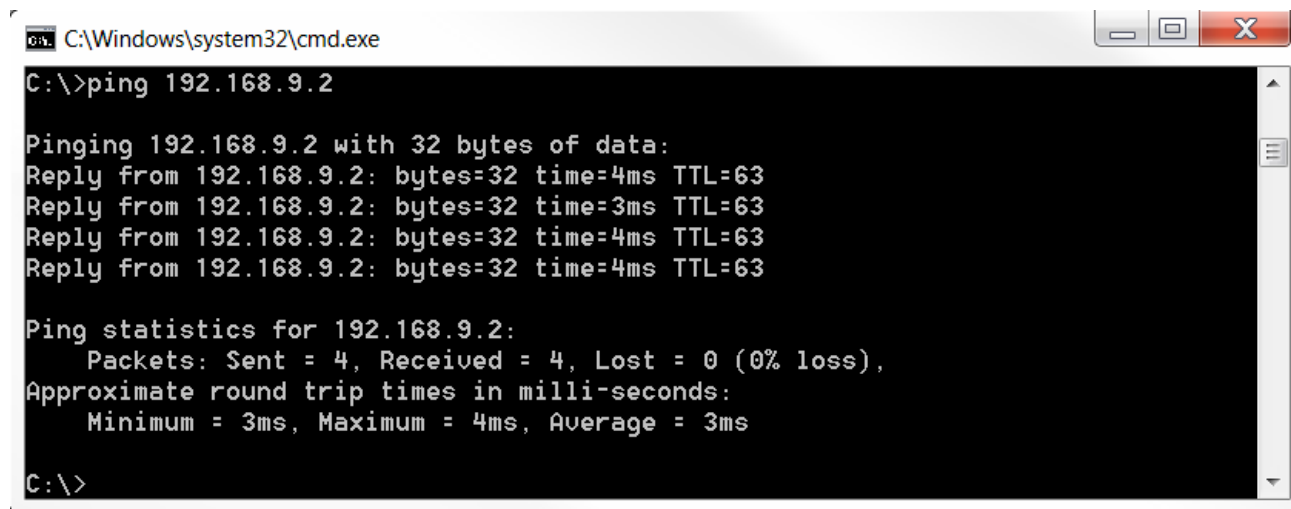


- The SCALANCE S module and the SOFTNET Security Client have established a communication tunnel

VPN with Certificates

7. Test the tunnel function

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC3
“ping 192.168.9.2”



```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.9.2

Pinging 192.168.9.2 with 32 bytes of data:
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63
Reply from 192.168.9.2: bytes=32 time=3ms TTL=63
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms

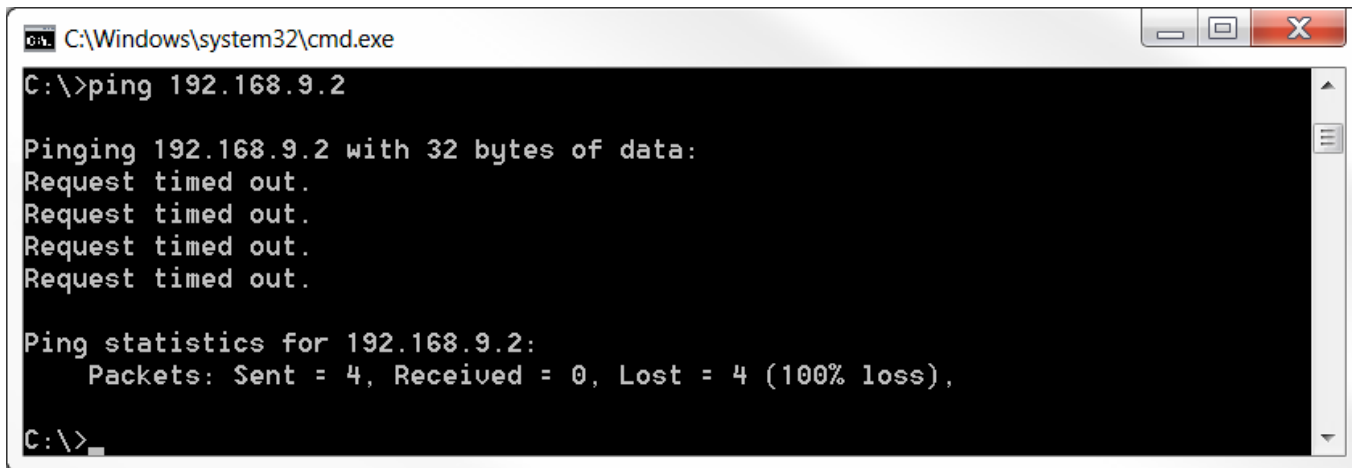
C:\>
```

- All packets reach PC3 through the tunnel

VPN with Certificates

7. Test the tunnel function

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC3
“ping 192.168.9.2”



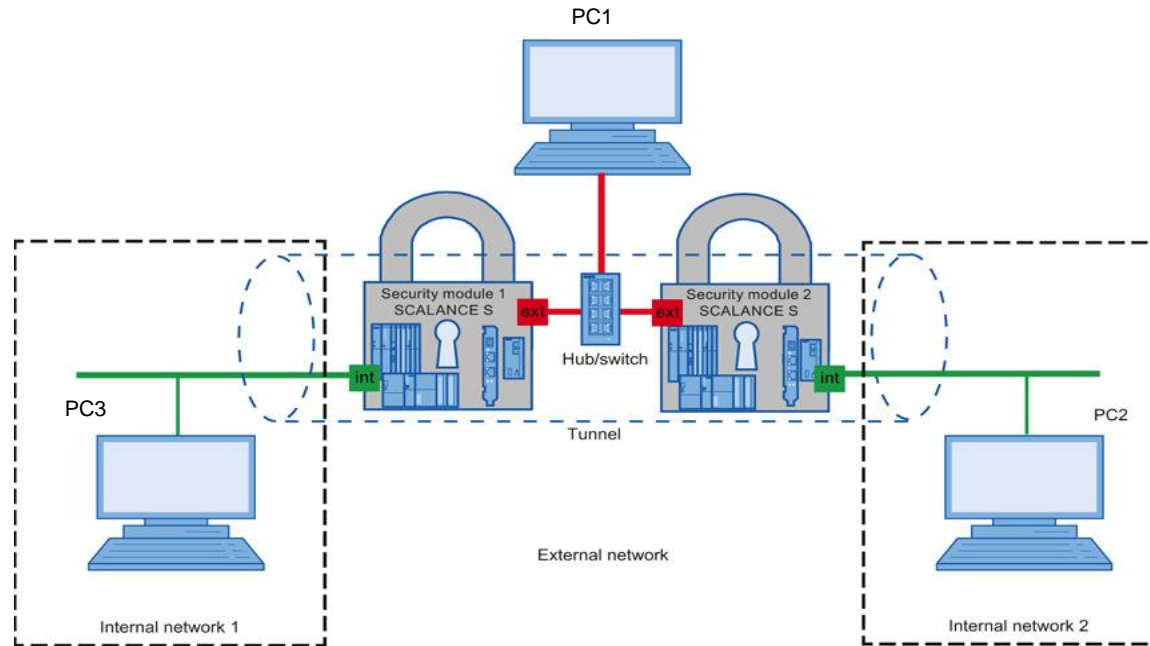
```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.9.2

Pinging 192.168.9.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

- The packets cannot reach PC3 since there is no tunnel communication between these two devices

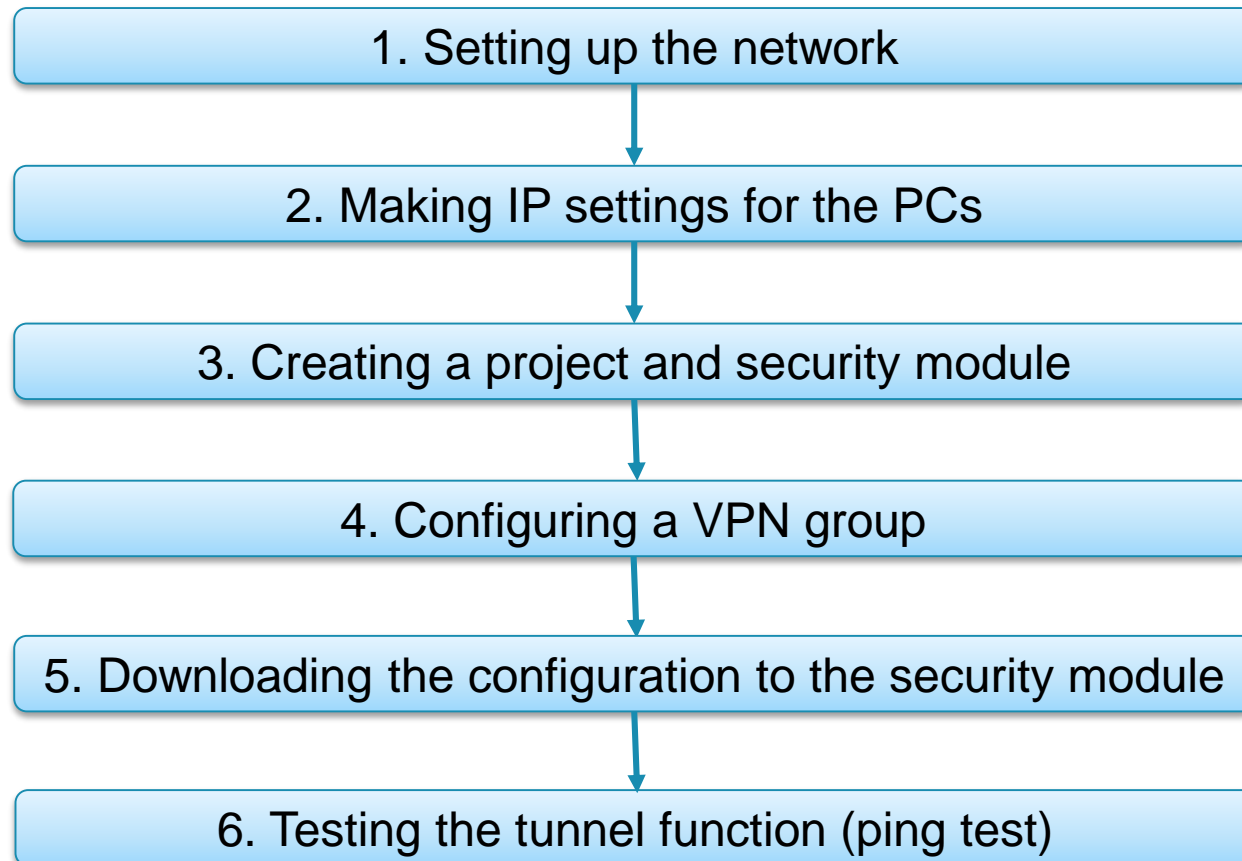
Gateway-to-Gateway with VPN



In this example, a VPN tunnel is set up between two security modules

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

Gateway-to-Gateway with VPN



Gateway-to-Gateway with VPN

1. Setting up the network

- Connect the PC with the Security Configuration Tool (PC1) to the switch
- Connect both SCALANCE S modules to the switch through their external interface
- Connect PC2 and PC3 to the internal interface of a SCALANCE S module

Gateway-to-Gateway with VPN

2. Making IP settings for the PCs

PC	IP address	Subnet mask
PC1	192.168.10.2	255.255.0.0
PC2	192.168.10.3	255.255.0.0
PC3	192.168.10.4	255.255.0.0

- Set the IP addresses of the PCs as in the table above

Gateway-to-Gateway with VPN

3. Creating a project and security module

- Create a new project
