

# Determine the Security Status of the CP1628 over the Online View of the Security Configuration Tool (SCT)

CP1628 and Security Configuration Tool

FAQ • July 2012



## Service & Support

Answers for industry.

**SIEMENS**

---

This entry is from the Siemens Industry Online Support. The general terms of use ([http://www.siemens.com/terms\\_of\\_use](http://www.siemens.com/terms_of_use)) apply.

Clicking the link below directly displays the download page of this document.

<http://support.automation.siemens.com/WW/view/en/62080477>

**Caution**

The functions and solutions described in this article confine themselves predominantly to the realization of the automation task. Furthermore, please take into account that corresponding protective measures have to be taken in the context of Industrial Security when connecting your equipment to other parts of the plant, the enterprise network or the internet. Further information can be found in Entry ID 50203404.

<http://support.automation.siemens.com/WW/view/en/50203404>

## Question

How you can display the security status of the CP1628 over the Online View in the Security Configuration Tool (SCT).

## Answer

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

---

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>4</b>
<b>2</b>	<b>Locale and Remote Diagnostics of a CP1628 .....</b>	<b>6</b>
2.1	NDIS IP Address and IE IP Address of a CP1628 are in the same subnet.....	6
2.2	NDIS IP Address and IE IP Address of a CP1628 are not in the same subnet.....	7
2.3	NDIS IP Address and IE IP Address of multiple CP1628s are not in the same subnet .....	10

# 1 Introduction

The CP1628 enables safe connection to the Industrial Ethernet for SIMATIC PG/PC and PCs with PCI Express slot.

## Conditions

You can configure two different IP addresses for the CP1628, because it is designed for two different communication tasks:

- Office communication, for example TCP/IP
- Data communication on an automation level with S7 communication, open communication (SEND/RECEIVE), etc.

Different IP addresses are assigned to the CP1628 to identify the connections clearly:

- NDIS IP address for office communication via Microsoft network connections
- Industrial Ethernet IP address used in the configured mode for communication on the automation level.

If you are using two or more CP1628 in a PC, then the NDIS IP addresses must not be in the same subnet in Windows.

The Security Configuration Tool (SCT) executes the diagnostics over HTTPS and addresses the CP1628 over its NDIS IP address to access the Industrial Ethernet diagnostics data. This applies for local and remote diagnostics of a CP1628.

If you configure your own firewall rules for the CP1628 through the SCT, use the syntax below for those firewall rules:

*<Action> <From> <To> <Source IP> <Target IP>*

## Security Functions

The security functions below are integrated in the CP1628.

- Integrated security mechanisms like firewall, VPN, etc.
- Secure integration in the network management (SNMP V3)
- Secure transfer of the time (NTP V3)
- Traceability through data logging using standard IT mechanisms

The integrated security mechanisms of the CP1628 enable you to secure important computer systems including the associated data communication in an automation network or as secure remote access.

The security functions are made exclusively over the Security Configuration Tool (SCT) that is called through STEP 7/NCM PC.

**Scenarios for local and remote diagnostics of a CP1628.**

The Security Configuration Tool (SCT) enables you to display the security status of the CP1628 in the Online view.

Three scenarios:

1. Local and remote diagnostics of a CP1628 when the NDIS IP address and the Industrial Ethernet IP address of the module are in the same subnet.
2. Local and remote diagnostics of a CP1628 when the NDIS IP address and the Industrial Ethernet IP address of the module are not in the same subnet.
3. Local and remote diagnostics of several CP1628 when the NDIS IP address and the Industrial Ethernet IP address of the module are not in the same subnet.

