SecNet Labor

Practise and test industrial network security on your PC: VLANs, firewall, NAT and port forwarding

Manual · Version of 4 November 2026

For Windows · optionally with Siemens PLCSIM Advanced

PLCPrime

Contents

This manual guides you step by step through SecNet Labor: from the first start and planning a network to firewall rules, NAT and connecting real PLC simulations.

1 What is SecNet Labor? 2

2 Installation and start 3

3 The interface at a glance 4

4 Planning a network 5

5 Firewall and stateful inspection 7

6 Testing connections 9

7 Live with PLCSIM Advanced 11

8 TIA Portal through the firewall: connecting the PC 12

9 NAT 1:1: equal addresses, uniquely reachable 14

10 Port forwarding (NAPT) and OPC UA 18

11 Connecting two security switches (trunk) 21

12 Projects, examples and PDF 23

13 Troubleshooting 24

14 Notes and legal information 25

> **ABOUT THE INTERFACE**
> The interface is available in German, English and Italian. Switch the language with **DE**, **EN** or **IT** at the top of the program window. The screenshots in this manual show the interface in English.

1 What is SecNet Labor?

SecNet Labor is a practice and test program for network security in automation. Instead of real hardware, you rebuild industrial networks on your PC and try them out. You can test zone concepts and firewall rules safely, trace errors and run training sessions without putting a real plant at risk.

What you can do with it

- **Plan a network:** drag controllers, IO devices, HMI and engineering PCs, ordinary switches and security switches onto a canvas and cable them.
- **Configure the security switch:** VLANs and zones, access and trunk ports, routing, static routes, firewall rules with stateful inspection, NAT (1:1, masquerading, port forwarding), modelled on an industrial security switch.
- **Check:** a test packet shows step by step which way it takes and which rule lets it through or blocks it. The communication matrix shows who may talk to whom.
- **Live with PLCSIM Advanced:** the simulated controllers are connected and their real traffic (for example PUT/GET or OPC UA) runs through the simulated switch. What the firewall blocks really does not reach the controller.

Two modes

Mode	What it does
Model mode (without PLCSIM)	Plan and check inside the program: path tracing, matrix, configuration check. No real traffic flows.
Live mode (with PLCSIM Advanced and Npcap)	In addition, real traffic between PLCSIM instances runs through the simulated switch, with a live firewall log and live I/O on IO devices.

> **IMPORTANT**
> Siemens, TIA Portal and PLCSIM Advanced are trademarks of Siemens AG. SecNet Labor is an independent program and is not affiliated with Siemens. It is meant for learning and testing, not for use on real plants.

2 Installation and start

Requirements

What	What for	Required?
Windows with Microsoft Edge	The program opens its window with Edge (included in Windows).	yes
Siemens PLCSIM Advanced	The simulated controllers. Setting “TCP/IP Single Adapter” with `<Local>`.	live mode only
Npcap (`npcap.com`)	Lets the program forward traffic between the instances. Often already installed, for example with Wireshark.	live mode only

Starting

1. **Unzip** the ZIP file into a folder of its own. Do not start the program from inside the ZIP file.
2. Start `SecNetLabor.exe` with a double click. A window of its own opens.
3. On the first start Windows shows a warning because the program is not code-signed: click **“More info”** and then **“Run anyway”**.

Language: the program starts in the language of Windows (German or Italian; with any other language it starts in English). To change it, click **DE**, **EN** or **IT** in the header at the top of the program window. The program remembers your choice.

