SIEMENS

Configuration Example• 06/2016

Setting up a Secure VPN Connection between CP 1543-1 and CP 1243-1

CP 1543-1, CP 1243-1

https://support.industry.siemens.com/cs/ww/en/view/109737287

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete with regard to configuration, equipment or any contingencies. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for the correct operation of the described products. These Application Examples do not relieve you of the responsibility of safely and professionally using, installing, operating and servicing equipment. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time and without prior notice. If there are any deviations between the recommendations provided in this Application Example and other Siemens publications – e.g. Catalogs – the contents of the other documents shall have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of fundamental contractual obligations ("wesentliche Vertragspflichten"). The compensation for damages due to a breach of a fundamental contractual obligation is, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of Siemens AG.

Security information

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

In order to secure plants, systems, machines and networks against cyber threats it is necessary to implement (and to maintain continuously) a holistic, state-of-the-art industrial security concept. With this in mind, Siemens' products and solutions are only part of such a concept.

It is the client's responsibility to prevent unauthorized access to his plants, systems, machines and networks. Systems, machines and components should only be connected with the company's network or the Internet, when and insofar as this is required and the appropriate protective measures (for example, use of firewalls and network segmentation) have been taken.

In addition, the recommendations by Siemens regarding the respective protective measures have to be observed. For more information on industrial security, visit http://www.siemens.com/industrialsecurity.

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

In order to always be informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at http://www.siemens.com/industrialsecurity.

Table of Contents

Warranty and Liability 2

1 Task and Solution 4

1.1 Task 4
1.2 Possible solution 4
1.3 Characteristics of the solution 5

2 Configuration and Settings 6

2.1 Setting up the environment 6
2.1.1 Required components and IP address overview 6
2.1.2 TIA Portal project and SIMATIC stations 8
2.1.3 DSL access for CP1543-1 9
2.1.4 Setting up the infrastructure 9
2.2 Configuring the VPN tunnel 10
2.2.1 Configuring the VPN endpoint CP 1543-1 10
2.2.2 Configuring the VPN endpoint CP 1243-1 13
2.2.3 Configuring the VPN tunnel 15
2.2.4 Loading the components 19
2.3 Configuration and diagnostics of the VPN connection 20

3 Related literature 22

4 History 22

1 Task and Solution

1.1 Task

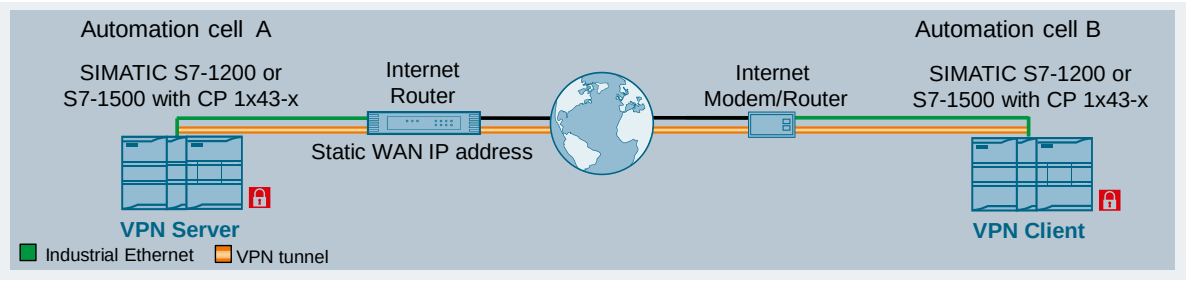
The objective is to enable a secure connection between two automation cells via the Internet or a company's internal network.
The following customer requirements have to be considered:

- Protection against spying and data manipulation.
- Prevention of unauthorized access.
- Provision of a secure communication level.
- Network protection without own security appliance on the automation side.

1.2 Possible solution

General overview

The figure below shows one way of implementing the customer requirements:



The connection between the two automation cells is protected by a VPN tunnel.

In this example, the security CPs of the new controller generation form the tunnel endpoints for the secure tunnel connection. The CP 1543-1 acts as VPN server in this example, the CP 1243-1 as VPN client.

Access to the CP 1543-1 is predefined by the use of a static WAN IP address.

WAN access on the client side is flexible; the IP address of the WAN access is not relevant.

When establishing the VPN tunnel, the roles are defined as follows:

Table 1-1

Component	VPN role
CP 1543-1 (firmware version V1.1 or higher)	Responder (VPN server); waits for the VPN connection
CP 1243-1	Initiator (VPN client); starts the VPN connection

CP 1x43-x

The communication processors

- CP 1243-1 (6GK7243-1BX30-0XE0)
- CP 1243-7 LTE (6GK7242-7KX30-0XE0)
- CP 1243-8 IRC (6GK7243-8RX30-0XE0)
- CP 1543-1 (6GK7543-1AX00-0XE0)

connect the SIMATIC S7-1200 or S7-1500 securely with the Ethernet networks.

The module provides secure data transmission between devices or network segments against data manipulation/spying and unauthorized access without additional security equipment.

In addition to the basic communications services, it offers the following integrated security functions:

- High-quality stateful inspection firewall with filtering of IP- and MAC-based data traffic.
- IPSec VPN (data encryption and authentication).
- Protection of the S7 station in which the CP is operated.
- Support of multiple VPN tunnels at a time.
- Use of an IPV6 infrastructure.
- Additional communication options via email and FTPs (only CP 1543-1).

1.3 Characteristics of the solution

- Controlled and encrypted data traffic between CP 1243-1 and CP 1543-1
- Integrated network diagnostics via SNMP or Syslog.
- Protection of the SIMATIC controller without an additional security module.
- Secure lower-level networks can be operated via additional Ethernet/PROFINET interfaces, realized by the CPU or additional CPs.

2 Configuration and Settings

2.1 Setting up the environment

2.1.1 Required components and IP address overview

Software packages

This solution requires the software packages STEP 7 Professional V13 SP1 Update 7.