- In the “Configuration” area enter the MAC address
- Enter the external IP address (192.168.10.201) and the external subnet mask (255.255.0.0)
- Confirm with “OK”

Selection of a module or software configuration

Product type

☒ SCALANCE S

☐ SOFTNET configuration
(SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

☐ S602 ☒ S623 ☐ S627-2M

☐ S612 ☐ S613

Firmware release

☒ V4 ☐ V3

Configuration


Name of the module: Module1

MAC address: 00-1B-1B-BB-99-DE

IP address (ext.): 192.168.10.201 Subnet mask (ext.): 255.255.0.0

Interface routing external/internal: Bridge mode

IP address (int.): Subnet mask (int.):



Gateway-to-Gateway with VPN

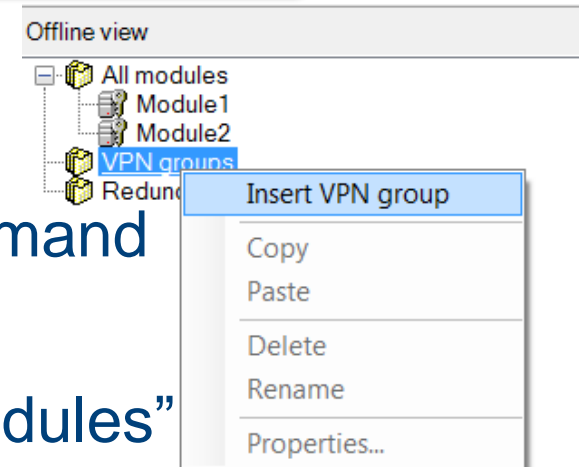
3. Creating a project and security module

- Select the menu command “Insert” > “Module”
- Select the same options as for the previous module but with the following address parameters
 - MAC address: MAC address of the module
 - IP address (ext): 192.186.10.202
 - Subnet mask (ext): 255.255.0.0
- Confirm with “OK”

Gateway-to-Gateway with VPN

4. Configuring a VPN group

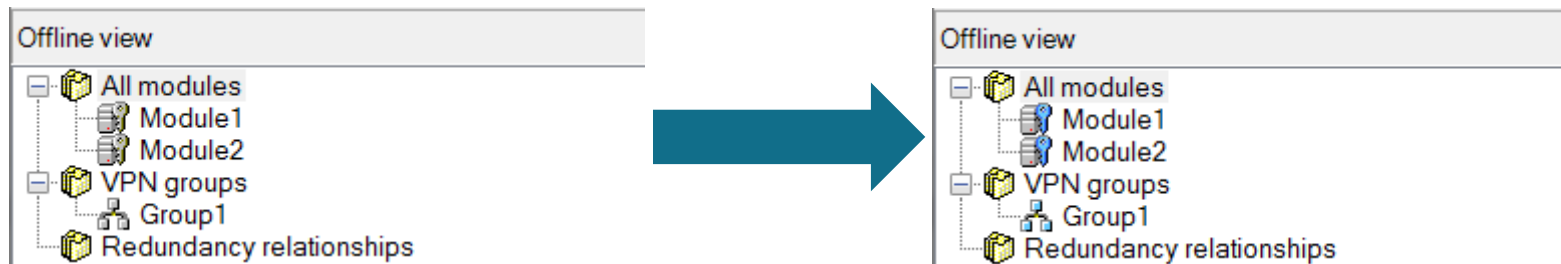
- Select “VPN groups” in the navigation
- Select the “Insert” > “Group” menu command
- In the navigation panel, click the “All modules” entry
- Drag the SCALANCE S Module to the VPN group “Group1” in the navigation panel
The module is now assigned to the VPN group
The color of the key symbol changes to blue



Gateway-to-Gateway with VPN

4. Configuring a VPN group

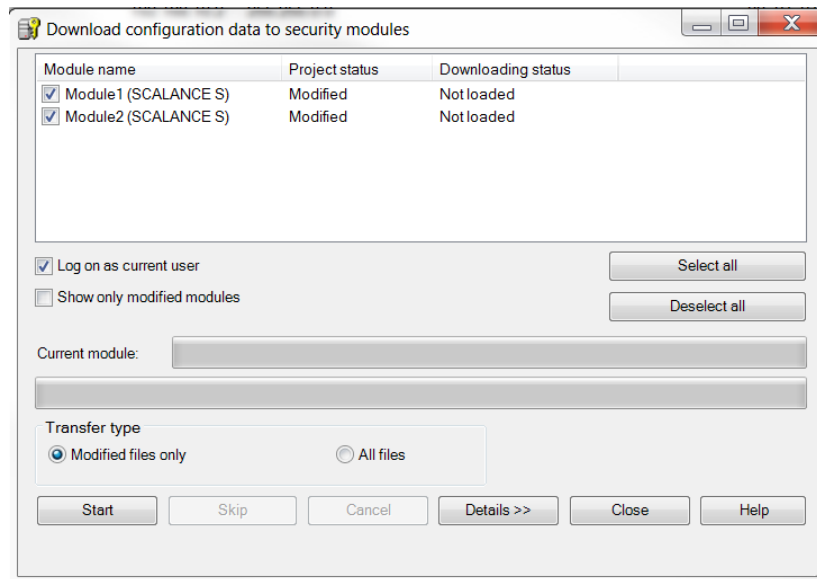
- Drag the second SCALANCE S module to the VPN group “Group1” in the navigation panel
The module is now assigned to the VPN group
The color of the key symbol changes to blue



Gateway-to-Gateway with VPN

5. Downloading the configuration to the security module

- Save the project
- Use the menu command “Transfer” > “To all modules...”