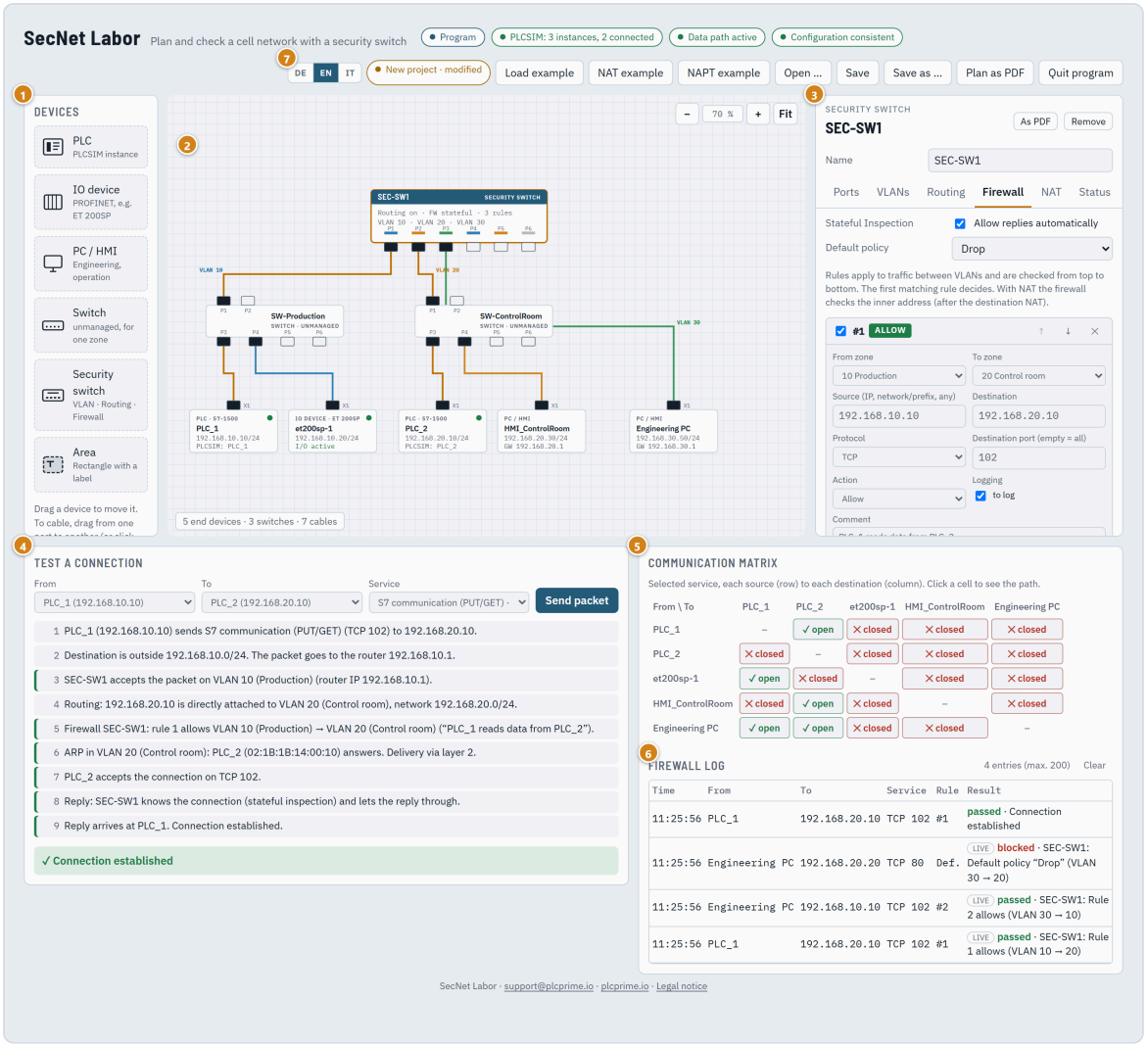
Quitting

Closing the window with the **X** does **not** quit the program: the simulated switch keeps running in the background (icon in the notification area next to the clock) so that connections do not drop. There are two ways to quit:

- Click **“Quit program”** at the top of the program window.
- Or right-click the icon in the notification area and choose **“Quit SecNet Labor”**.

> **TIP**
> After quitting there is no simulated router any more, and connections between the zones break. If you had connected the PC with “Connect PC”, the routes it created are removed automatically (see chapter 8).

3 The interface at a glance



The program window with the "Load example" scenario. The numbers are explained below.