Install this software on a PC/PG.

Required devices/components:

Use the following components for the configuration:

- 1 x CP 1543-1 (firmware version V1.1 or higher) (MLFB: 6GK7543-1AX00-0XE0)
- 1 x CPU 1516-3 PN/DP (firmware V1.5 or higher) (MLFB: 6ES7516-3AN00-0AB0) with a SIMATIC MEMORY CARD.
- 1 x CP 1243-1 (MLFB: 6GK7243-1BX00-0XE0)
- 1 x CPU 1212C DC/DC/DC (MLFB: 6ES7212-1AE40-0AB0) with a SIMATIC MEMORY CARD.
- DSL access with a static WAN IP address and a DSL router.
- DSL access with a dynamic WAN IP address and a DSL router.
- A 24V power supply with cable connector and terminal block plug.
- DIN rail with mounting material for the S7-1500 and S7-1200.
- 1 x PC on which the “STEP 7 Professional V13 SP 1” configuration tool is installed.
- The necessary network cables, TP cables (twisted pair) according to the IE FC RJ45 standard for Industrial Ethernet.
- Optional: a switch in order to view the online diagnostic of the CP

Note Instead of the DSL access, you can also use a different Internet access method (for example, UTMS) and other CPU types.
The configuration described below explicitly refers only to the components listed in the section "Required devices/components".

Note To make sure that no old configurations and certificates are stored in the modules, reset the modules to factory settings. In the configuration below, it is assumed that the modules are in this state.

IP addresses

For this example, the IP addresses are assigned as follows:

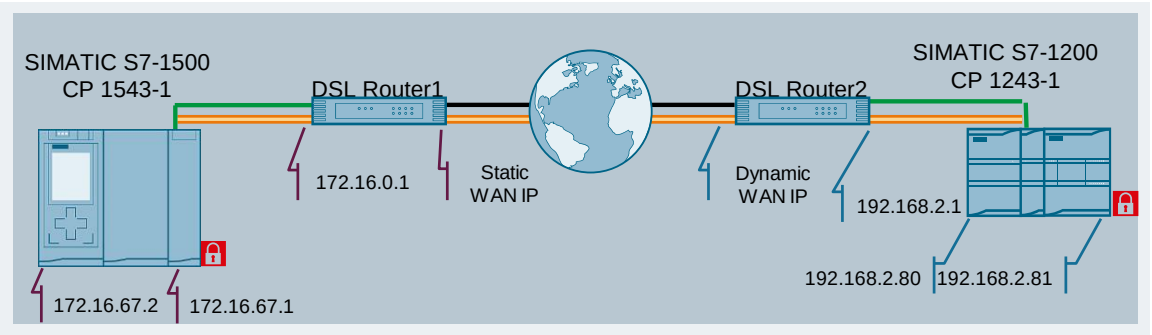


Table 2-1

Component	Port	IP address	Router	Subnet
S7-1516	PROFINET port	172.16.67.2	172.16.67.1	255.255.0.0
CP 1543-1	External port	172.16.67.1	172.16.0.1	255.255.0.0
DSL Router1	LAN port	172.16.0.1	-	255.255.0.0
DSL Router1	WAN port	Static IP address	-	Assigned by provider
DSL router2	WAN port	Dynamic IP address	-	Assigned by provider
DSL router2	LAN port	192.168.2.1	-	255.255.255.0
CP 1243-1	Ethernet port	192.168.2.80	192.168.2.1	255.255.255.0
CPU 1212C	PROFINET port	192.168.2.81	192.168.2.1	255.255.255.0

2.1.2 TIA Portal project and SIMATIC stations

Hardware configuration

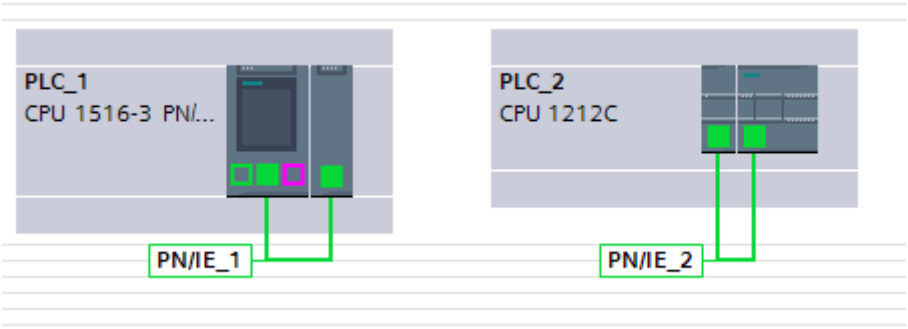
Use the TIA V13 configuration software to create a new project. Create a hardware configuration with the S7-1500 modules you are using.

Add another device using the project navigation. Create a hardware configuration with the S7-1200 modules you are using.

Configuring the interfaces

Configure the interfaces of the CPU and CPs according to the specifications of Table 2-1. Disable the IPv6 functionality in the properties of the CP.

Result:
Two SIMATIC controllers are configured and networked in the project.



Connection between PC and controller

Connect the PC to a PROFINET port of the CPU and change the network settings on the PC as follows:

For the S7-1500 station:

IP address: 172.16.67.100

Subnet mask: 255.255.0.0

For the S7-1200 station:

IP address: 192.168.2.100

Subnet mask: 255.255.255.0

Changing the IP address of the CPU

To download the project data into the CPU, it is useful to first change the IP address of the CPU as shown in Table 2-1.

The STEP 7 function "Edit Ethernet Node…" is suitable for assigning the IP address (“Accessible nodes...”). Connect the PC to a PROFINET port of the CPU and change the network settings on the PC as described in the previous chapter:

Loading the stations

Save the TIA project.
Select both controllers one after the other in the project navigation and load their configuration into the modules. Connect the PC to a PROFINET port of the CPU and change the network settings on the PC as described in the previous chapter:

Click on the "Finish" button if the loading process was done without errors.