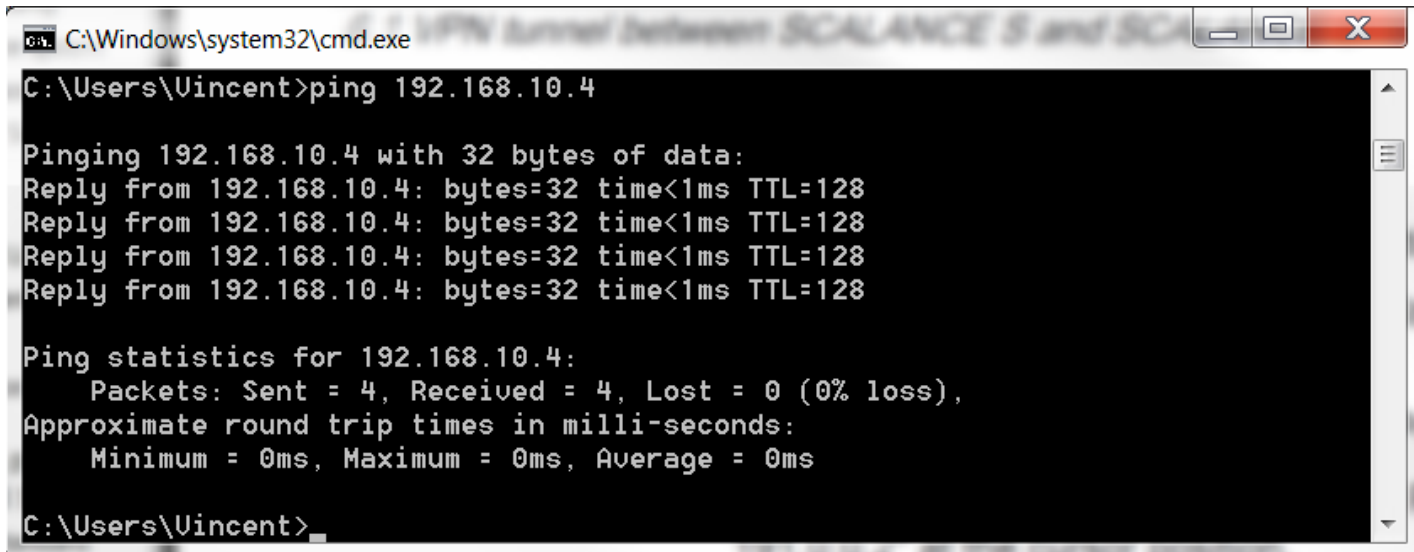


- Start the download with the “Start” button

Gateway-to-Gateway with VPN

6. Testing the tunnel function (ping test)

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC3
“ping 192.168.10.4”



```
C:\Windows\system32\cmd.exe
C:\Users\Vincent>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

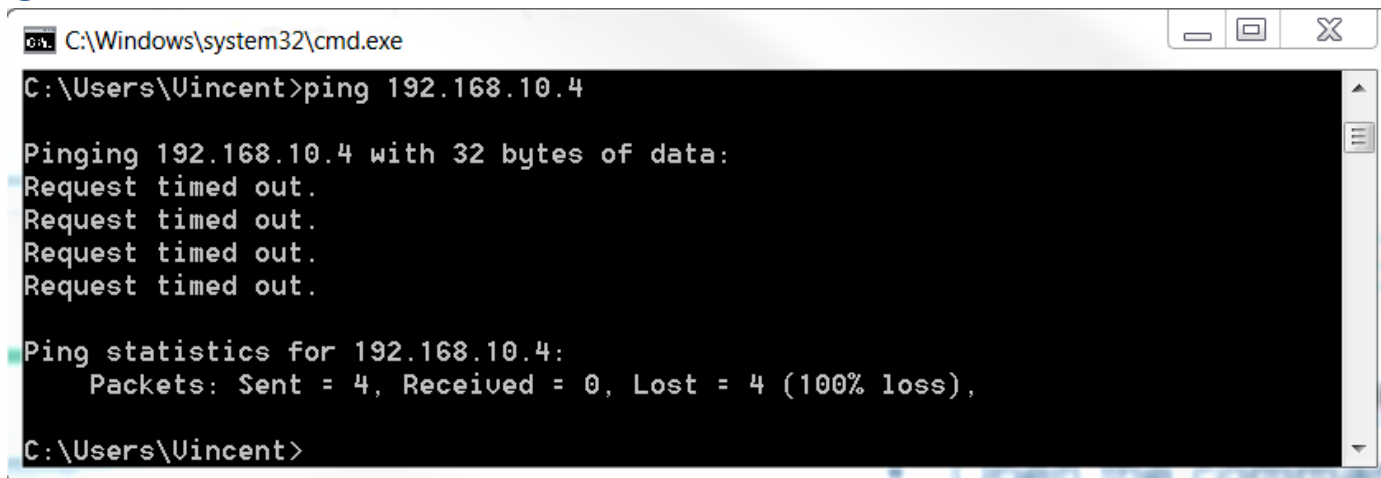
C:\Users\Vincent>
```

- All packets reach PC3 through the tunnel

Gateway-to-Gateway with VPN

6. Testing the tunnel function (ping test)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC3
“ping 192.168.10.4”



A screenshot of a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The prompt shows the user "Vincent" at "C:\Users\Vincent" entering the command "ping 192.168.10.4". The output shows four "Request timed out." messages and a summary: "Ping statistics for 192.168.10.4: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)".

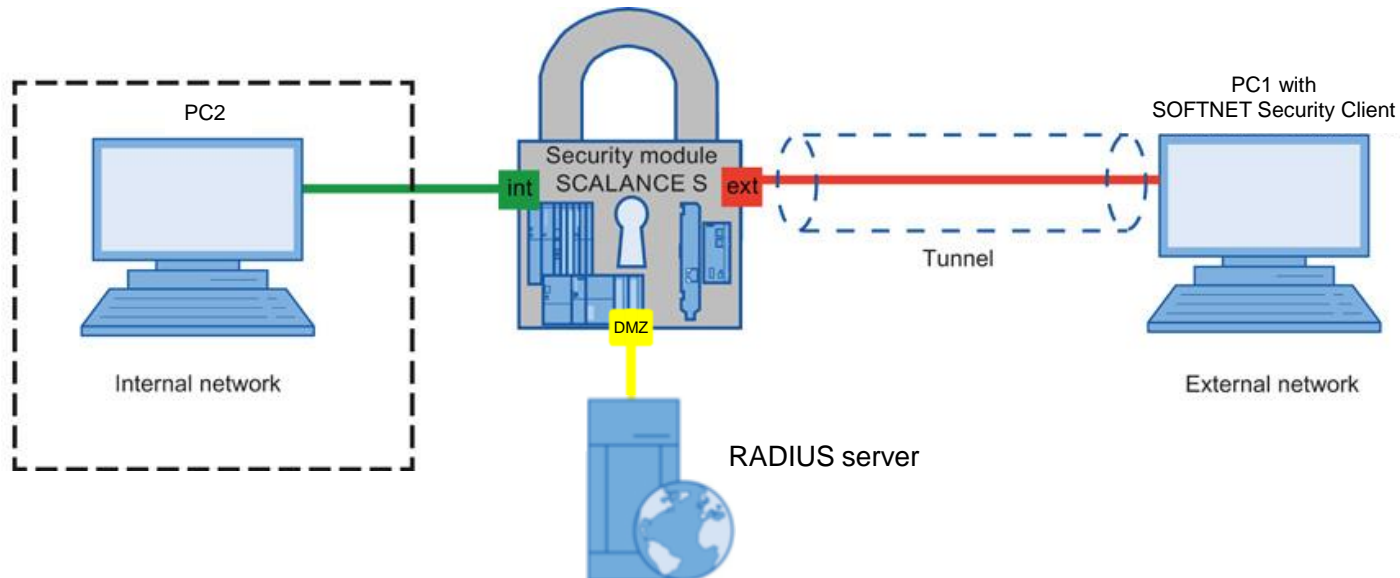
```
C:\Windows\system32\cmd.exe
C:\Users\Vincent>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Vincent>
```

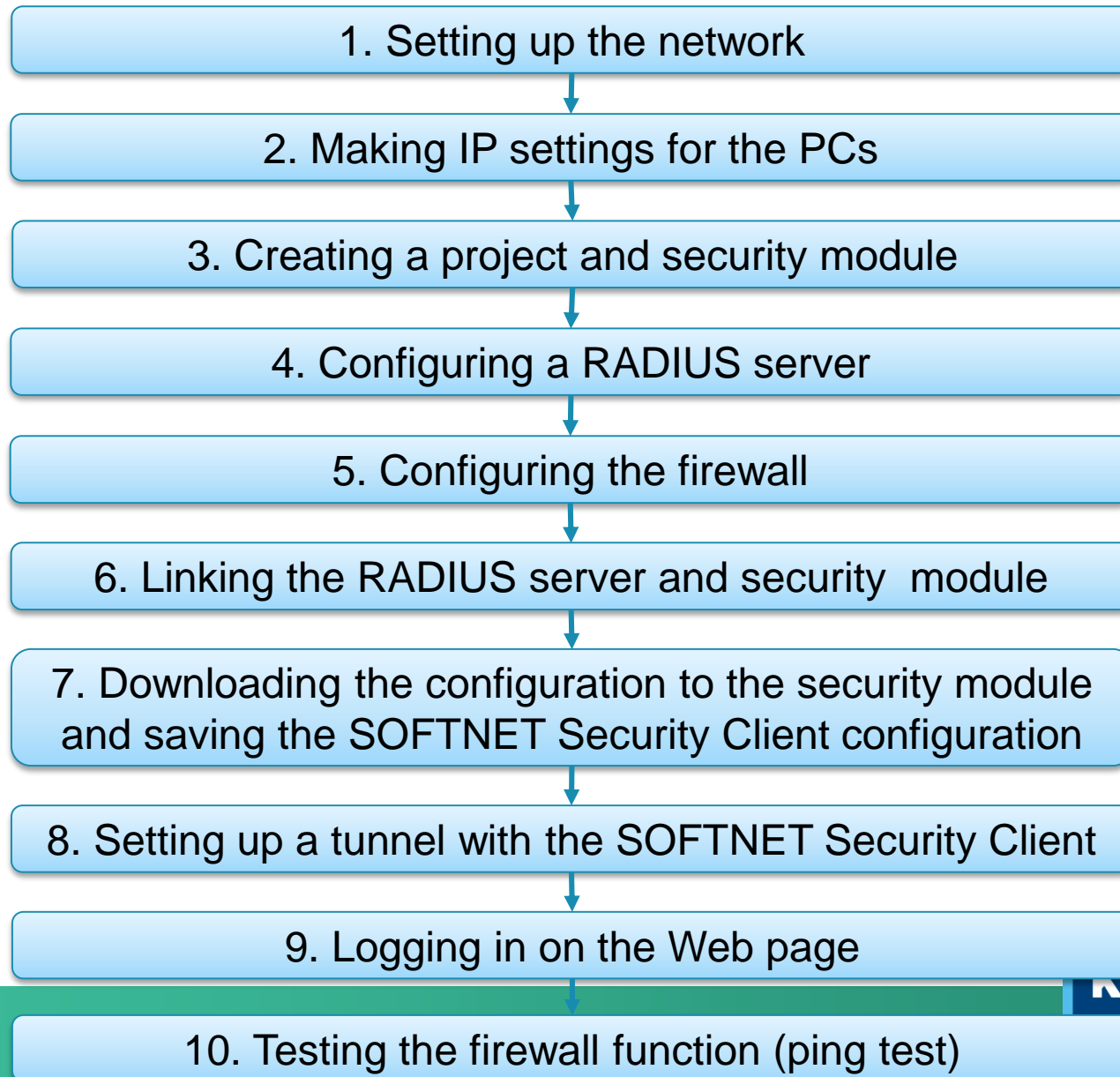
- The packets cannot reach PC3 since there is no tunnel communication between these two devices

VPN with User Authentication



In this example, a VPN tunnel is established between a PC and a security module using the SOFTNET Security Client. The firewall is configured so that the access from PC1 in the external network to PC2 in the internal network is possible for a specific user only, who needs to log in at the RADIUS server.

VPN with User Authentication



VPN with User Authentication

1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface
- Connect the Linux PC that will be used as RADIUS server to the DMZ interface

VPN with User Authentication

2. Making IP settings for the PCs

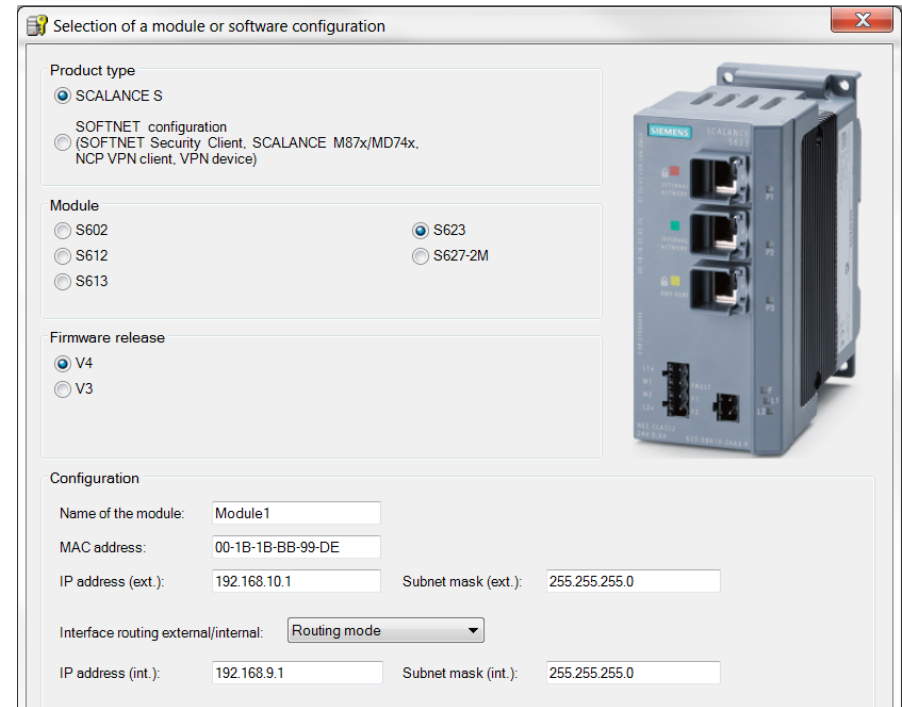
PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.9.2	255.255.255.0	192.168.9.1
RADIUS	192.168.8.2	255.255.255.0	192.168.8.1

- Set the IP addresses of the PCs as in the table above
- The IP address of the Linux PC is preset to the correct value

VPN with User Authentication

3. Creating a project and security module

- Create a new project