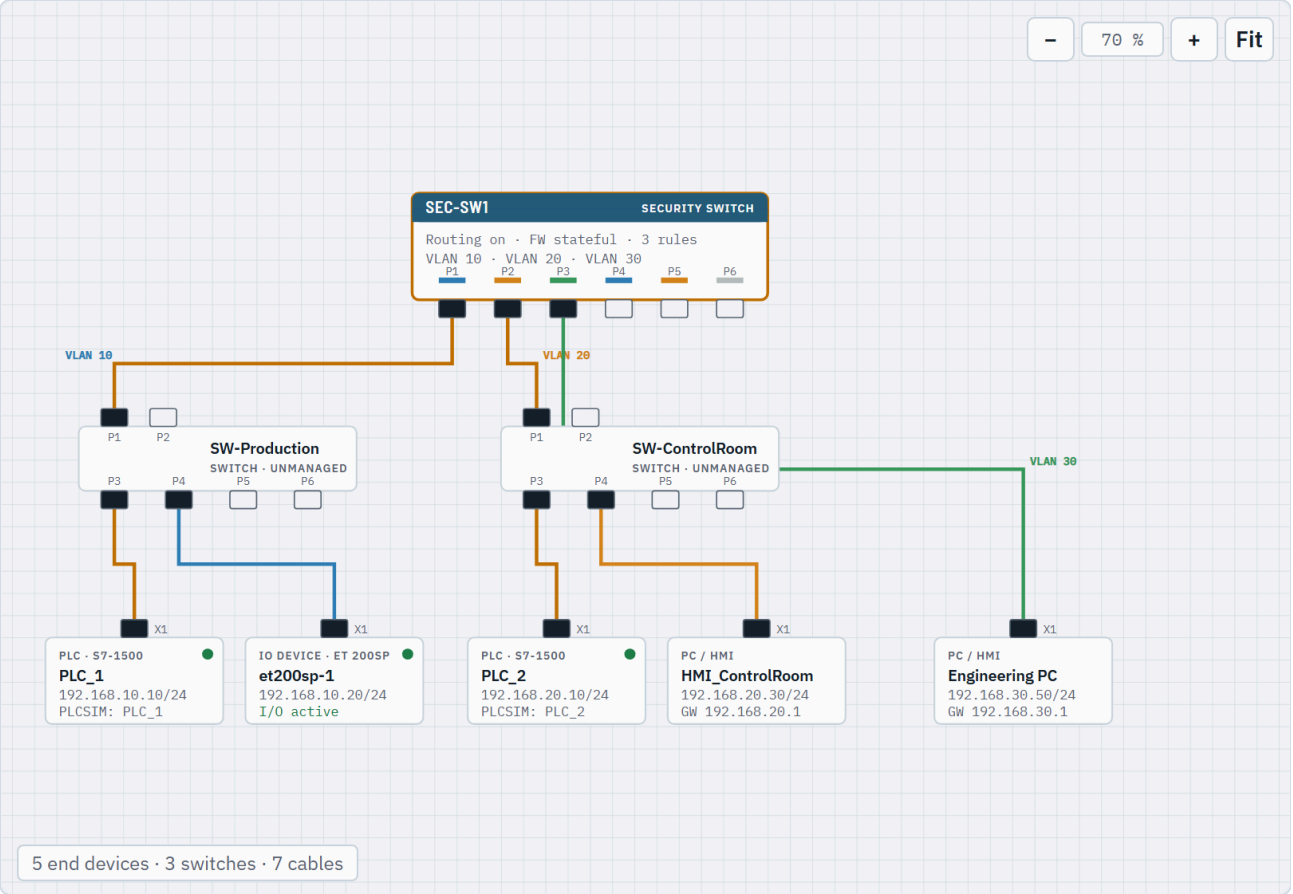
1. **Device bar:** PLC, IO device, PC/HMI, switch, security switch and area. Drag a device onto the canvas.
2. **Canvas:** this is where you build the network. Mouse wheel to zoom, drag on empty space to move the view.
3. **Inspector:** shows the settings of the selected device. For the security switch they are split into tabs.
4. **Test a connection:** choose source, destination and service, then "Send packet". The path appears step by step.
5. **Communication matrix:** who may talk to whom? Click a cell to see the path.
6. **Firewall log:** every decision of the firewall. Entries marked "LIVE" come from real traffic.
7. **Header:** switch the language (DE EN IT), load examples, open and save projects, plan as PDF, quit the program.