Result:
The modules automatically restart and the loaded configuration is activated.

2.1.3 DSL access for CP1543-1

Static IP address for the DSL Router1

WAN access of the CP 1243-1 to the CP 1543-1 is implemented using a fixed public IP address. This IP address must be requested from the provider and then stored in the DSL Router1.

Port forwarding on the DSL Router1

By using a DSL Router1 as Internet gateway, the following ports have to be enabled on the DSL Router1 and the data packets have to be forwarded to the CP 343-1 (VPN server; external port):

- UDP port 500 (ISAKMP)
- UDP port 4500 (NAT-T)

VPN function

If your DSL router1 are VPN-capable, make sure that this function is disabled.

2.1.4 Setting up the infrastructure

Connect all the components involved in this solution.

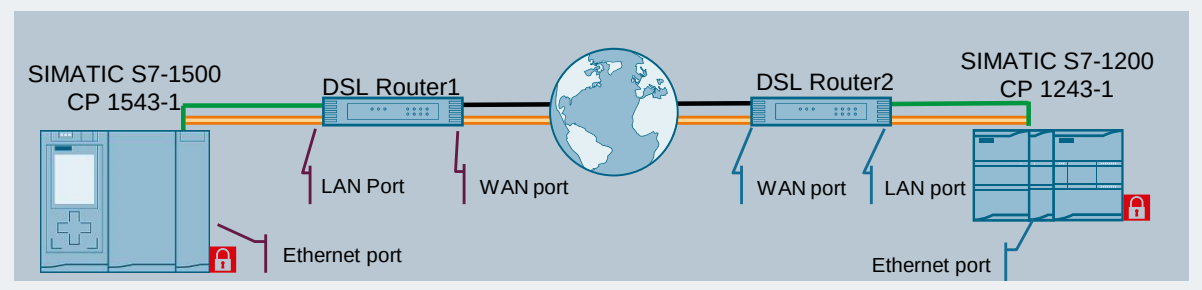


Table 2-2

Component	Local port	Partner	Partner port
CP 1543-1	Ethernet port	DSL Router1	LAN port
CP 1243-1	Ethernet port	DSL Router2	LAN port

2.2 Configuring the VPN tunnel

Configuration software

The VPN tunnel is configured directly in the TIA Portal V13.

Components used

This solution uses the security components
CP 1543-1 (firmware V1.1 or higher) and CP 1243-1.

2.2.1 Configuring the VPN endpoint CP 1543-1

Overview

The configuration of the CP as VPN endpoint requires the following steps:

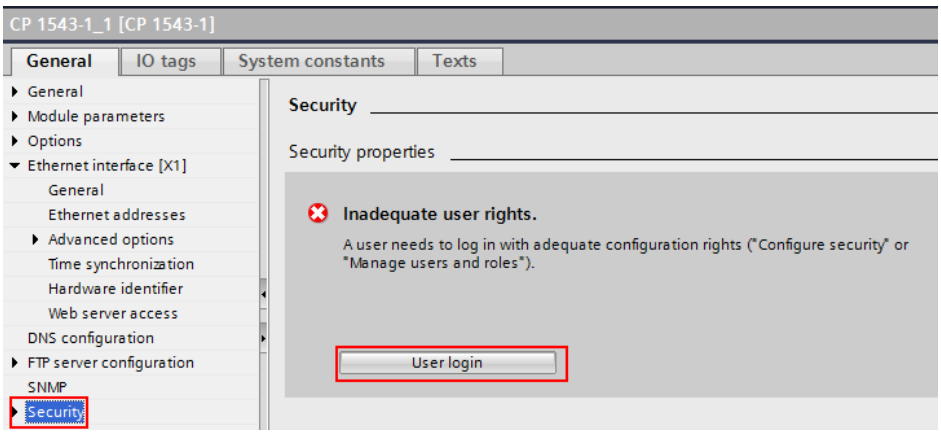
- Create a new security project.
- Enable the security function of the CP.
- Enable the firewall for diagnostics

Creating new security project

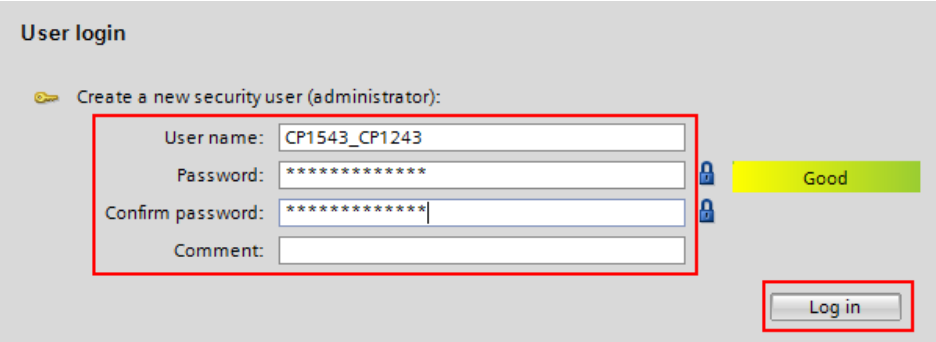
Proceed as follows:

1. Select the menu item “Security” > “Security properties” in the “General” window tab.

2. In the following screen click “User login”.



3. Create a new user with a user name and the appropriate password. The user is automatically assigned the "Administrator" role.