- In the “Configuration” area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the “Routing mode”
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with “OK”



Selection of a module or software configuration

Product type

- ☒ SCALANCE S
- ☐ SOFTNET configuration (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

- ☐ S602
- ☐ S612
- ☐ S613
- ☒ S623
- ☐ S627-2M

Firmware release

- ☒ V4
- ☐ V3

Configuration

Name of the module: Module1

MAC address: 00-1B-1B-BB-99-DE

IP address (ext.): 192.168.10.1 Subnet mask (ext.): 255.255.255.0

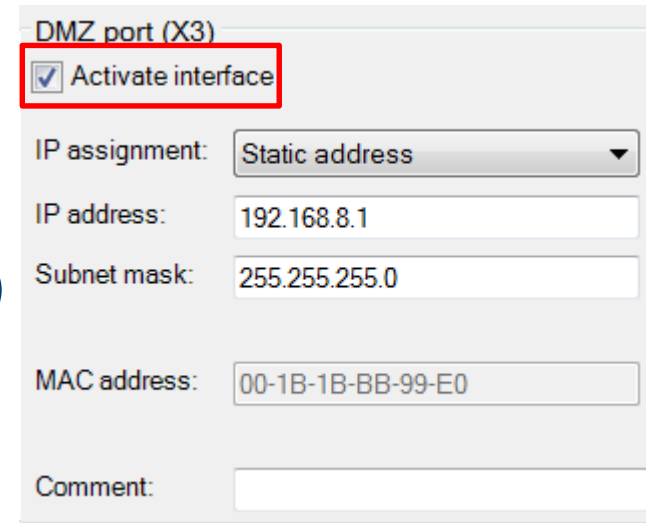
Interface routing external/internal: Routing mode

IP address (int.): 192.168.9.1 Subnet mask (int.): 255.255.255.0

VPN with User Authentication

3. Creating a project and security module

- Select the security module created and select the “Edit” > “Properties” menu command, “Interfaces” tab
- Select the “Activate Interface” check box in the “DMZ port (X3)” area
- Enter the IP address (192.168.8.1) and the subnet mask (255.255.255.0) for the DMZ interface
- Confirm with “OK”



DMZ port (X3)

☒ Activate interface

IP assignment: Static address

IP address: 192.168.8.1

Subnet mask: 255.255.255.0

MAC address: 00-1B-1B-BB-99-E0

Comment:

VPN with User Authentication

3. Creating a project and security module

- Use the “Insert” > “Module” menu command with the following parameters
 - Product type: SOFTNET configuration
 - Module: SOFTNET Security Client
 - Firmware release: V4
- Confirm with “OK”

Selection of a module or software configuration

Product type

- ☐ SCALANCE S
- ☒ SOFTNET configuration
(SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

- ☒ SOFTNET Security Client
- ☐ SCALANCE M87x/MD74x
- ☐ NCP VPN client for Android
- ☐ VPN device

Firmware release

- ☒ V4
- ☐ V3
- ☐ 2008
- ☐ 2005

Configuration

Name of the module:

MAC address:

IP address (ext.): Subnet mask (ext.):

Interface routing external/internal:

IP address (int.): Subnet mask (int.):

VPN with User Authentication

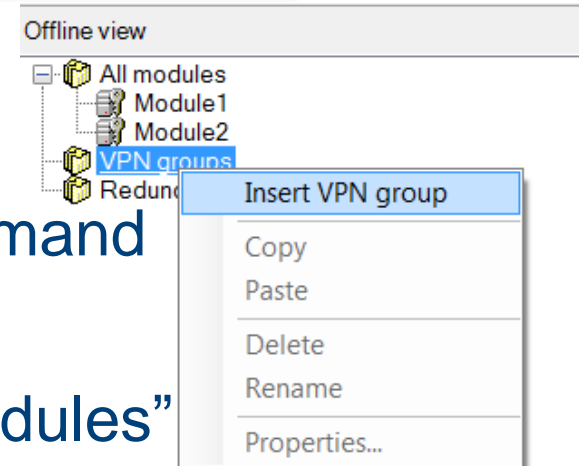
4. Configuring a RADIUS server

- We'll use the previously configured RADIUS server for this example

VPN with User Authentication

5. Configuring the firewall

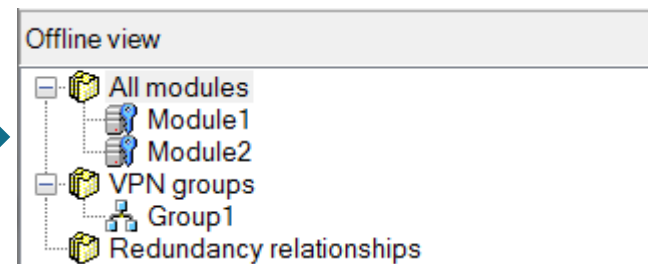
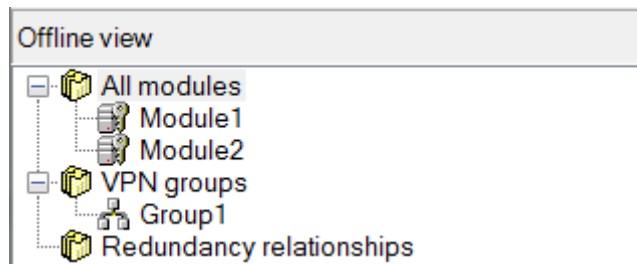