The status indicators at the top show the program, the PLCSIM instances and the data path. The last one, **"Configuration consistent"** or **"n hints"**, checks your plan continuously: invalid addresses, devices without a router, IP conflicts in the same segment, wrong NAT and firewall entries. Click a security switch and its "Status" tab to read the hints in plain text.

4 Planning a network

Adding and cabling devices

1. **Drag a device** from the bar on the left onto the canvas. Alternatively open an example with “Load example”.
2. **Drag from one port to another port** with the mouse to lay a cable. Clicking two ports one after the other also works.
3. Click a device: on the right, in the inspector, you set name, IP address, subnet mask and **router**. Delete the selection with the **Del** key.

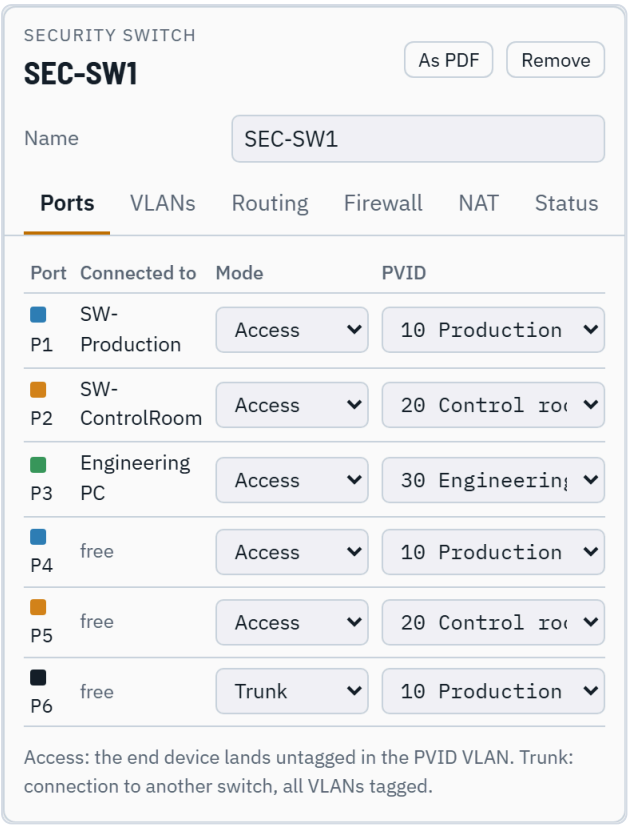


Example: two zones (production, control room) and an engineering network on one security switch. Orange and green are different VLANs.

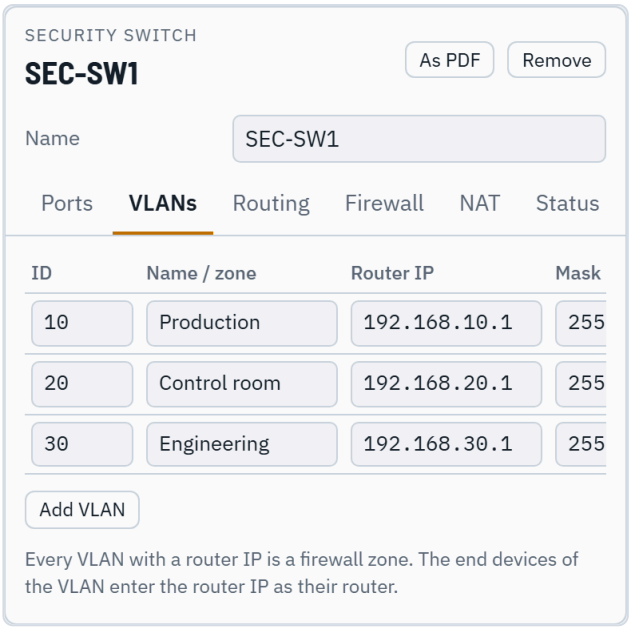
> **IMPORTANT**
> Every controller and device needs the **router** if it is to talk to another network. Enter the **router IP of the VLAN** on the security switch as the router. Otherwise the reply never comes back.