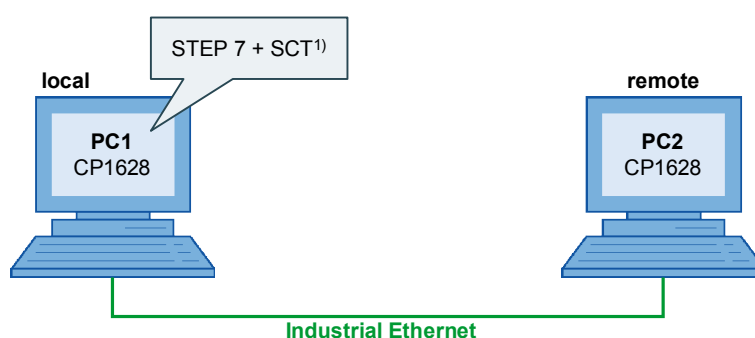
## 2 Locale and Remote Diagnostics of a CP1628

### 2.1 NDIS IP Address and IE IP Address of a CP1628 are in the same subnet

#### Overview

Figure 2-1 shows an overview of the configuration for local and remote diagnostics of a CP1628. The NDIS IP Address and IE IP Address of a module are in the same subnet.

Figure 2-1



PC1 (local)	PC2 (remote)
CP1628	CP1628
NDIS IP address: <b>192.168.0.110</b> / 24	NDIS IP address: <b>192.168.0.220</b> / 24
IE IP address: <b>192.168.0.10</b> / 24	IE IP address: <b>192.168.0.20</b> / 24

¹) The Security Configuration Tool (SCT) executes the diagnostics over the CP1628 in PC1.

#### Local diagnostics of the CP1628 in PC1

Over the NDIS IP address 192.168.0.110 the SCT can address the local IE IP address 192.168.0.10 and read out the data of the CP1628 in PC1, because both IP addresses are in the same subnet.

If the firewall is enabled in the CP1628 of the PC1, there is no need to add any special rules for the module in the SCT.

#### Remote diagnostics of the CP1628 in PC2

Over the NDIS IP address 192.168.0.110 of the CP1628 in PC1 and the NDIS IP address 192.168.0.220 of the CP1628 in PC2, the SCT can address the remote IE IP address 192.168.0.20 and read out the data of the CP1628 in PC2 because all the IP addresses are in the same subnet.

If the firewall is enabled in the CP1628 of the PC2, you must enter an allow rule in the firewall of the module for the diagnosing CP1628 in PC1.

Table 2-1 shows the allow rule required.

Table 2-1

Action	From	To	Source IP address	Destination IP address
Allow	External	Station	192.168.0.110	-.-.-.-

## 2.2 NDIS IP Address and IE IP Address of a CP1628 are not in the same subnet

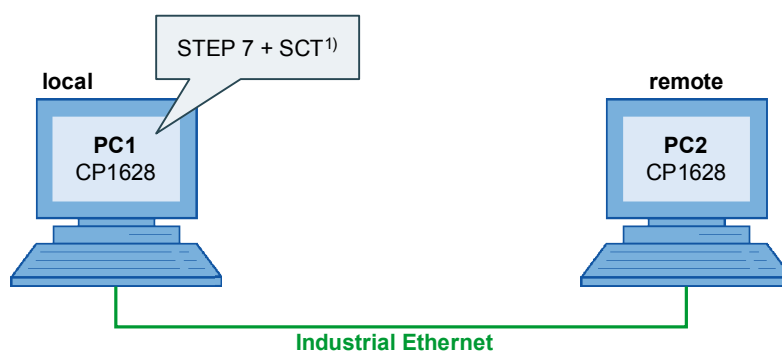
### Overview

Figure 2-2 shows an overview of the configuration for local and remote diagnostics of a CP1628.

Since the NDIS IP address and the IE IP address of the module are not in the same subnet, you enter routes in Windows on the local PC1.

In the configuration of the remote CP1628 you enter the IE IP address 192.168.1.10 of the diagnosing CP1628 in PC1 as router.

Figure 2-2



PC1 (local)	PC2 (remote)
<b>CP1628</b>	<b>CP1628</b>
NDIS IP address: <b>192.168.0.110</b> / 24	NDIS IP address: <b>192.168.0.220</b> / 24
IE IP address: <b>192.168.1.10</b> / 24	IE IP address: <b>192.168.1.20</b> / 24
Interface Number: 15 <sup>2)</sup>	Interface Number: 14 <sup>2)</sup>

<sup>1)</sup> The Security Configuration Tool (SCT) executes the diagnostics over the CP1628 in PC1.