- Select “VPN groups” in the navigation
- Select the “Insert” > “Group” menu command
- In the navigation panel, click the “All modules” entry
- Drag the SCALANCE S Module to the VPN group “Group1” in the navigation panel
The module is now assigned to the VPN group
The color of the key symbol changes to blue



VPN with User Authentication

5. Configuring the firewall

- Drag the SOFTNET Security Client module to the VPN group “Group1” in the navigation panel
The module is now assigned to the VPN group
The color of the key symbol changes to blue



- Activate “Advanced Mode”

VPN with User Authentication

5. Configuring the firewall

- Use the menu command “Options” > “User Management”
- Create a new user with the following settings
- Confirm with “OK”

Edit users

User data

User name: radius

Authentication method: RADIUS

Password:

Repeat password:

Comment:

Settings for user-specific IP rule sets

Maximum time of the session: 30 Minutes

Role

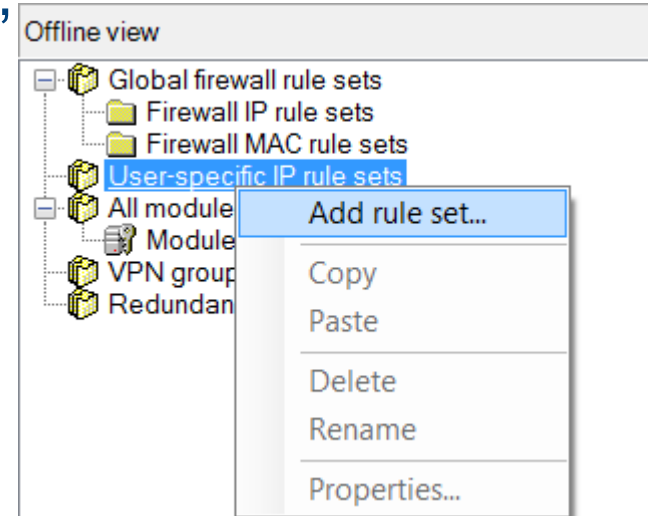
Assigned role: radius

OK Cancel Help

VPN with User Authentication

5. Configuring the firewall

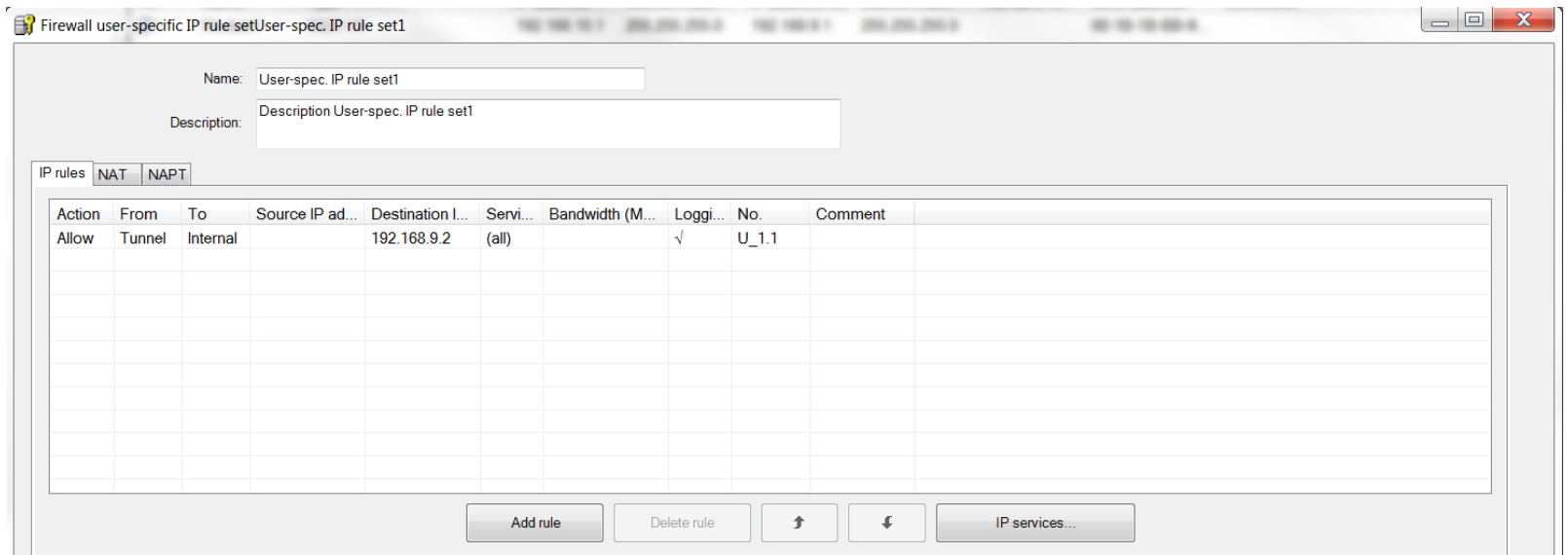
- Select the “User-specific IP rule sets” in the navigation window
- Select the “Add rule set...” option in the shortcut menu



VPN with User Authentication

5. Configuring the firewall

- Enter a rule in the dialog as shown below



VPN with User Authentication

5. Configuring the firewall

- From the “Available users and roles” list, select the “radius (user)” entry and click the “Assign” button, then select the “radius (role)” entry and click “Assign”

Available users and roles:		Assigned users and roles:
admin (User) administrator (Role) administrator(radius) (Role) diagnostics (Role) remote access (Role) standard (Role)	Assign Remove	radius (Role) radius (User)

- Confirm with “OK”

VPN with User Authentication

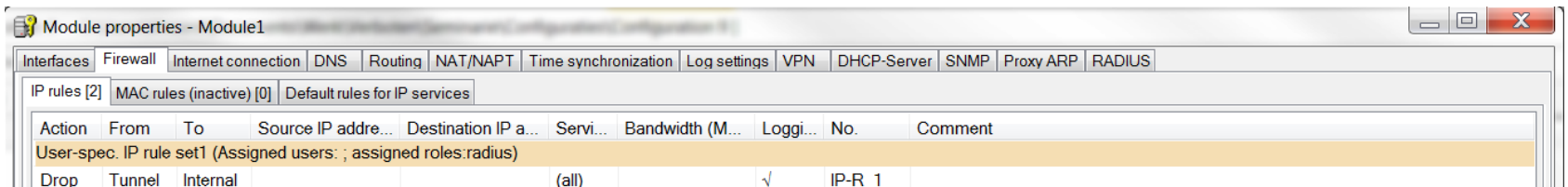
5. Configuring the firewall

- Select the security module in the navigation panel and drag it to the newly created user-specific IP rule set
- The assignment can be checked by opening the module properties and selecting the “Firewall” tab

VPN with User Authentication

5. Configuring the firewall

- Open the properties of the SCALANCE module and go to the “Firewall” tab