Setting up the security switch

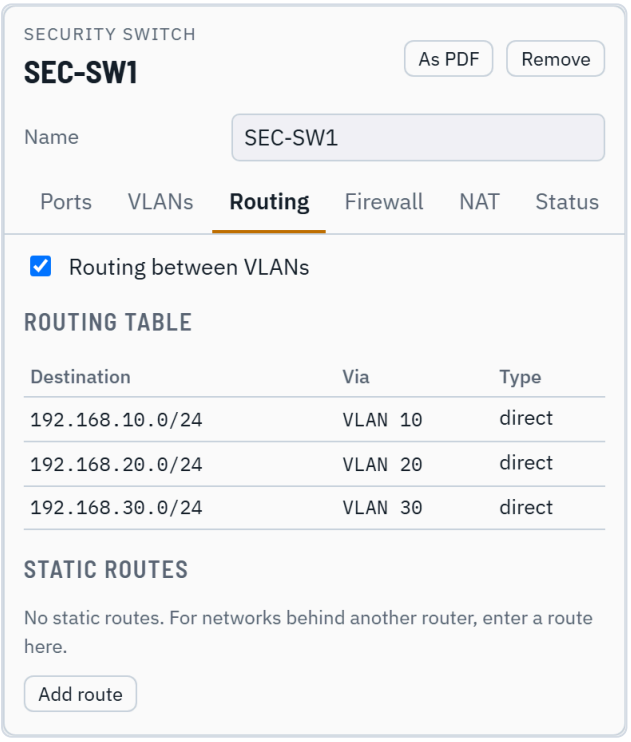
Clicking the security switch opens six tabs in the inspector (Ports, VLANs, Routing, Firewall, NAT, Status). The most important settings:



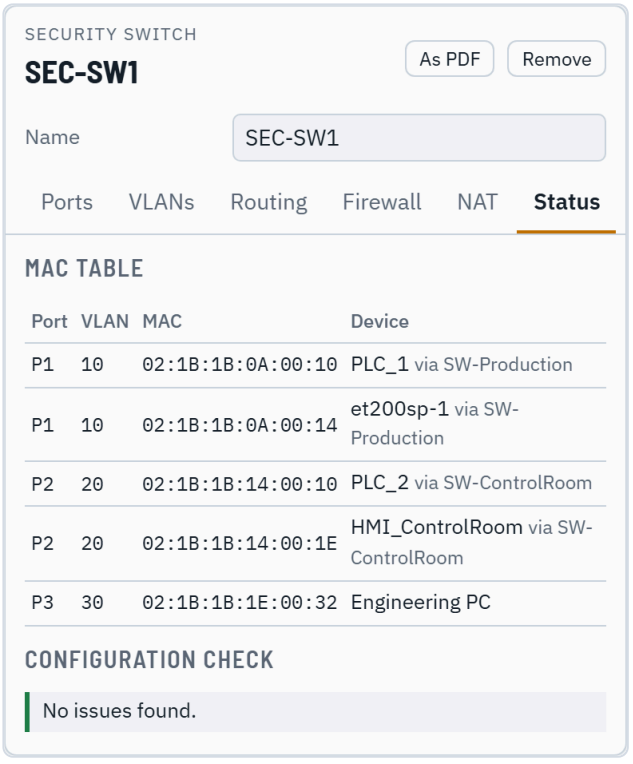
Ports: access (one VLAN) or trunk (all VLANs, for the link to another switch)



VLANs: name, router IP and mask. Every VLAN with a router IP is a firewall zone.