4. Click on the “Log in” button.

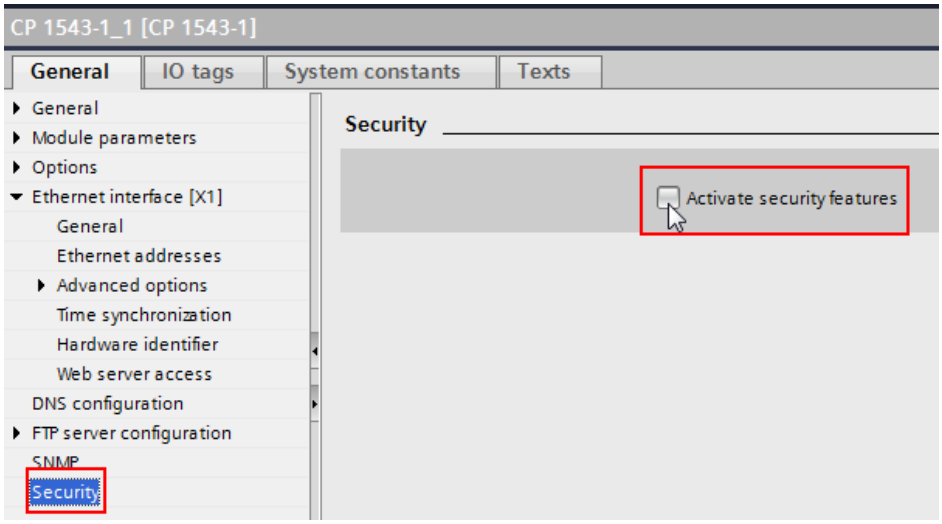
Result:
A new security project has been created. All security settings that you make from now on are stored encrypted in the project and can only be viewed and edited with the created user and password.

Enabling security function

Proceed as follows to enable the security function:

1. Go back to the “Device configuration” of your S7-1500 station and reselect the CP 1543-1 in order to configure the properties.

2. Enable the “Activating security features” checkbox in the local security settings.

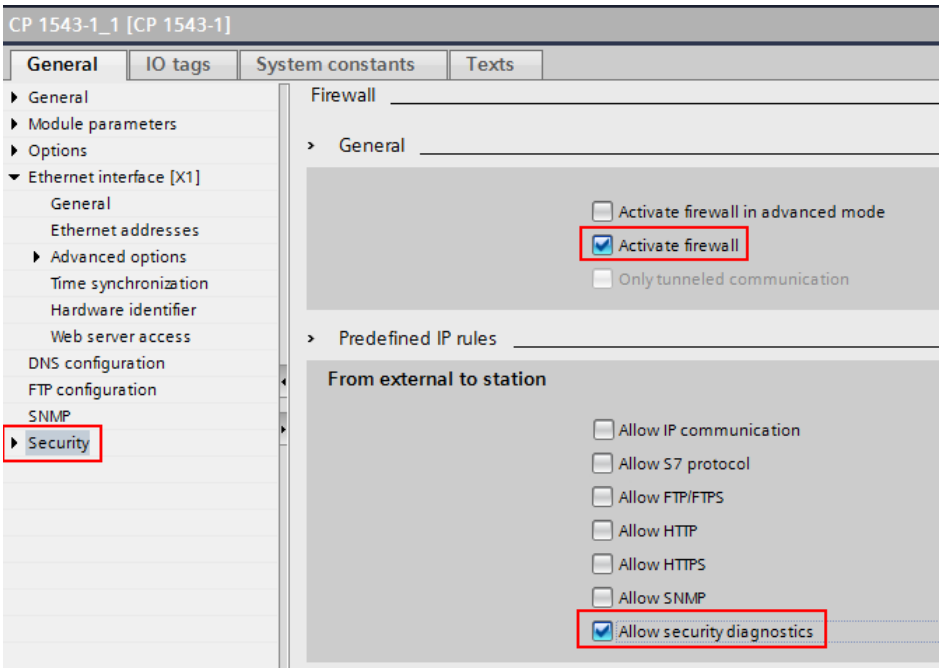


Result:
The security functions are now available for this CP.

Enabling firewall for diagnostics

By default, the online diagnostic of the security functions is allowed via the VPN tunnel. For a PC to be able to read the information from the internal network of the CP, two firewall settings are required. Proceed as follows:

1. Enable the firewall as well as the “security diagnostics” for the security functions you just enabled.



2. Save the project.

2.2.2 Configuring the VPN endpoint CP 1243-1

Overview

The configuration of the CP as VPN endpoint including online diagnostic options requires the following steps:

- Specify the communication types
- Enable the security function of the CP.
- Enable the firewall for diagnostics

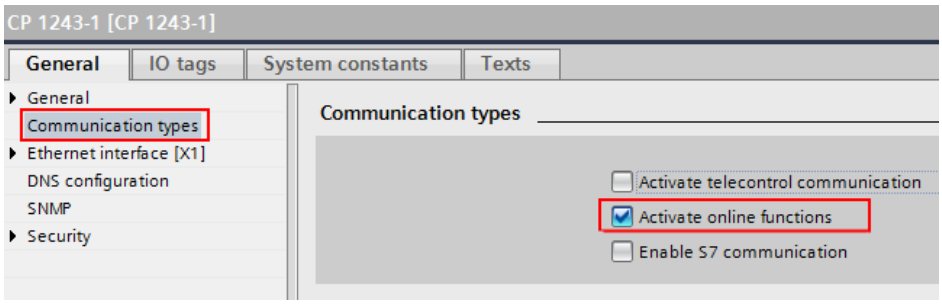
Specifying communication types

For the diagnostic of the CP the online functions on the CP have to be enabled.

1. Open your TIA project and go to the “Device configuration” in your S7-1200 station.

2. Select the CP 1243-1 to be able to configure the properties.

3. Enable the “Activate online functions” checkbox in communication types.

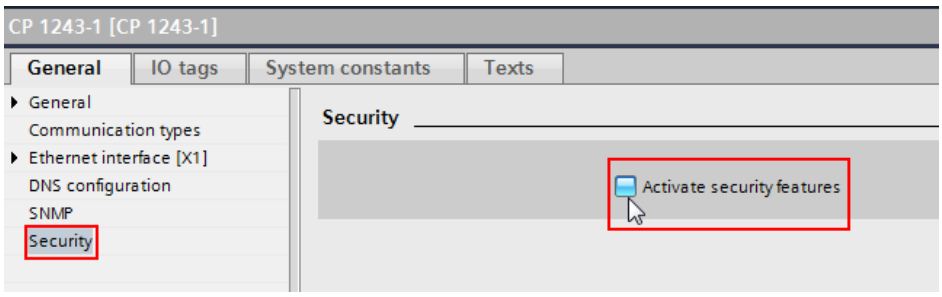


Result:

The online functions via the CP interface are enabled.