- Add a firewall rule as in the image

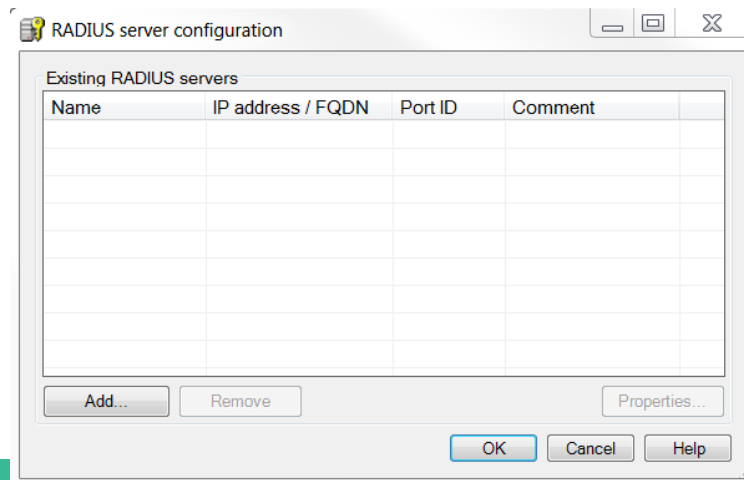
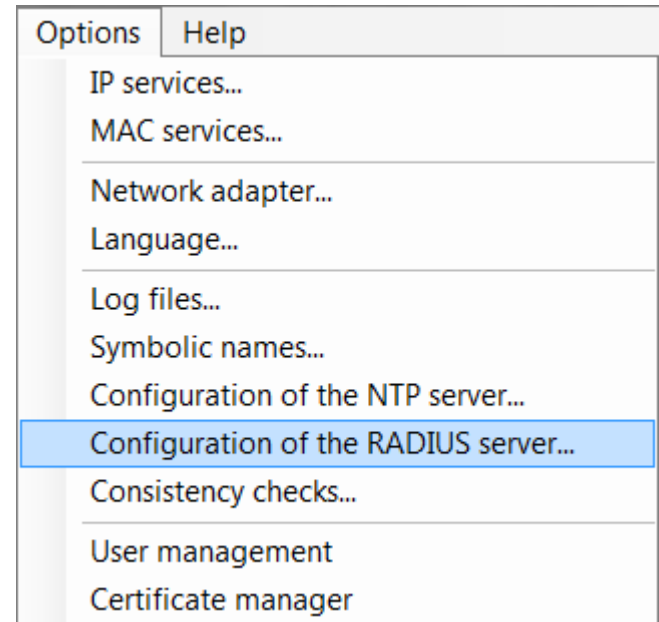


- Confirm with “OK”

VPN with User Authentication

6. Linking the RADIUS server and security module

- Select the menu option “Options” > “Configuration of the RADIUS server...”
- Click the “Add...” button in the dialog

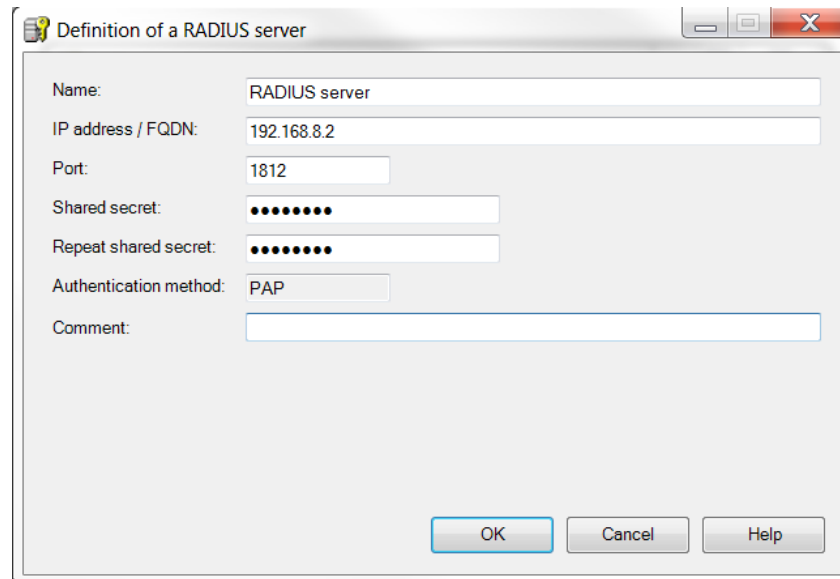


VPN with User Authentication

6. Linking the RADIUS server and security module

- Define the server with the following values
 - IP address/FQDN: 192.186.8.2
 - Shared secret: SiemensSecret
 - Repeat shared secret: SiemensSecret

- Confirm with “OK”

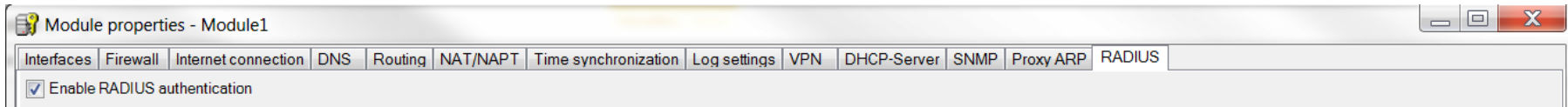


The screenshot shows a Windows-style dialog box titled "Definition of a RADIUS server". It contains several input fields and buttons. The fields are: "Name:" with the value "RADIUS server"; "IP address / FQDN:" with the value "192.168.8.2"; "Port:" with the value "1812"; "Shared secret:" with a masked value of "....."; "Repeat shared secret:" with a masked value of "....."; "Authentication method:" with the value "PAP"; and "Comment:" with an empty field. At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

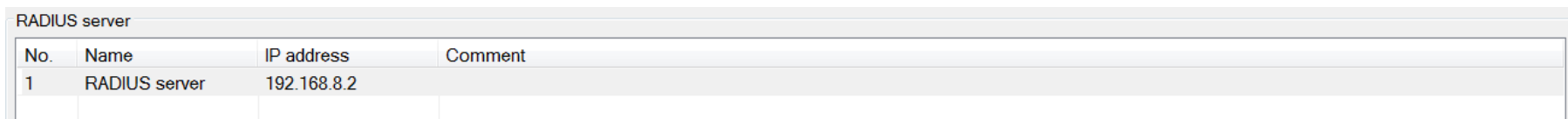
VPN with User Authentication

6. Linking the RADIUS server and security module

- Open the SCALANCE S module properties and go to the “RADIUS” tab



- Check the “Enable RADIUS authentication” box
- Click the “Add” button
This adds the newly configured RADIUS server



The screenshot shows a table titled 'RADIUS server'. The table has four columns: No., Name, IP address, and Comment. There is one row of data.

No.	Name	IP address	Comment
1	RADIUS server	192.168.8.2	

VPN with User Authentication

6. Linking the RADIUS server and security module

- In the “RADIUS setting” area, check the “Allow RADIUS authentication of non-configured users” box

RADIUS settings

RADIUS timeout: Seconds

RADIUS retries:

☒ Allow RADIUS authentication of non-configured users

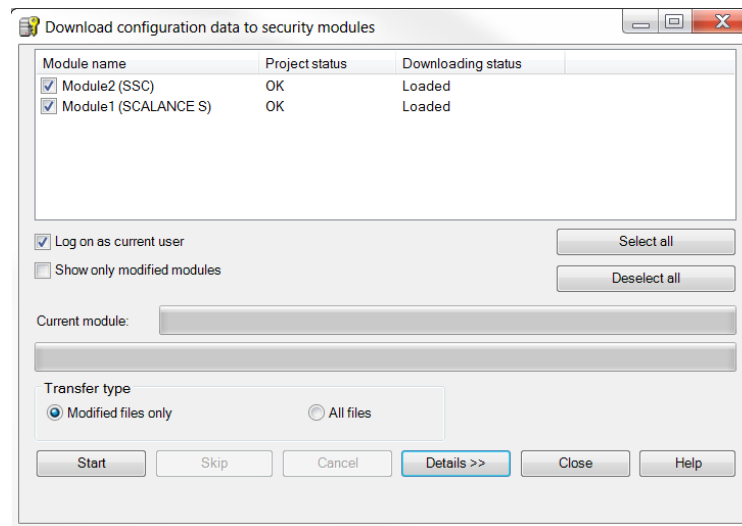
☐ Filter ID is required for authentication

- Confirm with “OK”

VPN with User Authentication

7. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the project
- Use the menu command “Transfer” > “To all modules...”