Routing: switch routing between the VLANs on or off, enter static routes

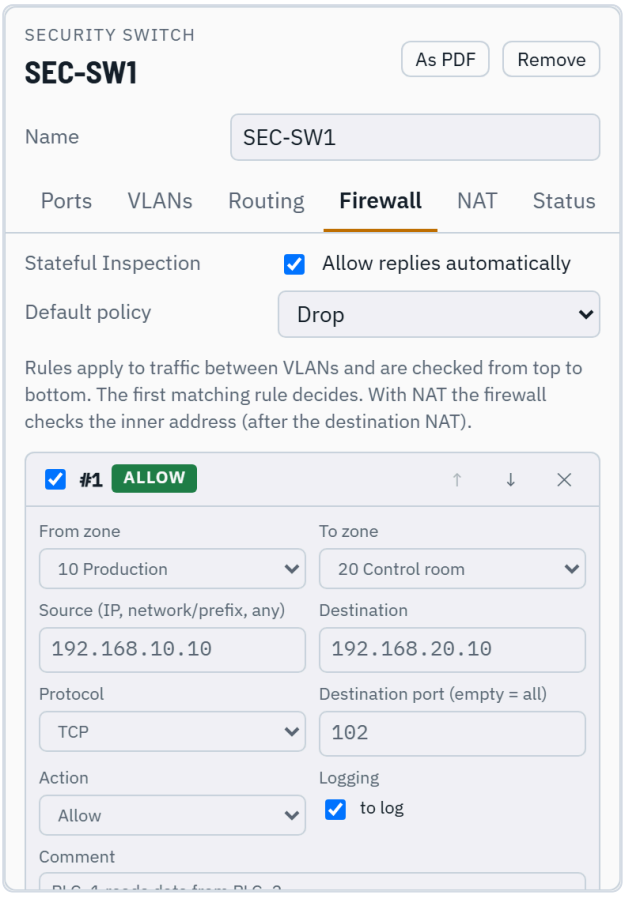


Status: connected devices with MAC address and the configuration check

With the **“Area”** tool you place coloured rectangles with a label behind your plan, for example for “plant network” or “machine 1”. This keeps larger plans readable.

5 Firewall and stateful inspection

The firewall of the security switch checks traffic **between** the VLANs. It does not check inside a VLAN. The rules are searched from top to bottom and the **first matching rule decides**. If no rule matches, the **default policy** applies (usually “Drop”).



“Firewall” tab: stateful inspection, default policy and the rules. Each rule has zones, source, destination, protocol, destination port and action.

Creating a rule

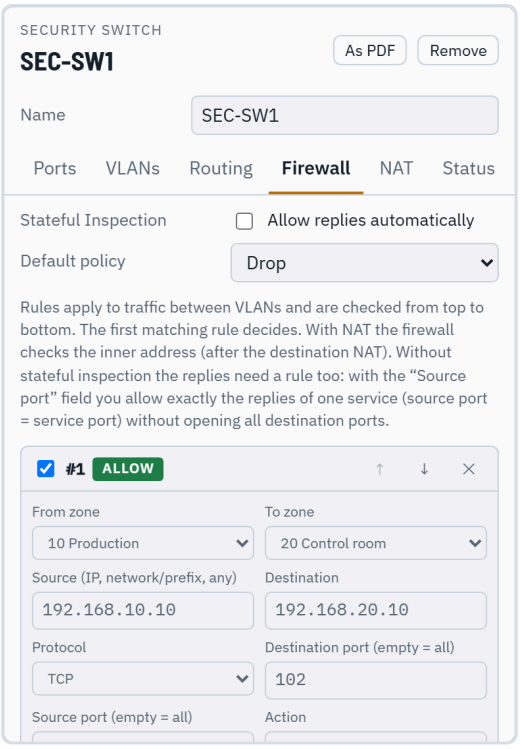
1. Click the security switch, open the **Firewall** tab and click **“Add rule”**.
2. Choose **From zone** and **To zone**, enter source and destination as an IP address, a network (for example `192.168.10.0/24`) or `any`.
3. Set **Protocol** and **Destination port** (for S7 for example TCP 102). An empty port means all ports.
4. Choose the **Action** “Allow” or “Drop”. With “Logging” ticked the decision appears in the log.