Enabling security function

Enable the “Activating security features” checkbox in the local security settings.



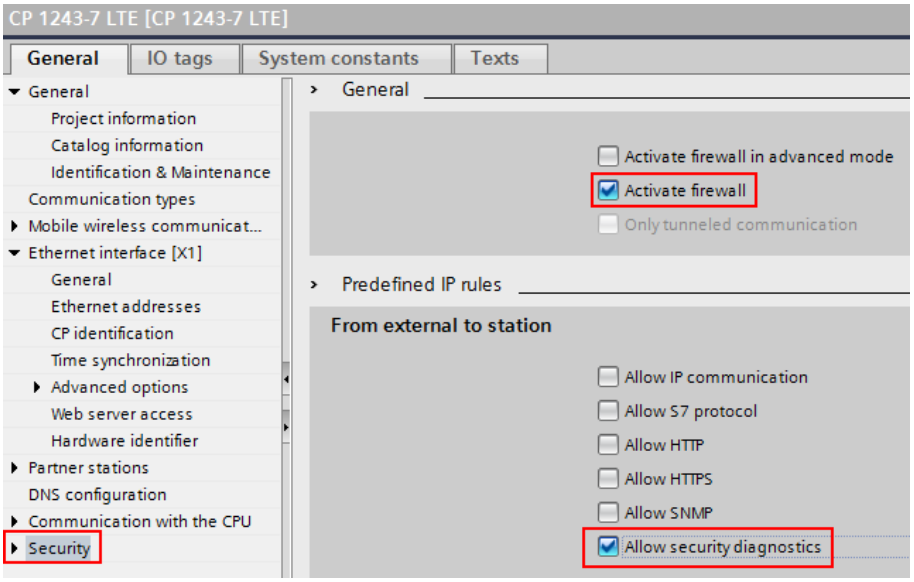
Result:

The security functions are now available for the CP.

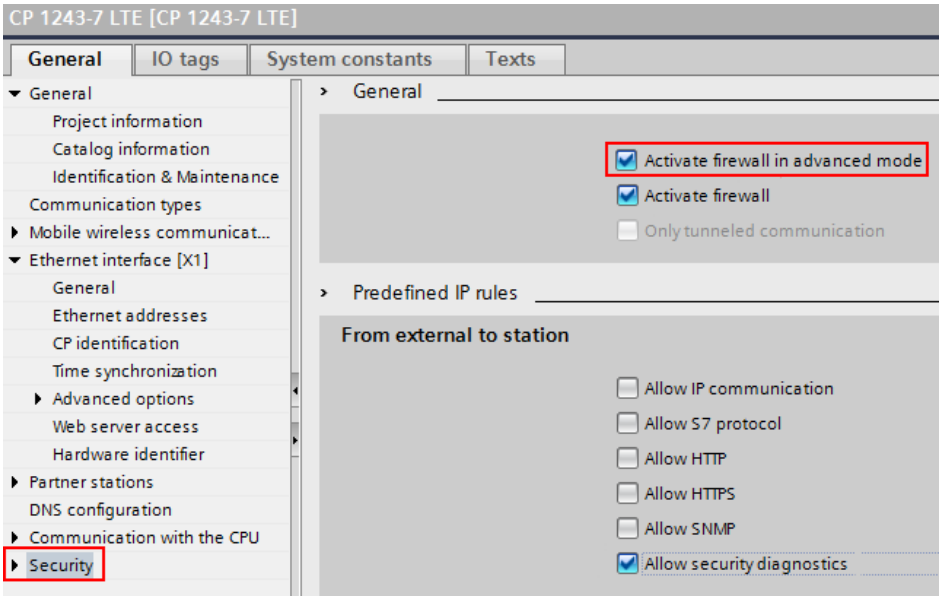
Enabling firewall for diagnostics

By default, the online diagnostic of the security functions is allowed via the VPN tunnel. For a PC to be able to read the information from the internal network of the CP, two firewall settings are required. Proceed as follows:

1. Enable the firewall as well as the “security diagnostics” for the security functions you just enabled in the “Firewall” > “General” section.



2. Then enable the Firewall in the advanced mode.



3. Save the project.

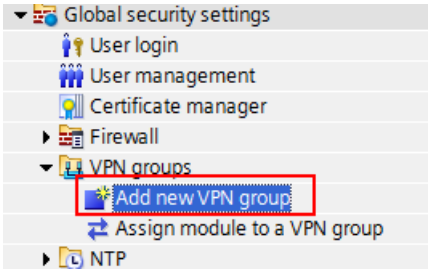
2.2.3 Configuring the VPN tunnel

Creating a VPN group

All members of a VPN group are authorized to communicate with each other through a VPN tunnel.