<sup>2)</sup> In the Windows Console you use the command "route print interface" to detect the Interface Number.

If the NDIS IP address is in a different subnet to the IE IP address, you enter a gateway in the routing table in Windows on PC1. In this example you enter the NDIS IP address of the CP1628 in PC1 as gateway.

On PC1 you start the Windows console by means of the menu "Start → Run → cmd.exe".

In the Windows console you enter the "route" command with the syntax below:  
`route -p add <Target IP address> mask <Subnet> <Gateway> if <Interface no.>`

To ensure that Windows uses the right interface for the specified gateway, you enter the interface number of the CP1628 in PC1 in the "route" command. You determine the interface number in the Windows console using this command:

`route print interface`

The interface number 15 is determined in this example.

**Local diagnostics of the CP1628 in PC1**

For local diagnostics of the CP1628 in PC1 you enter the route below in Windows on the PC1.

Table 2-2

	Target IP address		Subnet	Gateway	Interface no.
route -p add	192.168.1.10	mask	255.255.255.255	192.168.0.110	if 15

Once you enter the route the SCT can address the local IE IP address 192.168.1.10 through the NDIS IP address 192.168.0.110 that was entered as gateway and read out the data of the CP1628 in PC1.

If the firewall is enabled in the CP1628 of the PC1, there is no need to add any special rules for the module in the SCT.

**Remote diagnostics of the CP1628 in PC2**

For remote diagnostics of the CP1628 in PC2 you enter the route below in Windows on the PC1.

Table 2-3

	Target IP address		Subnet	Gateway	Interface no.
route -p add	192.168.1.20	mask	255.255.255.255	192.168.0.110	if 15

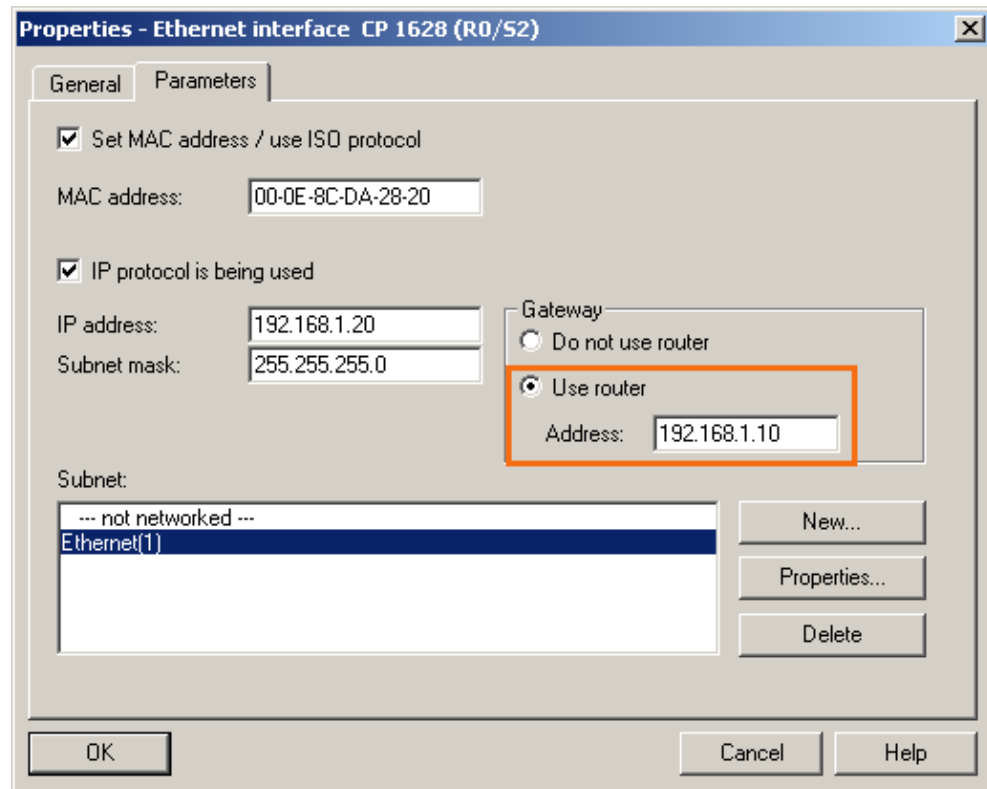
In order to perform remote diagnostics on the CP1628 in PC2 you must enter the IP address of the router in its configuration.

