VPN tunnel via Internet

SCALANCE S61x and SOFTNET Security Client Edition 2008

FAQ • August 2010

Service & Support

Answers for industry.

SIEMENS

Question

How do I configure a VPN tunnel between PC station and SCALANCE S61x via the Internet with the SOFTNET Security Client 2008?

Answer

The instructions and notes listed in this document provide a detailed answer to this question.

Table of content

1 Introduction

Using the SOFTNET Security Client Edition 2008 it's possible to establish a VPN tunnel to a SCALANCE S61x module via the Internet by means of the Security Configuration Tool. Use the SCALANCE S61x in routing modus.

The below-mentioned guideline describes the configuration of the VPN tunnel.

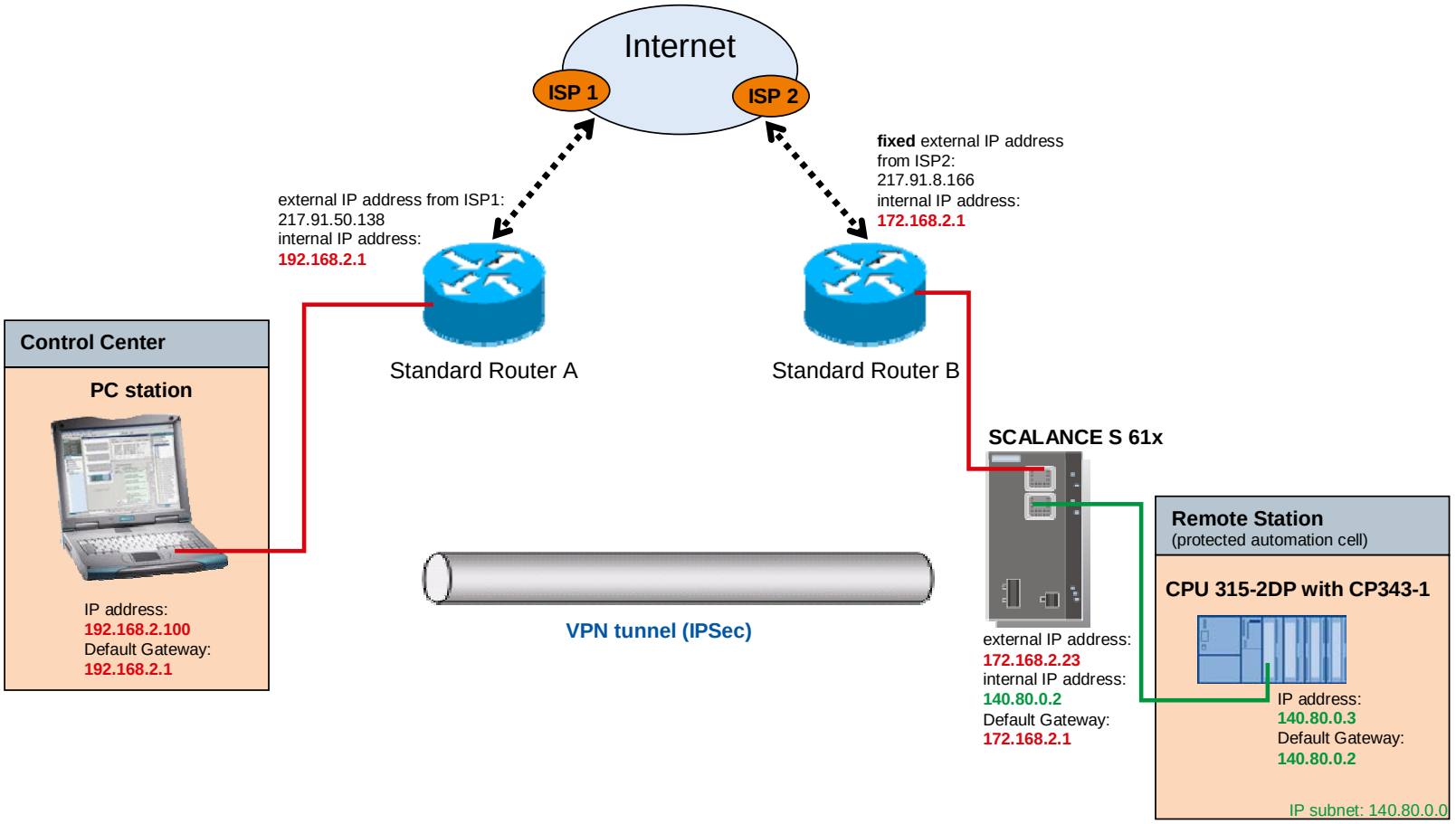
The Figure 1-1 Configuration shows the structure of this configuration.

Requirements for this are:

- In order to support the establishment of the VPN tunnel via the Internet in routing mode, you require the SCALANCE S 61x minimum with firmware V2.1. In the following entry the current Firmware V2.3 for the SCALANCE S 61x is available to download:
  http://support.automation.siemens.com/WW/view/en/37352999
- You need the following Software components:
  - SOFTNET Security Client V2.0 (Edition 2008) or higher version
  - Security Configuration Tool V2.2 or higher version

You need a fixed external IP address for the standard router B. The active module (SOFTNET Security Client) initiates the establishment of the VPN tunnel via this fixed external IP address. The passive module (SCALANCE S 61x) waits for connection from remote VPN gateway.