- Start the download with the “Start” button

VPN with User Authentication

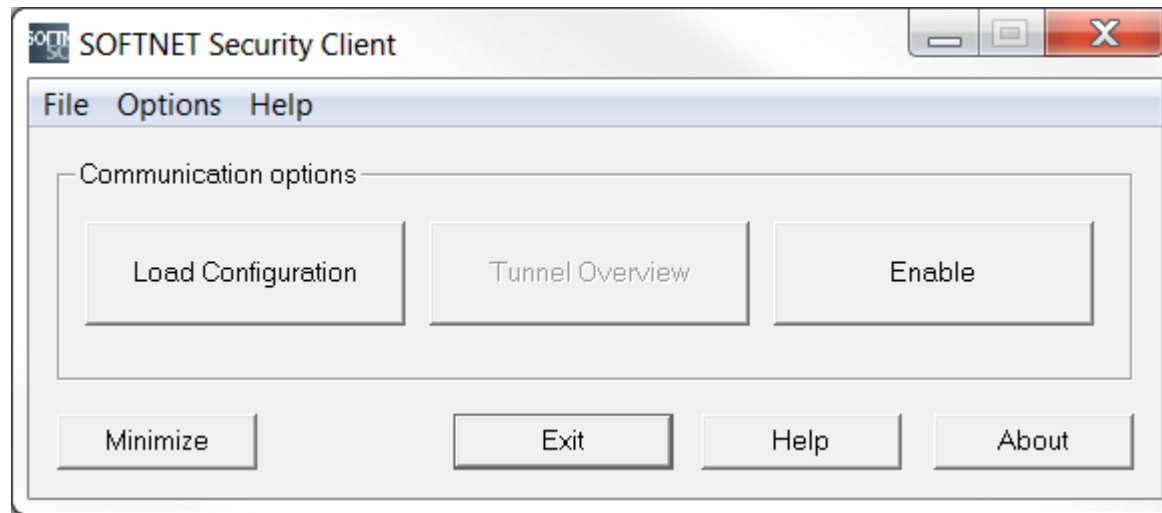
7. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the configuration file “projectname.Module2.dat” in your project folder
- Assign a password to the certificate
- Confirm the popup with “OK”

VPN with User Authentication

8. Setting up a tunnel with the SOFTNET Security Client

- Open the SOFTNET Security Client on PC2

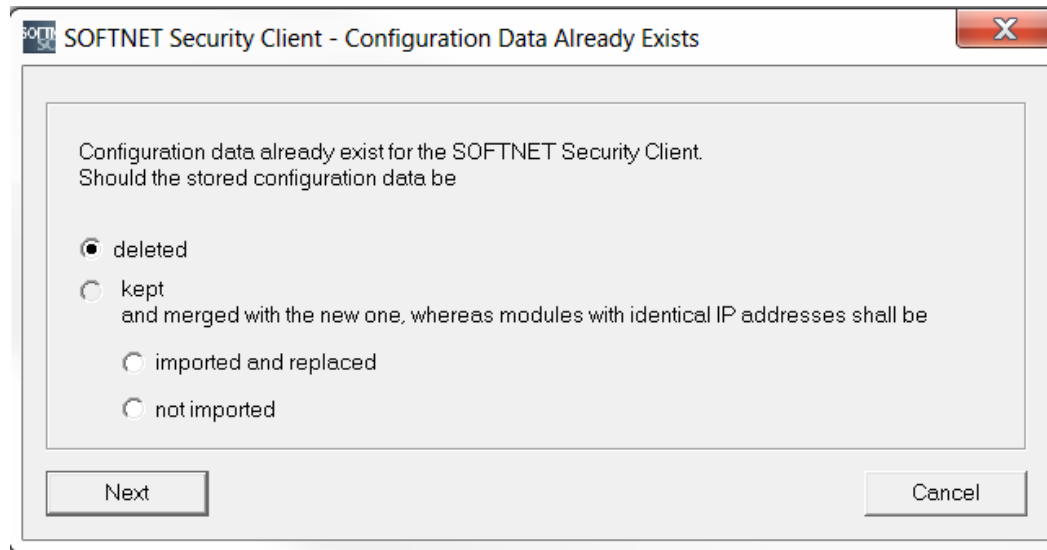


- Select “Load Configuration” and browse to where “projectname.Module2.dat” has been saved
- Open the configuration with the “Open” button

VPN with User Authentication

8. Setting up a tunnel with the SOFTNET Security Client

- Loading a new configuration will delete any previous configurations

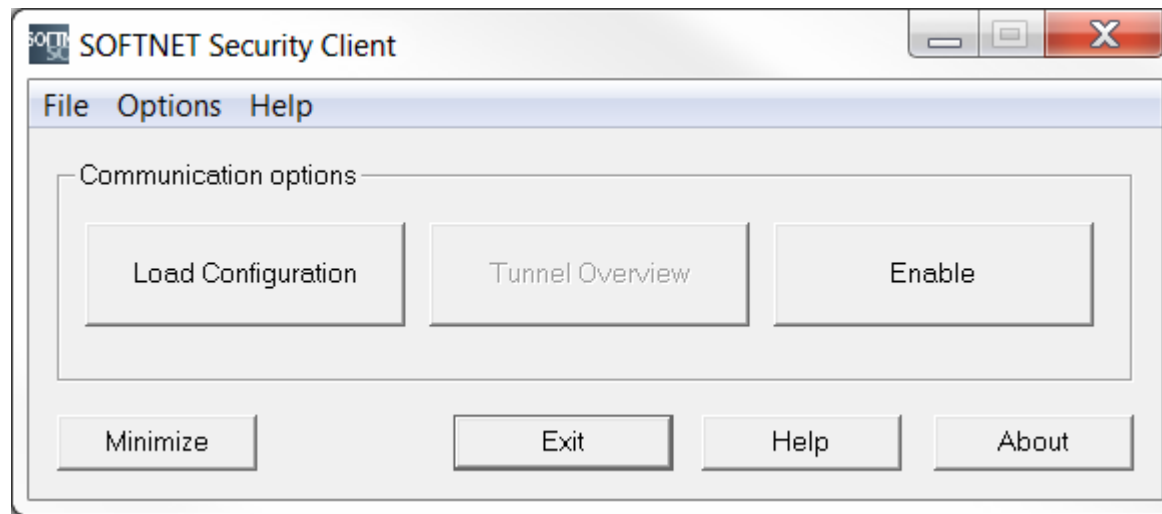


- When the dialog above pops up, select “deleted” and confirm with “Next”

VPN with User Authentication

8. Setting up a tunnel with the SOFTNET Security Client

- The VPN tunnel can now be opened by clicking the “Enable” button

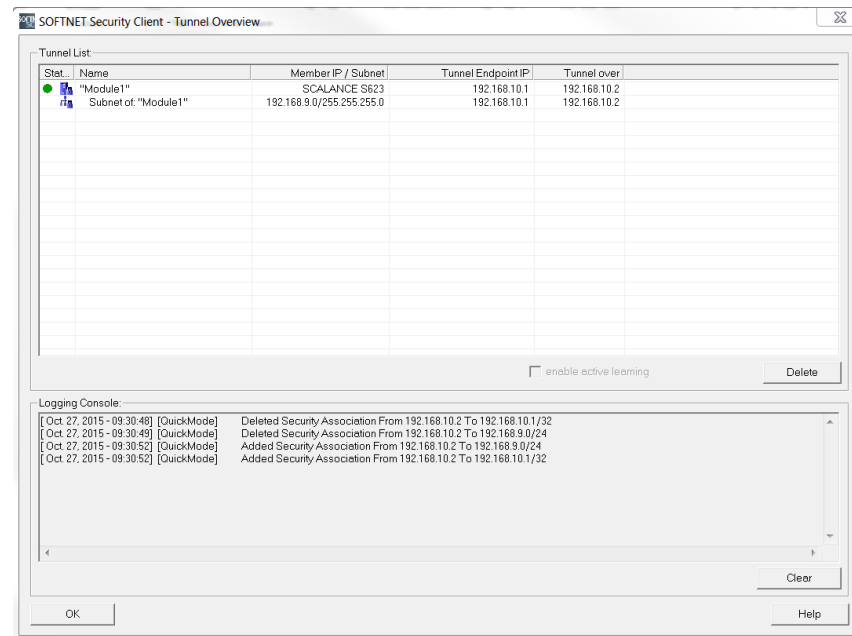


- Enter the certificate password in the dialog

VPN with User Authentication

8. Setting up a tunnel with the SOFTNET Security Client

- “Tunnel Overview” shows the status of the tunnel

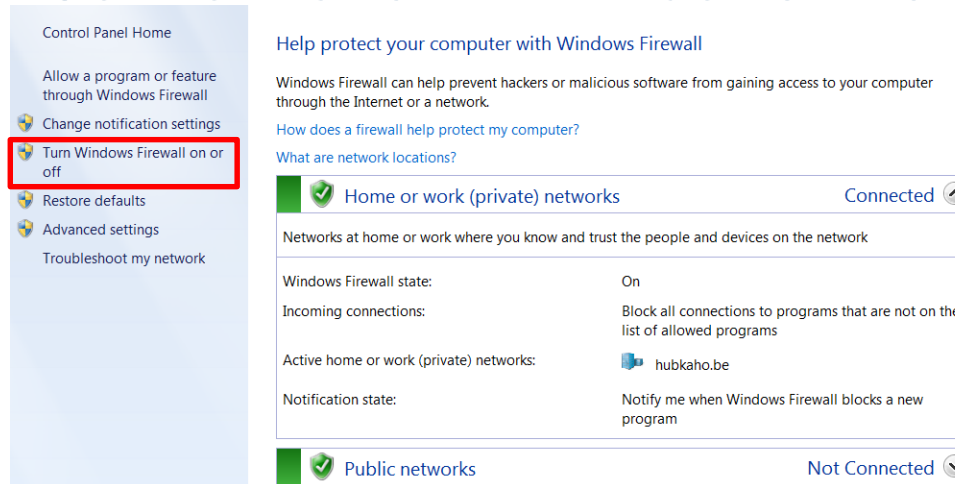


- The green circle shows that the tunnel has been established

VPN with User Authentication

6. Setting up a tunnel with the SOFTNET Security Client

- If the tunnel does not get set up, check whether the Windows Firewall has been enabled
- Open the “Control Panel” > “Windows Firewall”



- If the firewall is not enabled, click “Turn Windows Firewall on or off” and enable it

VPN with User Authentication

9. Logging in on the Web page

- In the Web browser of PC1, enter the address “https://192.168.10.1”



The screenshot shows a web browser window displaying the login page for the Siemens SCALANCE S user-specific firewall. The page has a dark blue header with the 'SIEMENS' logo on the left and a language dropdown menu set to 'English' on the right. Below the header, the page title is 'SCALANCE S'. The main content area is light blue and contains the text 'Welcome to the SCALANCE S user-specific firewall'. Below this, it says 'Please log on:'. There are two input fields: 'Name' and 'Password'. Below the 'Password' field is a 'Log in' button.