For this, in the STEP 7 you open the Hardware Configuration of the PC2. In the Hardware Configuration you double-click the CP1628 to open the Properties dialog of the module.

In the Properties dialog of the CP1628 you click the "Properties..." button to open the "Properties - Ethernet interface - CP1628" dialog. Here you enter the IE IP address 192.168.1.10 of the CP1628 in PC1 as gateway.



Figure 2-3



If the firewall is enabled in the CP1628 of the PC2, you must enter an allow rule in the firewall of the module for the diagnosing CP1628 in PC1.

Table 2-4 shows the allow rule required.

Table 2-4

Action	From	To	Source IP address	Destination IP address
Allow	External	Station	192.168.0.110	-. -. -. -

## 2.3 NDIS IP Address and IE IP Address of multiple CP1628s are not in the same subnet

### Overview

Figure 2-4 shows an overview of the configuration for local and remote diagnostics of a CP1628.

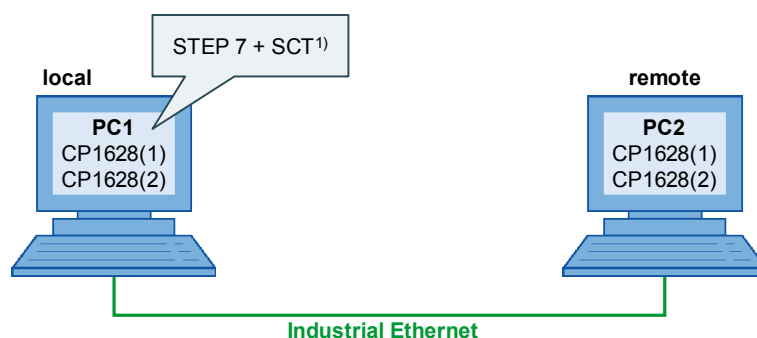
According to the Windows specifications, when using multiple network cards in one PC their NDIS IP addresses must not be in the same subnet. In this example the NDIS IP addresses of both CP1628 within one PC are in the subnet 192.168.0.x and 192.168.10.x.

Furthermore, the NDIS IP address and IE IP address of the modules are not in the same subnet.

You must enter routes in Windows on the local PC1.

In the configuration of the remote CP1628(1) and CP1628(2) you enter the IE IP address 192.168.1.10 of the diagnosing CP1628(1) in PC1 as router.

Figure 2-4



PC1 (local)	PC2 (remote)
<b>CP1628(1)</b>	<b>CP1628(1)</b>
NDIS IP address: <b>192.168.0.110</b> / 24	NDIS IP address: <b>192.168.0.220</b> / 24
IE IP address: <b>192.168.1.10</b> / 24	IE IP address: <b>192.168.1.20</b> / 24
Interface Number: 15 <sup>2)</sup>	Interface Number: 14 <sup>2)</sup>
<b>CP1628(2)</b>	<b>CP1628(2)</b>
NDIS IP address: <b>192.168.10.111</b> / 24	NDIS IP address: <b>192.168.10.221</b> / 24
IE IP address: <b>192.168.1.11</b> / 24	IE IP address: <b>192.168.1.21</b> / 24
Interface Number: 17 <sup>2)</sup>	Interface Number: 15 <sup>2)</sup>

<sup>1)</sup> The Security Configuration Tool (SCT) executes the diagnostics over the CP1628 in PC1.