Figure 1-1 Configuration



Description of the configuration

The S7-300 station consists of a CPU 315-2DP and a CP343-1. It is connected to the internal network of the SCALANCE S61x. The SCALANCE S 61x secures the S7-300 station from undesirably accesses from the external network.

The SCALANCE S 61x is router or gateway for the S7-300 station.

The PC station with the IP address 192.168.2.100 is located in the external network of the SCALANCE S 61x.

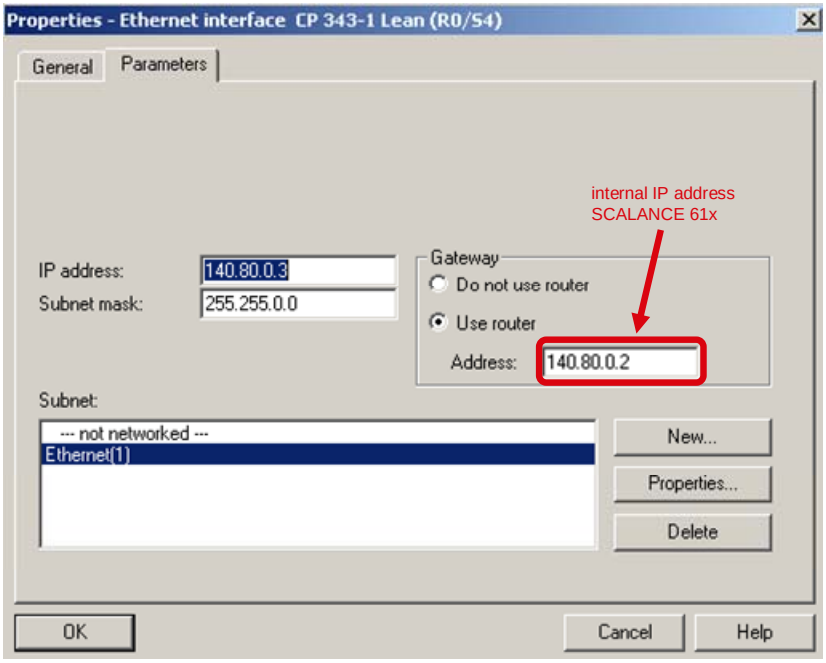
The standard router A is gateway or router and DNS server for the PC station.

The standard router B is gateway or router for the SCALANCE S 61x.

Defining the router or gateway in the S7-300 station

- Open the interface properties of the CP343-1 in the hardware configuration of the S7-300 station.
- Activate the function “Use router” and enter the internal IP address 140.80.0.2 of the SCALANCE S 61x.

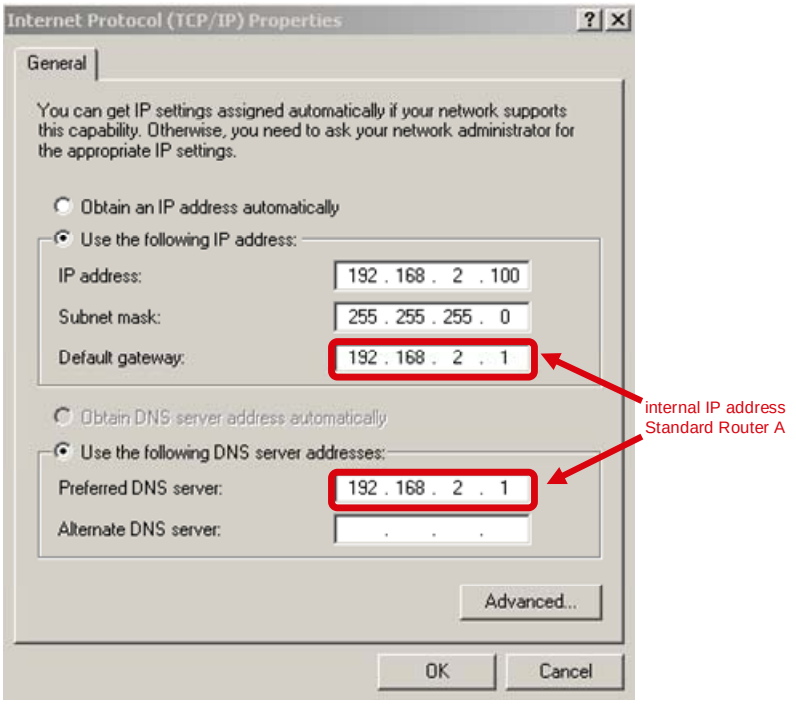
Figure 1-2 interface properties of the CP343-1



Defining the gateway in the PC station

- In Windows under Network Connection open the property dialog of the Local Area Network (LAN).
- Enter the internal IP address of the standard router A for the “Default Gateway” and DNS server.

Figure 1-3 property dialog of the LAN



NOTE If the standard router A possesses DHCP capability, the PC can automatically obtain its IP address and DNS server address from standard router A.

Following the standard router A and B are configured.