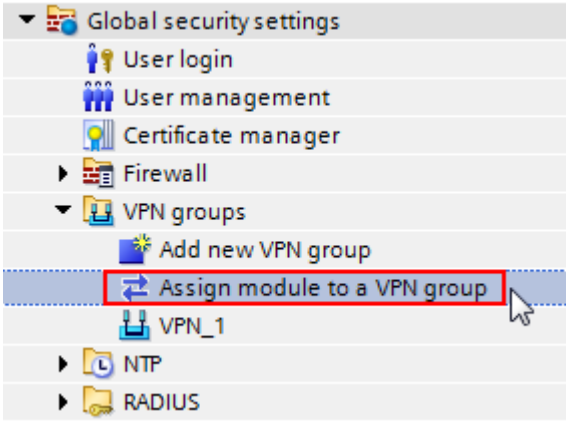
To create a VPN group, proceed as follows:

1. Double click the “VPN groups” > “Add new VPN group” entry in the project navigation in the global security settings.

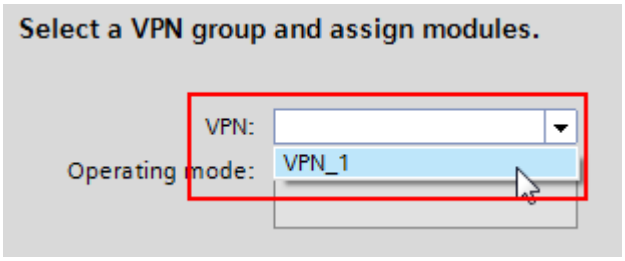


Result:
A new **VPN_1** group has been created and assigned to the “VPN groups” entry.

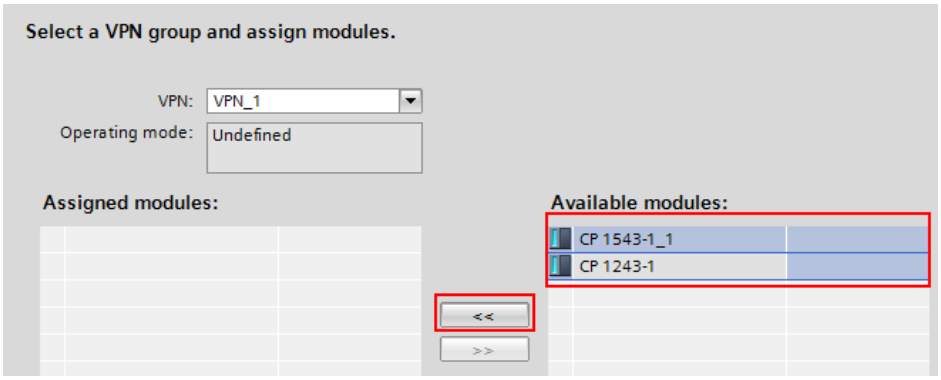
2. Double click the “VPN groups” > “Assign module to a VPN group” entry.



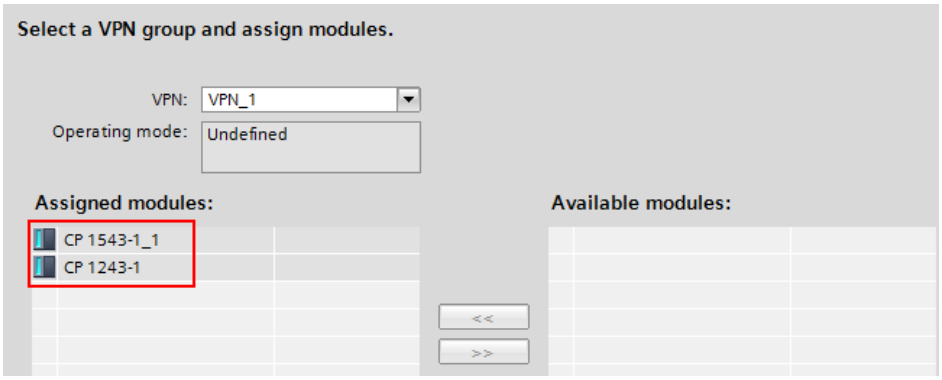
3. Select the VPN group you just created.



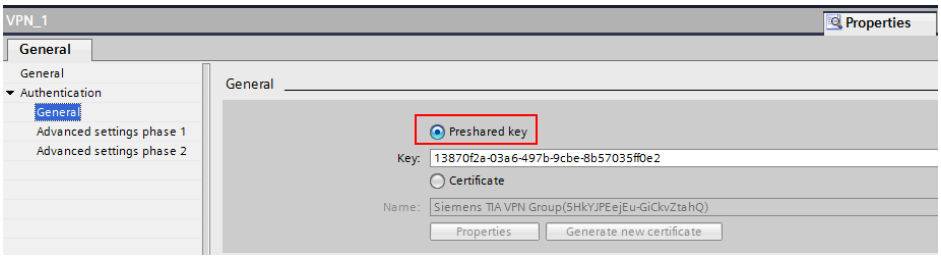
4. All configured security modules are listed in the “Available modules” column. Select the two security CPs and move them via the “<<” button to the “Assigned modules” list.



5. The security modules have been assigned to the **VPN_1** VPN group.



6. Select the “VPN groups” > “VPN_1” entry in order to configure the properties. Select the "Preshared key" authentication method in “General”.



Result:
The VPN group has been created and the modules involved are integrated.
You can check this in the network view in the “VPN” tab. Preshared key is used as authentication method.

VPN	Security module	Authentication	Group membership until	Type
VPN_1				
	CP 1543-1_1	Preshared key		CP 1543-1
	CP 1243-1	Preshared key		CP 1243-1

Note You can also use certificates for authentication. In this case, make sure that the two CPs always have the current time (for example, via the NTP procedure). Otherwise the certificates are interpreted as invalid and the VPN tunnel is not established.

Defining VPN parameter CP1543-1

To establish the VPN tunnel, you have to enter the following information:

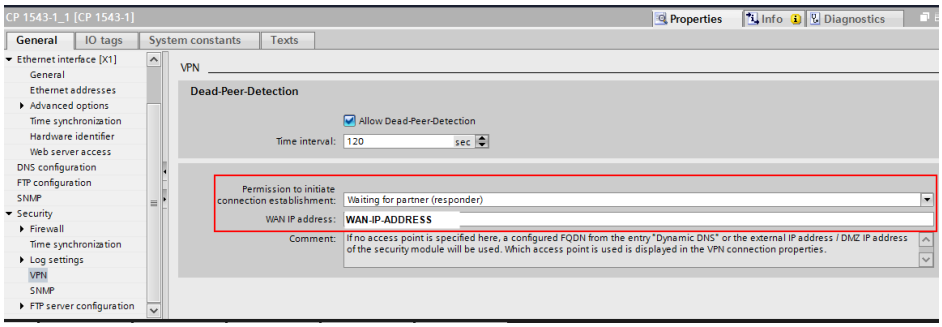
- WAN IP address of the DSL router
- VPN role

These module-specific properties can only be configured, once a VPN group has been configured in the local security settings:

1. Go to the “Device configuration” of your S7-1500 station and select the CP 1543-1 in order to configure the properties.