<sup>2)</sup> In the Windows Console you use the command "route print interface" to detect the Interface Number.

**Local diagnostics of the CP1628(1) in PC1**

For local diagnostics of the CP1628(1) in PC1 you enter the route below in Windows on the PC1.

Table 2-5

	Target IP address		Subnet	Gateway	Interface no.
route -p add	192.168.1.10	mask	255.255.255.255	192.168.0.110	if 15

Once you enter the route the SCT can address the local IE IP address 192.168.1.10 through the NDIS IP address 192.168.0.110 that was entered as gateway and read out the data of the CP1628(1) in PC1.

If the firewall is enabled in the CP1628(1) of the PC1, there is no need to add any special rules for the module in the SCT.

**Local diagnostics of the CP1628(2) in PC1**

For local diagnostics of the CP1628(2) in PC1 you enter the route below in Windows on the PC1.

Table 2-6

	Target IP address		Subnet	Gateway	Interface no.
route -p add	192.168.1.11	mask	255.255.255.255	192.168.10.111	if 17

Once you enter the route the SCT can address the local IE IP address 192.168.1.11 through the NDIS IP address 192.168.0.111 that was entered as gateway and read out the data of the CP1628(2) in PC1.

If the firewall is enabled in the CP1628(2) of the PC1, there is no need to add any special rules for the module in the SCT.

**Remote diagnostics of the CP1628(1) in PC2**

For remote diagnostics of the CP1628(1) in PC2 you enter the route below in Windows on the PC1.

Table 2-7

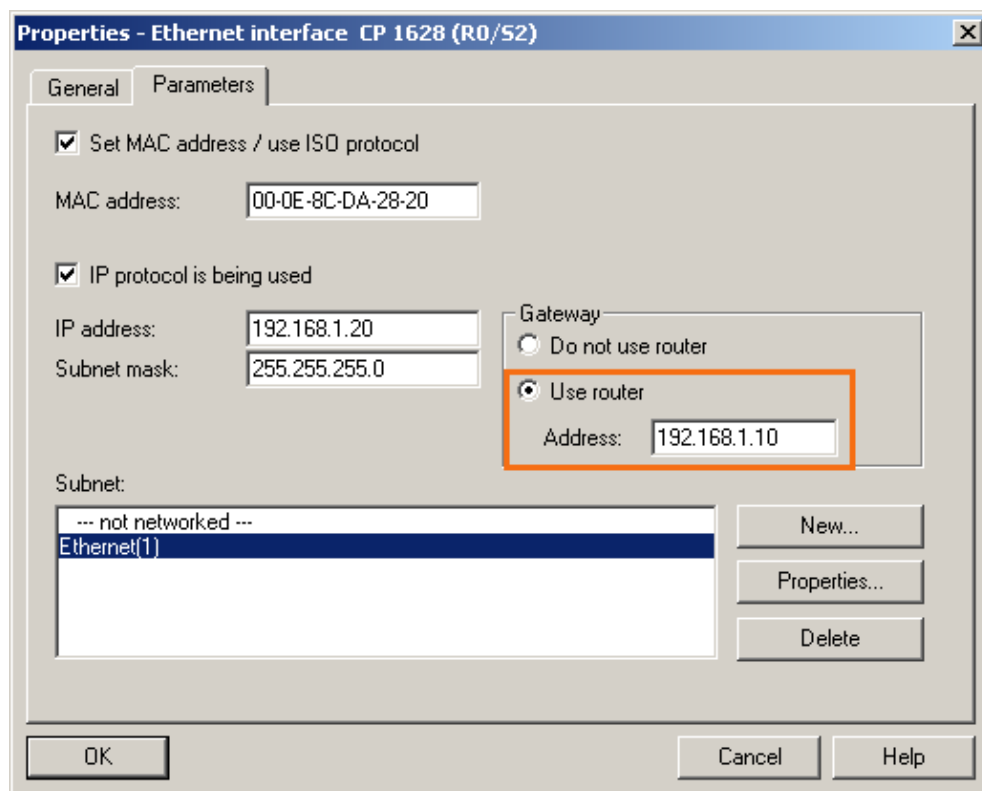
	Target IP address		Subnet	Gateway	Interface no.
route -p add	192.168.1.20	mask	255.255.255.255	192.168.0.110	if 15

In order to perform remote diagnostics on the CP1628(1) in PC2 you must enter in its configuration the IE IP address of the diagnosing CP1628(1) in PC1 as router.