2 Configuration of the Standard Router

The standard router A is connected to the PC station where the SOFTNET Security Client is installed. The active SOFTNET Security Client initiates the establishment of the VPN tunnel via the fixed external IP address of the standard router B.

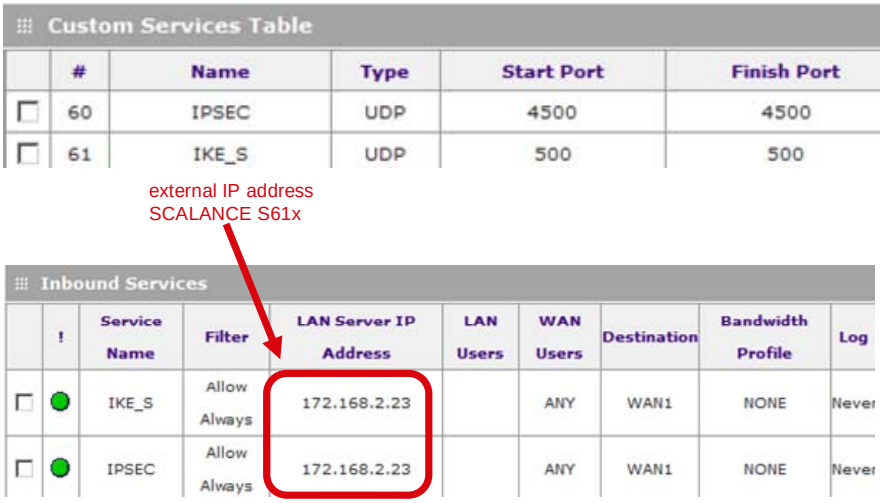
The standard router B is connected to the external network of the passive SCALANCE S 61x. The SCALANCE S 61x is passive involved in the establishment of the VPN tunnel. It waits for connection from remote VPN gateway.

Configuring the port forwarding rules in the standard router B

Configure the following port forwarding rule for the standard router which is connected to the passive component (standard router B):

- The UDP packages on the Internet, which are addressed to ports 500 and 4500 of the standard router B are forwarded to the external IP address 172.168.2.23 of the SCALANCE S 61x.

Figure 2-1 port forwarding standard router B



Using the following instruction to configure the SCALANCE S 61x and SOFTNET Security Client.

3 Configuration of the SCALANCE S 61x and SOFTNET Security Client

Starting the Security Configuration Tool

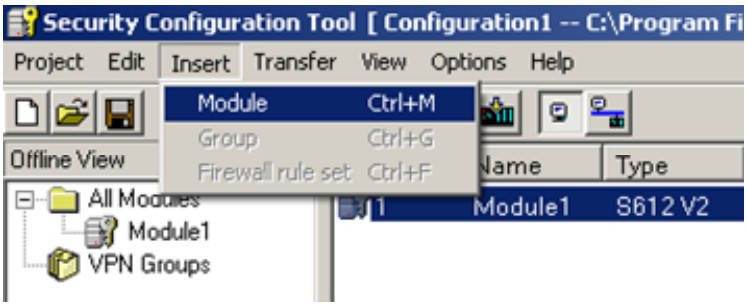
Starting the Security Configuration Tool with Start → SIMATIC → SCALANCE → Security → Security Configuration Tool and create a new project.

3.1 Configuring the SCALANCE S 61x

Inserting module

Insert a “S612 V2”-type module via the menu "Insert → Module".

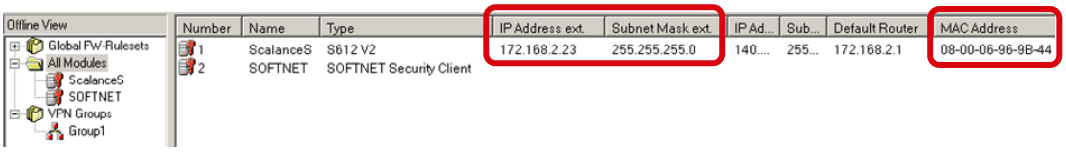
Figure 3-1 Inserting “S612 V2”-type module



Assign the external IP address and MAC address

- The external IP address 172.168.2.23 and subnet mask 255.255.255.0 is assigned to the “S612 V2”-type module.
- Enter the MAC address for the SCALANCE S 61x.

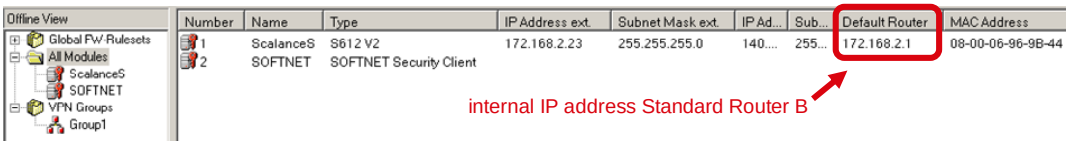
Figure 3-2 assigning the external IP address and MAC address



Enter the Default Router

Enter the internal IP address 172.168.2.1 of the standard router B for the Default Router.