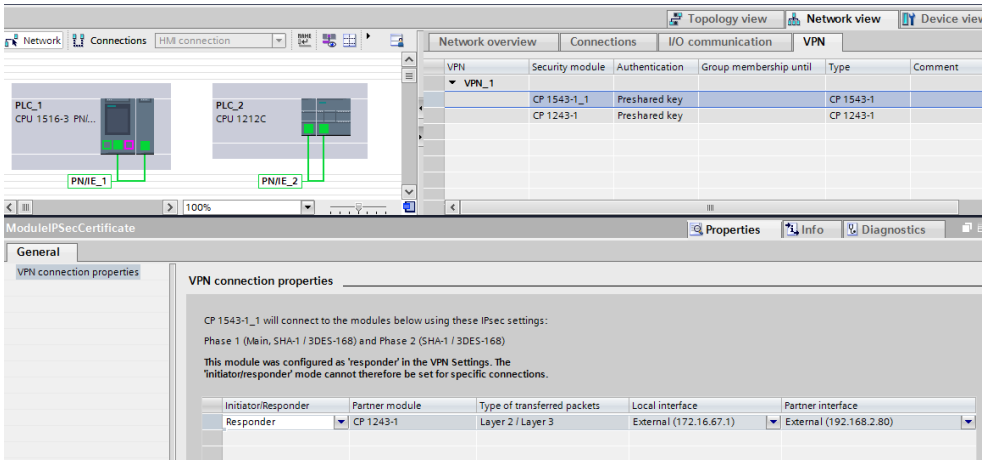
2. Go to “VPN” in the local security settings.

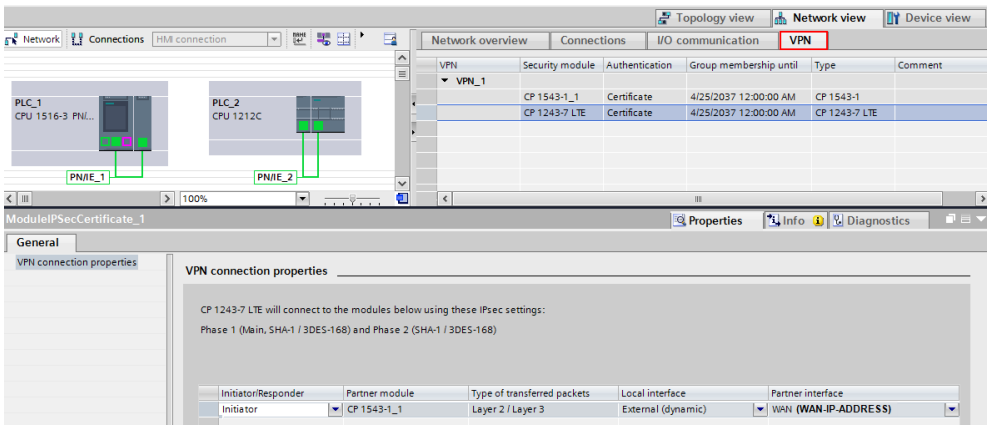
3. Change the VPN role to “Waiting for partner” and enter the WAN IP address of your DSL access (DSL Router1).



4. Save the TIA project.

Result:
The VPN configuration is complete. You can check the configuration by clicking the modules in the network view in the “VPN” tab.





2.2.4 Loading the components

Preparation

Since an external public network is using a WAN, the security modules with factory settings cannot be configured via this WAN. In this case, configure the security modules from the local network.

Connection between PC and SIMATIC station

Connect the PC to a PROFINET port of the CPU and change the network settings on the PC as follows:

For the S7-1500 station:

IP address: 172.16.67.100

Subnet mask: 255.255.0.0

For the S7-1200 station:

IP address: 192.168.2.100

Subnet mask: 255.255.255.0

Loading the modules

1. Select the CPU with which you connected in the project navigation and compile your project via “Edit” > “Compile”.

2. Load the configuration via “Online > Extended download to device” into your CPU.

3. If the modules are to be restarted directly after the loading, enable the “Start all" checkbox.

4. Press “Finish” to close the dialog box.

5. Proceed in the same way to load the other station as well.

Result:
The hardware configuration and the blocks have been loaded into the CPU. In the messages in the inspector window in “Info” > “General” you can see whether the loading process was successful.
The security module is in productive mode.

2.3 Configuration and diagnostics of the VPN connection

When all security modules have been configured, loaded and connected to the appropriate DSL routers, the CP 1243-1 initializes the VPN tunnel to the CP 1543-1.

Diagnostics via the LED display

The status can be read, based on the “VPN” LED that lights up in green on the CP 1243-1.

Status report via online diagnostic

A status report of the VPN connection can also be viewed via the online functions of the CP.

It is important to use the CP interface as online access and not the PROFINET interface of the CPU.