For this, in the STEP 7 you open the Hardware Configuration of the PC2. In the Hardware Configuration you double-click the CP1628(1) to open the Properties dialog of the module.

In the Properties dialog of the CP1628(1) you click the "Properties..." button to open the "Properties - Ethernet interface - CP1628" dialog. Here you enter the IE IP address 192.168.1.10 of the CP1628(1) in PC1 as gateway.

Figure 2-5



If the firewall is enabled in the CP1628(1) of the PC2, you must enter an allow rule in the firewall of the module for the diagnosing CP1628(1) in PC1.

Table 2-8 shows the allow rule required.

Table 2-8

Action	From	To	Source IP address	Destination IP address
Allow	External	Station	192.168.0.110	-.-.-.-

### Remote diagnostics of the CP1628(2) in PC2

For remote diagnostics of the CP1628(2) in PC2 you enter the route below in Windows on the PC1.

Table 2-9

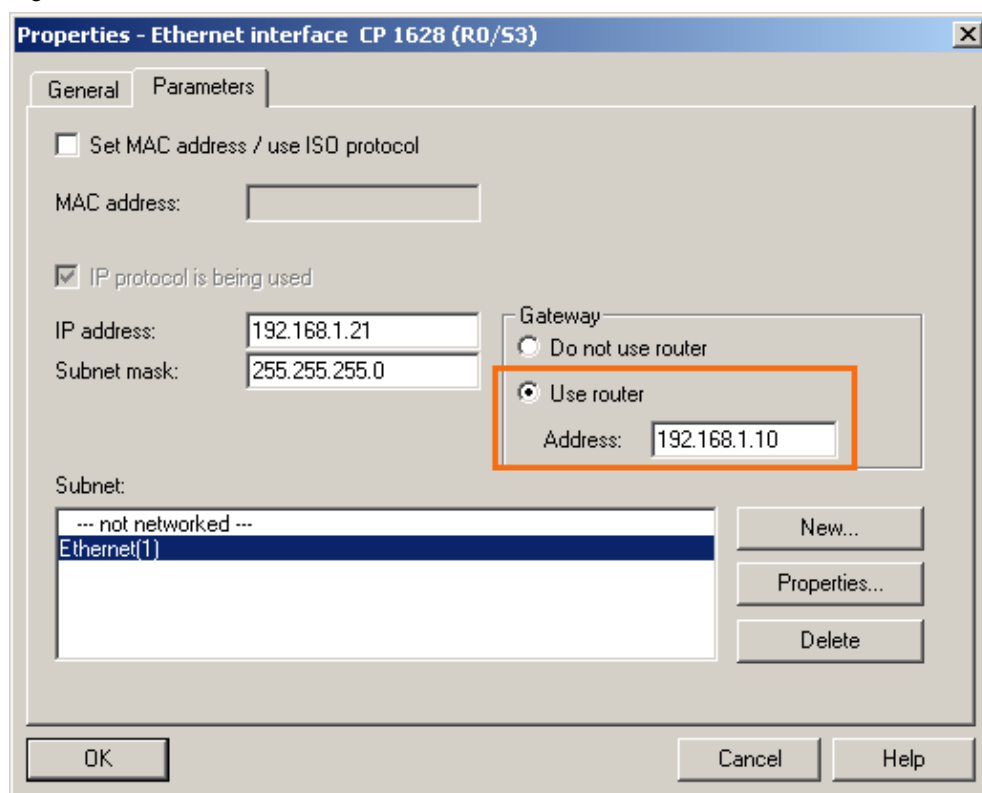
	Target IP address		Subnet	Gateway	Interface no.
route -p add	192.168.1.21	mask	255.255.255.255	192.168.0.110	if 15

In order to perform remote diagnostics on the CP1628(2) in PC2 you must enter in its configuration the IE IP address of the diagnosing CP1628(1) in PC1 as router.