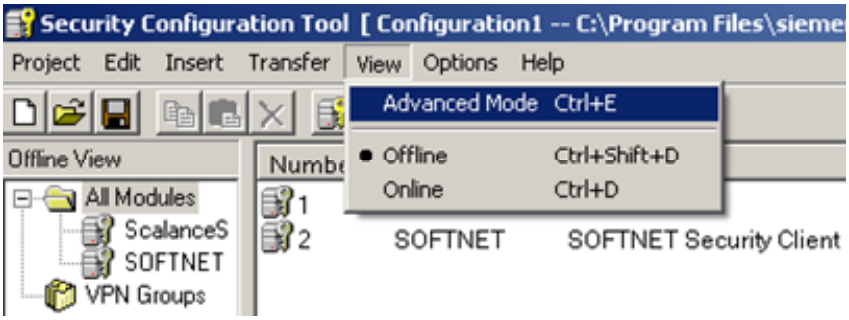
Figure 3-3 entering the default router



Enable the “Advanced Mode” and assign the internal IP address

Enable the "Advanced Mode" via the "View" menu.

Figure 3-4 enabling “Advanced Mode”



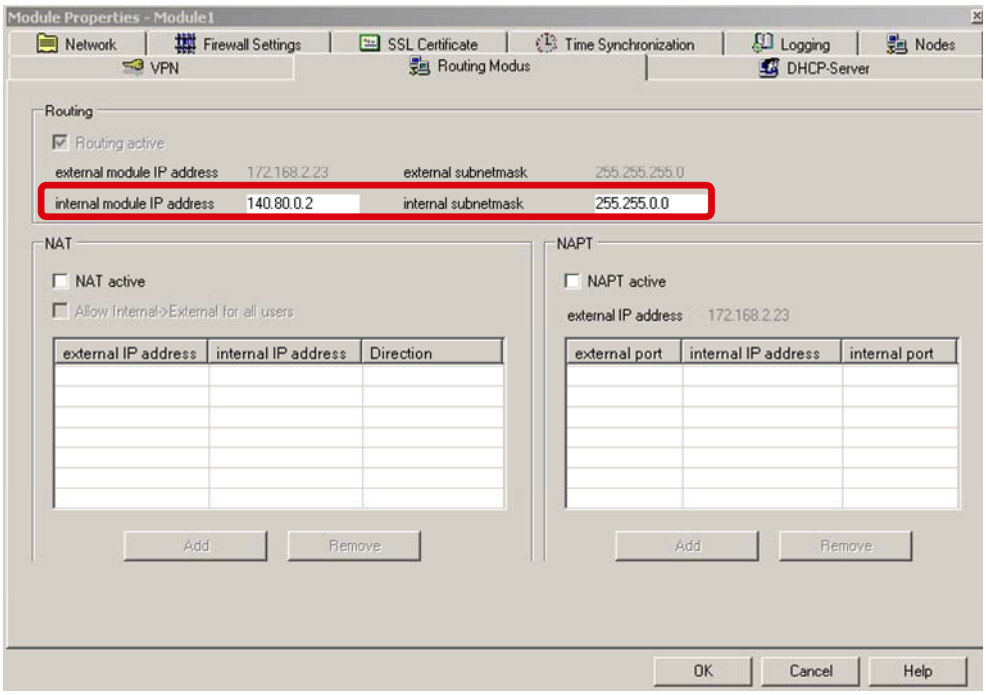
Double-click the “S612 V2”-type module under “All Modules” to open the module properties.

Change to the register “Routing Modus” in the module properties.

Enable the function “Routing active”.

Enter the internal IP address 140.80.0.2 and the subnet mask 255.255.0.0.

Figure 3-5 module properties “S612 V2” → register “Routing Modus”

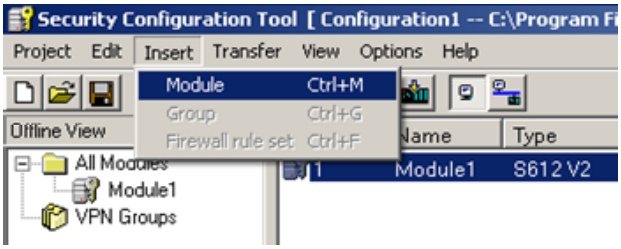


3.2 Configuring the SOFTNET Security Client

Inserting module

Insert an additional “SOFTNET Security Client”-type module via the menu "Insert → Module".

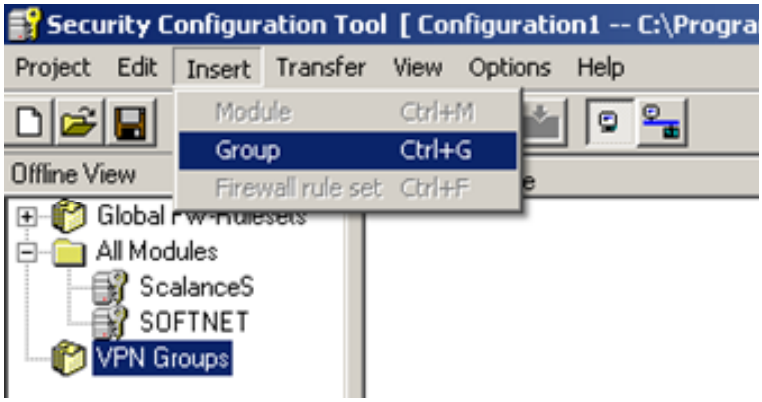
Figure 3-6 Inserting “SOFTNET Security Client”-type module



Creating group

Create a new group via the menu “Insert → Group”.