What stateful inspection means

With **stateful inspection** switched on, the firewall remembers every allowed connection and lets the **replies** back automatically. You only need a rule for the direction in which the connection is opened. If you switch stateful inspection off, traffic in the opposite direction needs a rule of its own.

The source port (advanced)

A rule can additionally require a **source port**. The field only appears where it makes sense: when stateful inspection is off or when a source port is already entered. A service's reply comes back with the service port as source port. A rule with that source port allows exactly the replies of that service without opening all destination ports.

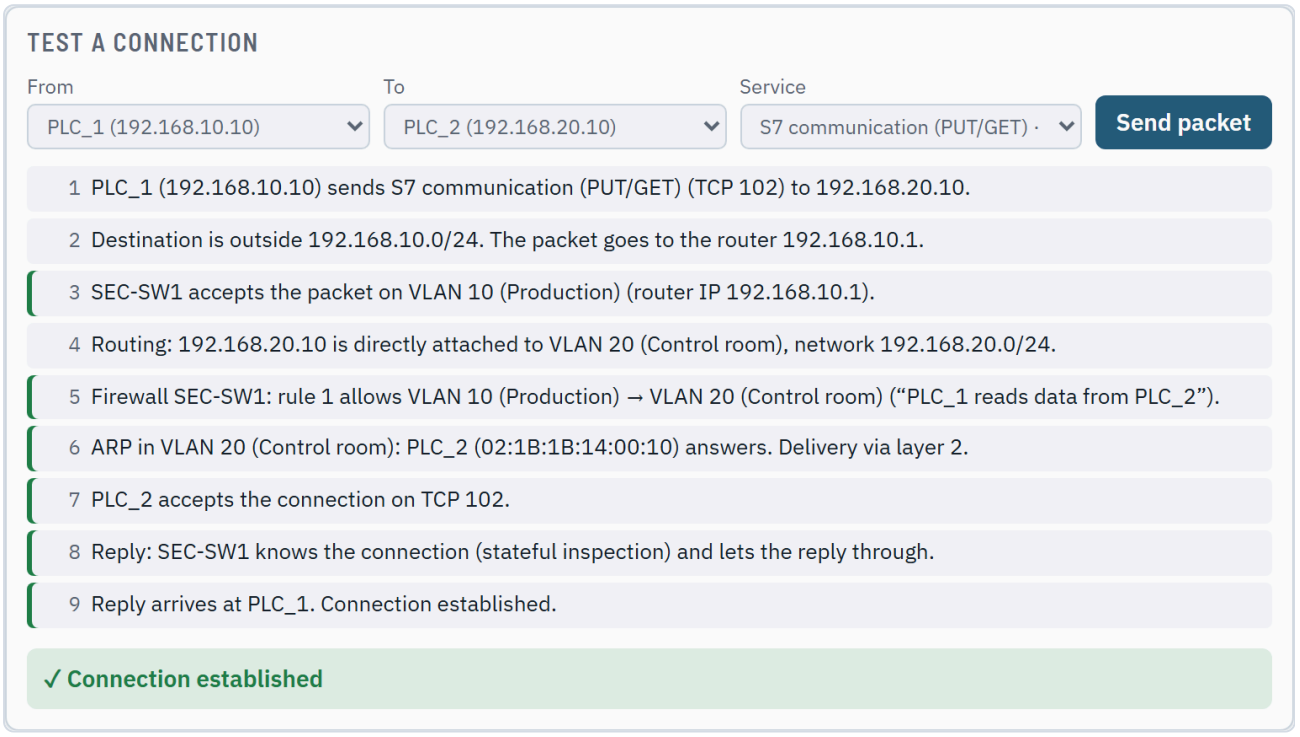


Without stateful inspection every rule shows the "Source port" field.