1. Connect the PC, the CP and the appropriate DSL router, using a switch.

2. Change the network settings on the PC as follows:

   For the S7-1500 station:

   IP address: 172.16.67.100

   Subnet mask: 255.255.0.0

   For the S7-1200 station:

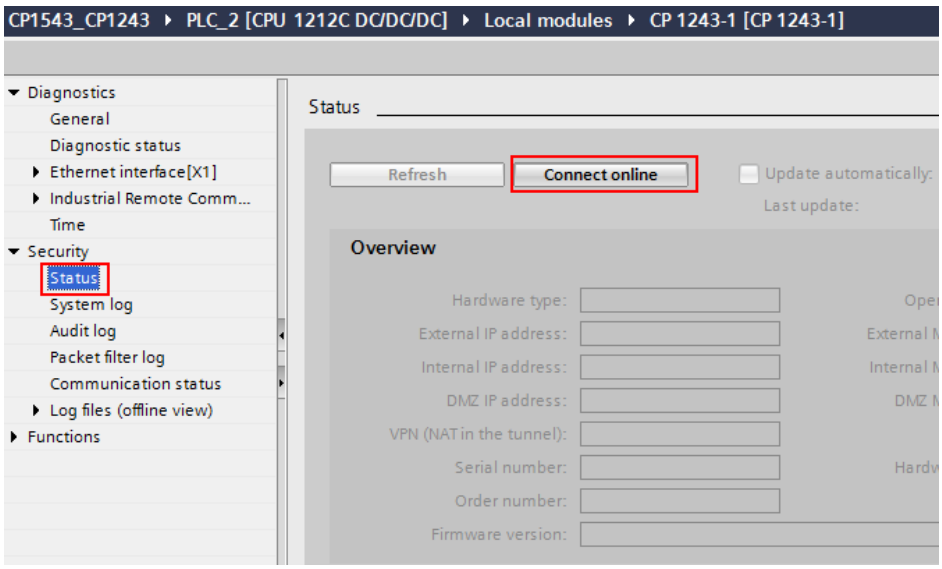
   IP address: 192.168.2.100

   Subnet mask: 255.255.255.0

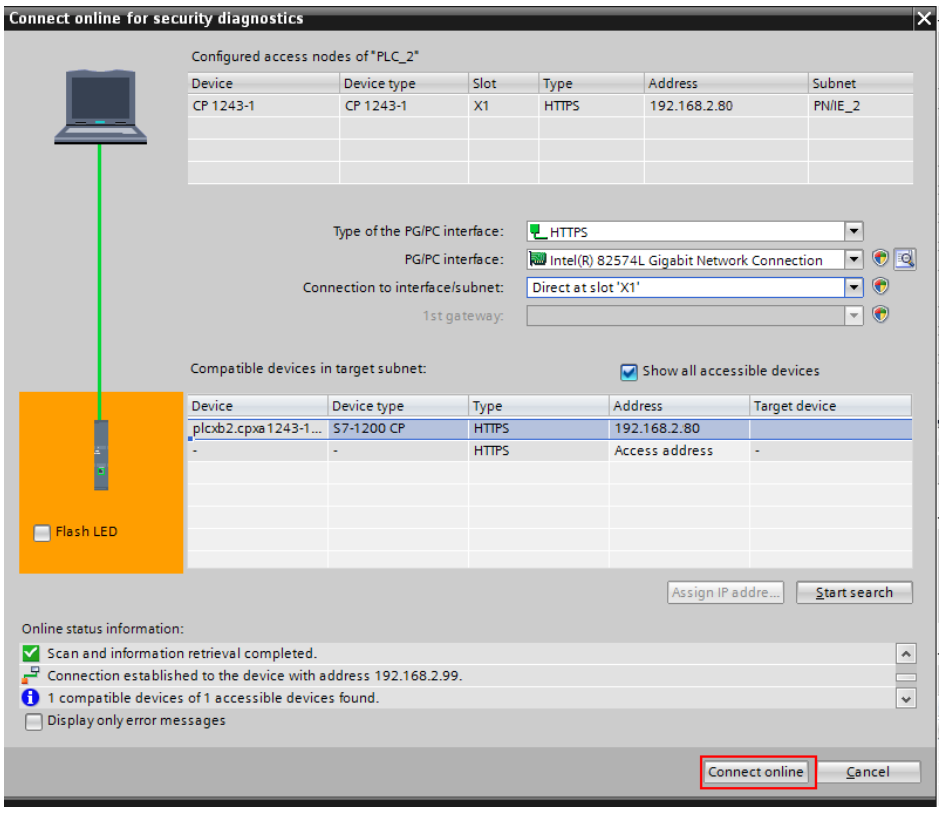
3. Open your TIA project and go to the “Device configuration” of your S7-1x00 station.

4. Select the CP and go to “Online & diagnostics” via the context menu (right mouse button).

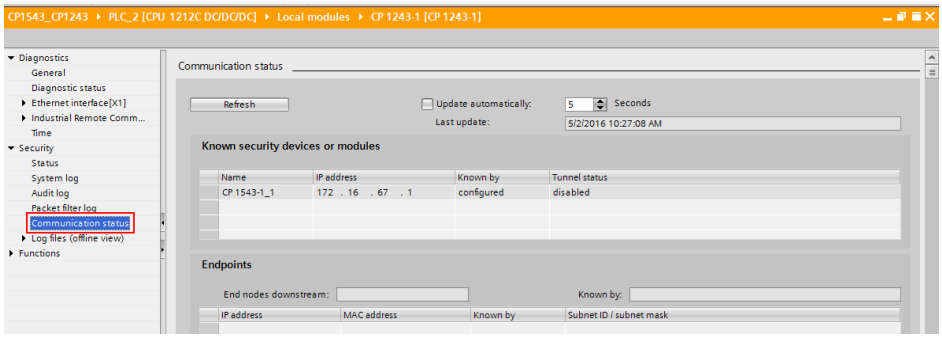
5. Click the “Connect online” button in “Security > “Status”.



6. Select the interface of the CP and start a search. Connect to the detected CP.



7. You can view the status of the VPN connection in “Security” > “Communication status”.



3 Related literature

Table 3-1

	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download page of this entry https://support.industry.siemens.com/cs/ww/en/view/109737287

4 History

Table 4-1

Version	Date	Modifications
V1.0	06/2016	First version