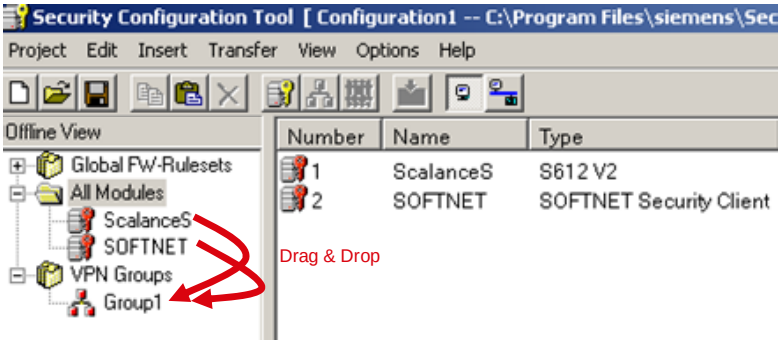
Figure 3-7 creating group



Assign the modules to the group

The “S612 V2”-type module and the “SOFTNET Security Client”-type module are assigned to the created group by means of drag & drop.

Figure 3-8 assigning the modules to the group



3.3 Configuring the Virtual Private Network (VPN)

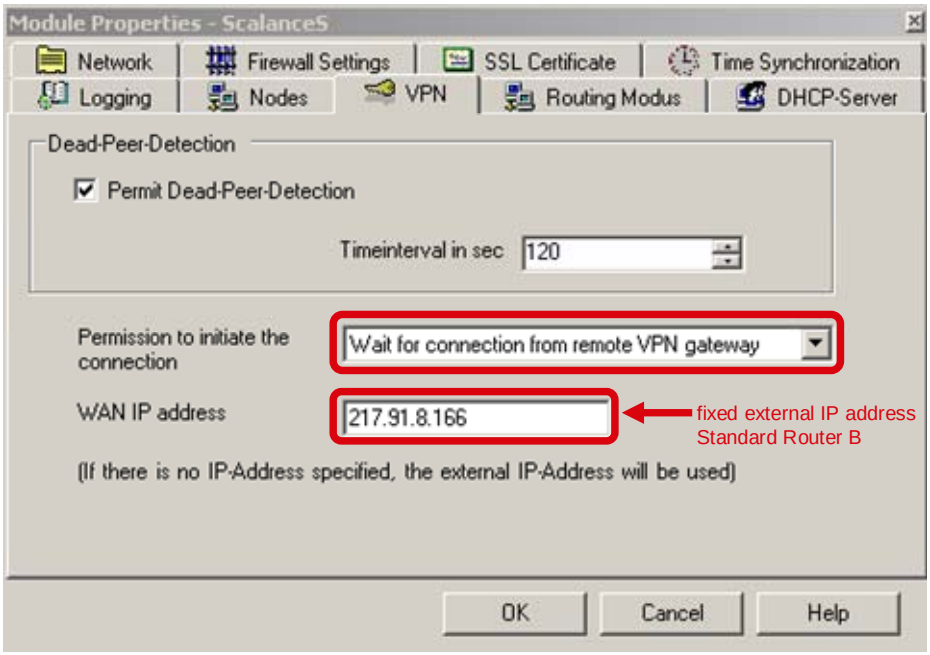
Double-click the “S612 V2”-type module under “All Modules” to open the module properties.

Change to the register “VPN” in the module properties.

Select the function “Wait for connection from remote gateway”.

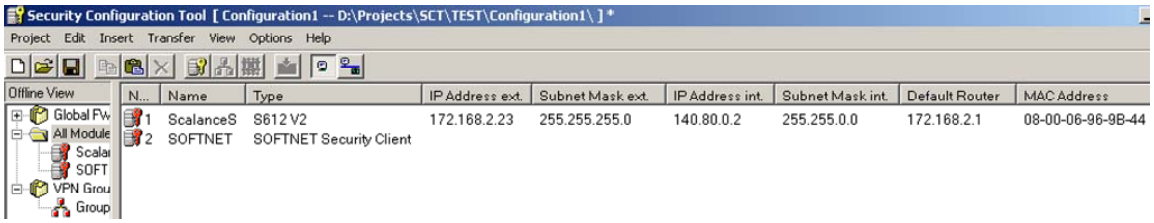
Enter the fixed external IP address 217.91.8.166 of the standard router B under “WAN IP address”.

Figure 3-9 module properties “S612 V2” → register “VPN”



Now the configuration of the SCALANCE S 61x and the SOFTNET Security Client is finished.

Figure 3-10 finished configuration

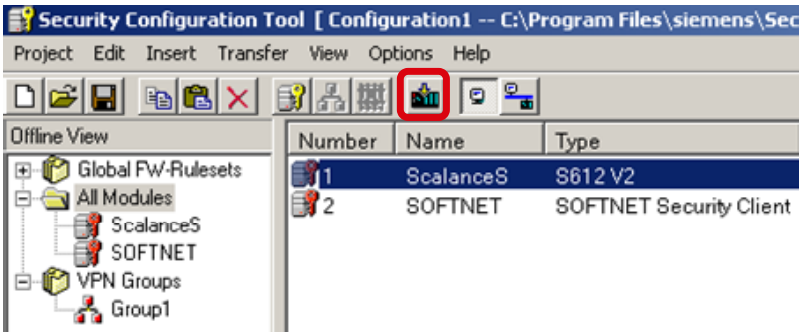


3.4 Download and save the configuration

Download the configuration in the SCALANCE S61x

Select the “S612 V2”-type module under “All Modules” and click the button “download” to assign the configuration to the SCALANCE S 61x.