For this, in the STEP 7 you open the Hardware Configuration of the PC2. In the Hardware Configuration you double-click the CP1628(2) to open the Properties dialog of the module.

In the Properties dialog of the CP1628(2) you click the "Properties..." button to open the "Properties - Ethernet interface - CP1628" dialog. Here you enter the IE IP address 192.168.1.10 of the CP1628(1) in PC1 as gateway.

Figure 2-6



If the firewall is enabled in the CP1628(2) of the PC2, you must enter an allow rule in the firewall of the module for the diagnosing CP1628(1) in PC1.

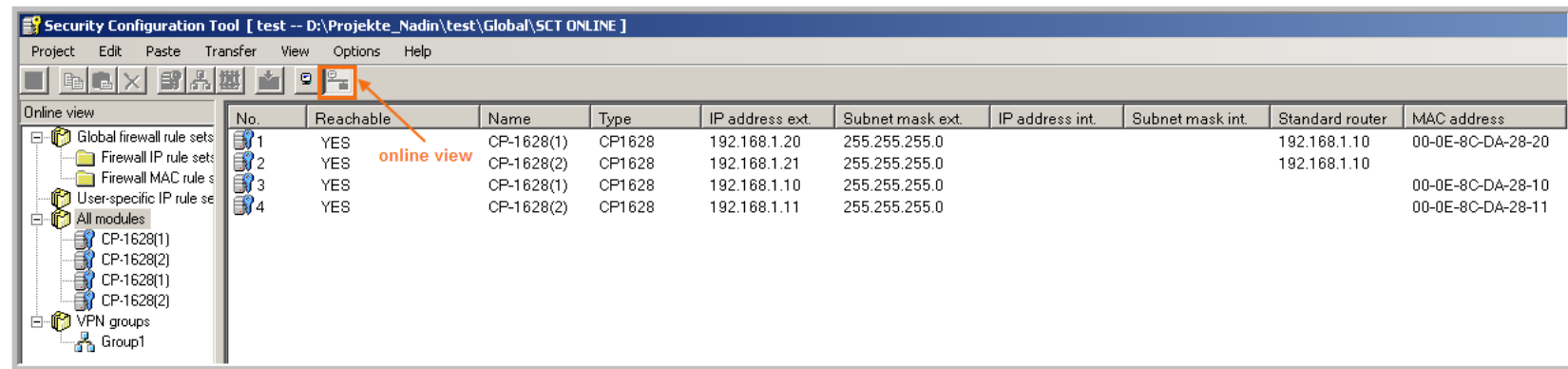
Table 2-10 shows the allow rule required.

Table 2-10

Action	From	To	Source IP address	Destination IP address
Allow	External	Station	192.168.0.110	-.-.-.-

Figure 2-7 shows the reachability of the four CP1628 in the Online view of the Security Configuration Tool.

Figure 2-7



The screenshot shows the Security Configuration Tool interface. The 'Online view' tab is active, displaying a table of four CP1628 devices. The 'Reachable' column for all devices is 'YES'. An orange arrow points to the 'Reachable' column header with the text 'online view'.

No.	Reachable	Name	Type	IP address ext.	Subnet mask ext.	IP address int.	Subnet mask int.	Standard router	MAC address
1	YES	CP-1628(1)	CP1628	192.168.1.20	255.255.255.0			192.168.1.10	00-0E-8C-DA-28-20
2	YES	CP-1628(2)	CP1628	192.168.1.21	255.255.255.0			192.168.1.10	
3	YES	CP-1628(1)	CP1628	192.168.1.10	255.255.255.0				00-0E-8C-DA-28-10
4	YES	CP-1628(2)	CP1628	192.168.1.11	255.255.255.0				00-0E-8C-DA-28-11