SIEMENS

English Go

SCALANCE S

Welcome to the SCALANCE S user-specific firewall

Please log on:

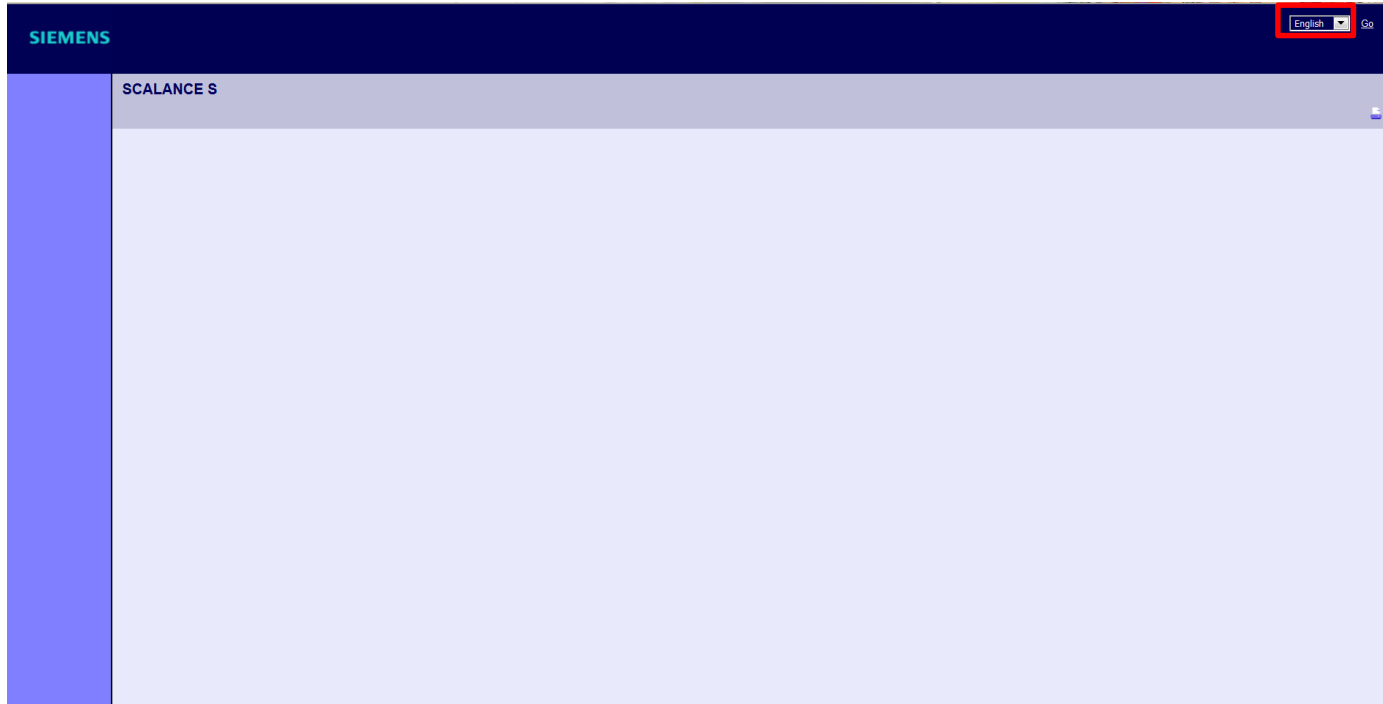
Name

Password

VPN with User Authentication

9. Logging in on the Web page

- If the web page does not show the login fields, try changing the language in the upper right corner



VPN with User Authentication

9. Logging in on the Web page

- Enter the user name “radius” and corresponding password and click the “Log in” button



The screenshot shows the login interface for the Siemens SCALANCE S user-specific firewall. The page has a dark blue header with the 'SIEMENS' logo on the left and a language dropdown set to 'English' on the right. Below the header, the page title 'SCALANCE S' is displayed. The main content area has a light blue background and contains the text 'Welcome to the SCALANCE S user-specific firewall'. Below this, it says 'Please log on:'. There are two input fields: 'Name' with the value 'radius' and 'Password' with masked characters. A 'Log in' button is positioned below the password field.

SIEMENS

English Go

SCALANCE S

Welcome to the SCALANCE S user-specific firewall

Please log on:

Name radius

Password ••••••••

Log in

VPN with User Authentication

9. Logging in on the Web page

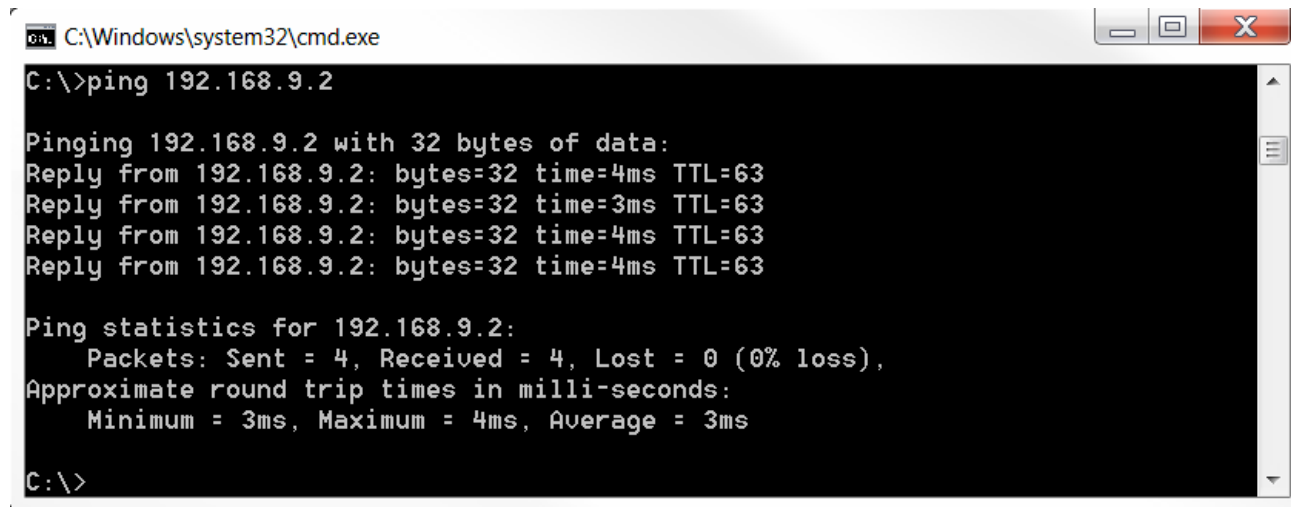
- The defined IP rule set is enabled for the “radius” user.



VPN with User Authentication

10. Testing the firewall function (ping test)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC2
“ping 192.168.9.2”



```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.9.2

Pinging 192.168.9.2 with 32 bytes of data:
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63
Reply from 192.168.9.2: bytes=32 time=3ms TTL=63
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63
Reply from 192.168.9.2: bytes=32 time=4ms TTL=63

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\>
```

- All packets reach PC2 through the tunnel