Figure 3-11 assigning the configuration to the SCALANCE S61x

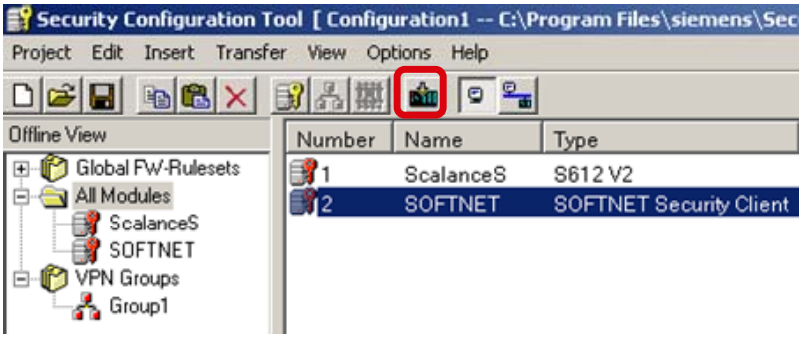


NOTE When the SCALANCE S61x is in factory setting, than the first download of the SCALANCE S61x isn’t possible via internet. The first download of SCALANCE S61x must takes place in the factory.

Save the configuration of the SOFTNET Security Client

Select the “SOFTNET Security Client”-type module under “All Modules” and click the button “download” to save the configuration data of the SOFTNET Security Client.

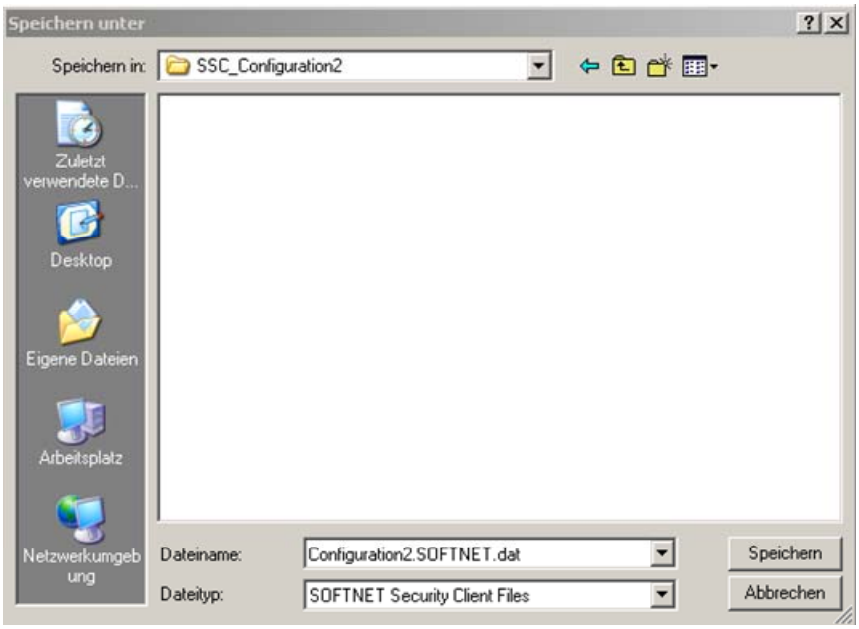
Figure 3-12 save the configuration data of the SOFTNET Security Client



The configuration data for the SSC are saved in a "*.dat" format file. Additional the PCKS12 certificate is saved in two “*.p12” and “*.cer” format files in the same directory as the configuration data.

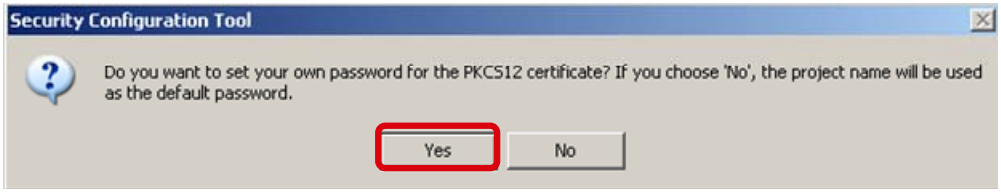
In this example the configuration file is called "Configuration2.SOFTNET.dat".

Figure 3-13 creating the configuration data



Saving PKCS12 certificate it’s possible to define a separate password. Confirm the following message with “Yes”.
When you confirm the message with “No” than the name of the project is used as password for the PKCS12 certificate.

Figure 3-14 defining the password for the PKCS12 certificate



In the following dialog you enter and confirm the password of the PKCS12 certificate. Close the dialog with “OK”.

Figure 3-15 password of the PKCS12 certificate

4 Establish the VPN tunnel with the SOFTNET Security Client

The SOFTNET Security Client establishes the VPN tunnel between PC station and SCALANCE S61x via the Internet.

Starting the SOFTNET Security Client

Start the SOFTNET Security Client with Start → SIMATIC → SCALANCE → Security → SOFTNET Security Client.

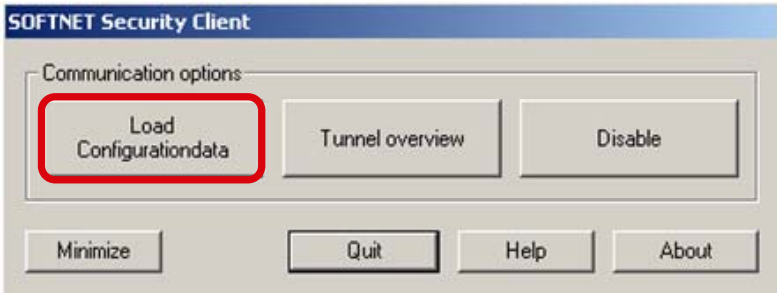
If you have installed multiple interfaces on your PC station for accessing the Internet (e.g. WLAN, UMTS card ...), then when you open the SOFTNET Security Client, a dialog window is displayed. In this dialog window you select the interface that you want to use for Internet access.

You can open the dialog to select the interface in the dialog “Tunnel overview”. Right-click the module to which the VPN tunnel is established and select the menu entry “Select Network Device”.

Load the configuration data

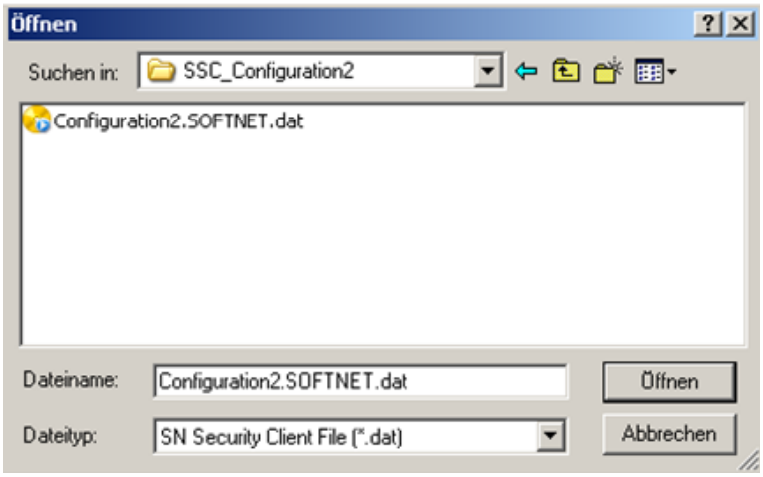
Click the button “Load Configurationdata” to load the configuration data in the SOFTNET Security Client.

Figure 4-1 loading the configuration data



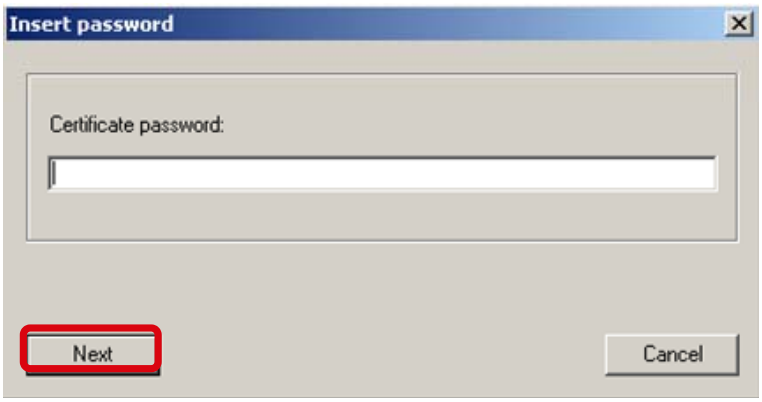
Open und load the configuration file “Configuration2.SOFTNET.dat”. The “*.p12” file and the “*.cer” file of the PCCS12 certificate must exist in the same directory as the configuration data.

Figure 4-2 opening and loading the configuration file



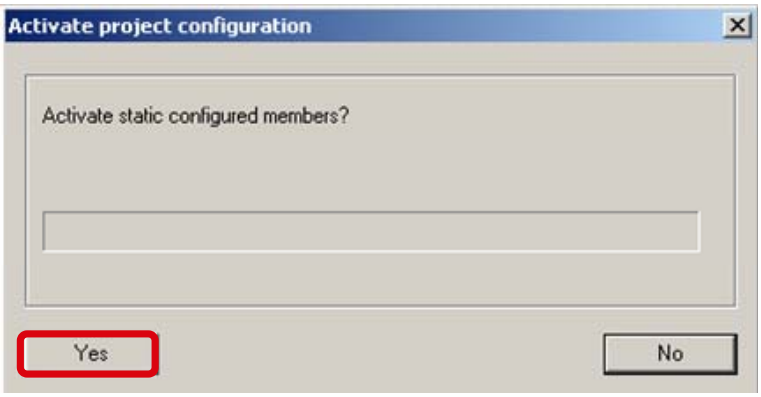
In the following dialog enter the password which you have defined for the PKCS12 certificate while saving the configuration data in the configuration file.
When you haven't defined a separate password for the PKCS12 certificate then enter the name of the project which you have created with the Security Configuration Tool and where the configuration of the SCALANCE S61x and SOFTNET Security Client is saved.

Figure 4-3 entering the password of PKCS12 certificate



Confirm the following message with "Yes".

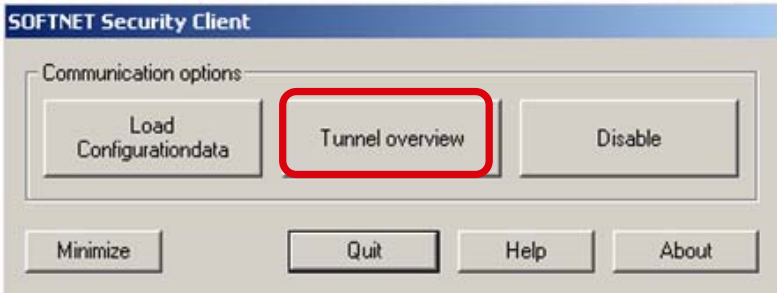
Figure 4-4 dialog "Activate project configuration"



Check the VPN tunnel

In the following dialog click the button "Tunnel overview". The dialog "Tunnel overview" is opened.

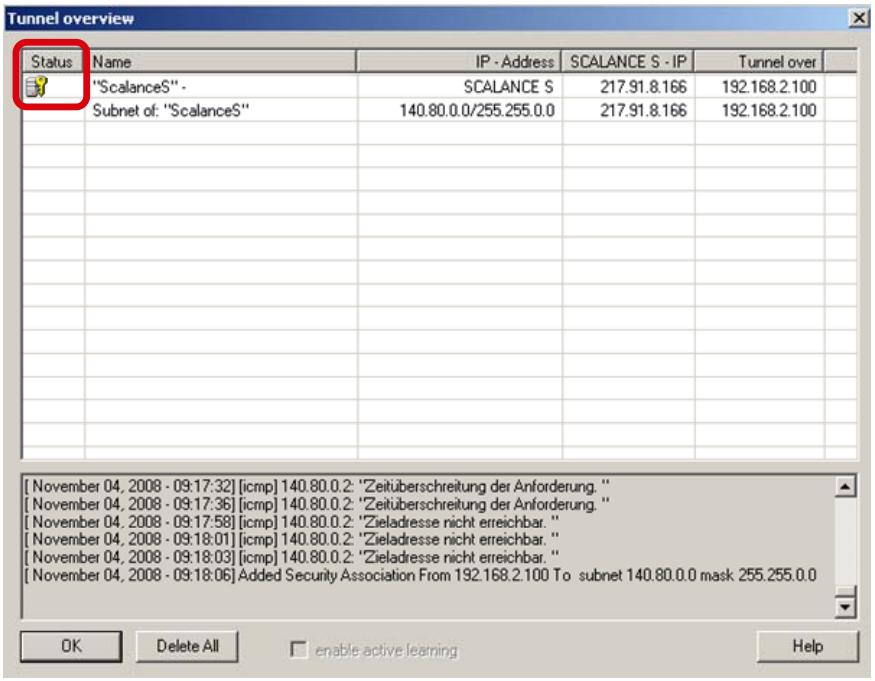
Figure 4-5 opening the dialog "Tunnel overview"



In the dialog “Tunnel overview” the modules and subnets are shown which are reachable via the VPN tunnel.

If the VPN tunnel is established successfully and the SCALANCE S61x is reachable by the PC station a yellow key will be shown in the column “Status”.

Figure 4-6 dialog “Tunnel overview”



5 Diagnostic

If the VPN tunnel between the PC station and the SCALANCE S61x is set up via the Internet, you can access the protected automation cell (S7-300 station) from the PC station, i.e.

- A ping can be transmitted from the PC station to the Industrial Ethernet CP which is used in the S7-300 station.
- In STEP 7 you can use the PG/OP functions to access the S7-300 controller online so as to enable you to load the STEP 7 project or the configuration into the S7-300 controller's CPU or to read out the CPU's diagnostic buffer.

NOTE The VPN tunnel does not support layer 2 protocols, such as the "accessible nodes" function in STEP 7.
Problems can also arise if there is a firewall additionally installed on the PC.

6 History

Table 6-1 History

Version	Date	Changes
V1.0	03.12.08	First issue
V1.1	15.12.08	Change the structure / composition of the document
V1.2	11.08.09	• Correct some spelling mistakes • When no separate password is defined while saving the certificate, than the name of the project is used as password. • Chapter 1: add the link to the download of the current firmware V2.3 for SCALANCE S61x • Chapter 3.1: delete the passage “Add firewall rules” • Chapter 4: Add the note how you can open the dialog to select the correct network adapter
V1.3	17.08.10	• New style sheet is used • Add-on in chapter 3.4, section “Save the configuration of the SOFTNET Security Client” → in addition to the configuration data the PKCS12 certificate is saved in the following files: “*.p12” and “*.cer” file • Add-on in chapter 4, section “Load the configuration data” → the “*.p12” and “*.cer” file must exist in the same directory as the configuration data