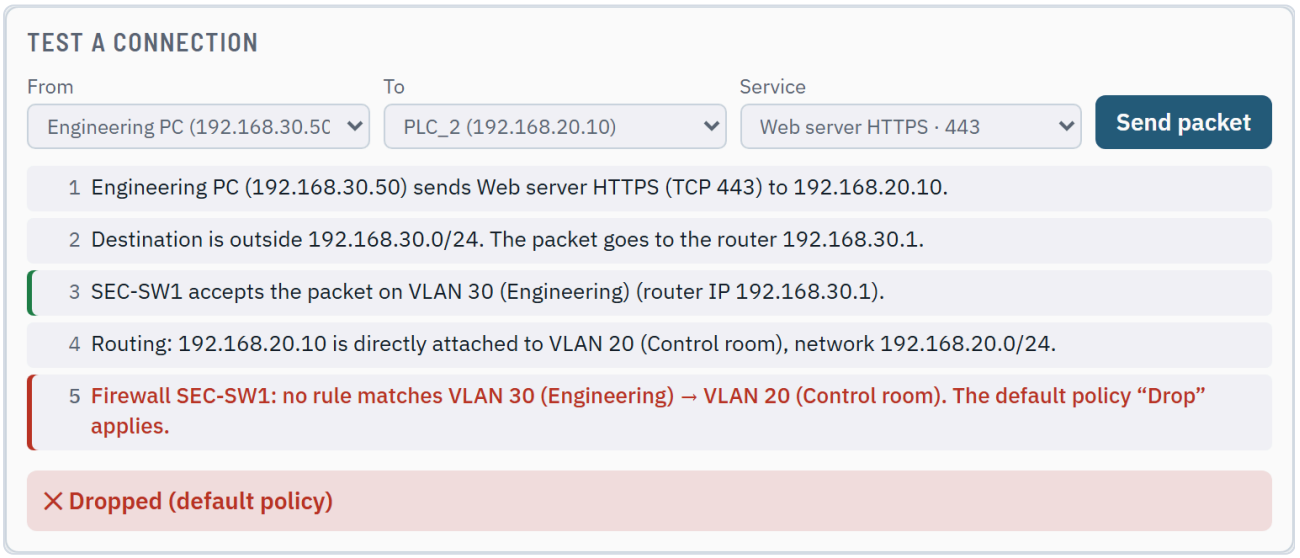
6 Testing connections

Sending a test packet

1. In **“From”** choose the sending device, in **“To”** the destination and in **“Service”** the protocol (for example S7 communication, web server, OPC UA, ping).
2. Click **“Send packet”**. Below, the path of the packet appears step by step: green for allowed steps, red for the step at which the packet dies.



The packet from PLC_1 to PLC_2 gets through: router, firewall rule 1, ARP, destination port open, reply back.



The same destination with a different service: the firewall drops the packet because no rule matches. The result is shown below the path.

The communication matrix and the log

For the selected service the **communication matrix** shows at a glance who may talk to whom (“✓ open” or “✕ closed”). Clicking a cell shows the path in the test box. The **firewall log** collects the decisions (at most 200 entries, “Clear” clears it). Rules without a tick at “Logging” do not appear there.

COMMUNICATION MATRIX

Selected service, each source (row) to each destination (column). Click a cell to see the path.

From \ To	PLC_1	PLC_2	et200sp-1	HMI_ControlRoom	Engineering PC
PLC_1	–	✓ open	✕ closed	✕ closed	✕ closed
PLC_2	✕ closed	–	✕ closed	✕ closed	✕ closed
et200sp-1	✓ open	✕ closed	–	✕ closed	✕ closed
HMI_ControlRoom	✕ closed	✓ open	✕ closed	–	✕ closed
Engineering PC	✓ open	✓ open	✕ closed	✕ closed	–

FIREWALL LOG

4 entries (max. 200) Clear

Time	From	To	Service	Rule	Result
11:25:56	PLC_1	192.168.20.10	TCP 102	#1	**passed** · Connection established
11:25:56	Engineering PC	192.168.20.20	TCP 80	Def.	LIVE **blocked** · SEC-SW1: Default policy “Drop” (VLAN 30 → 20)
11:25:56	Engineering PC	192.168.10.10	TCP 102	#2	LIVE **passed** · SEC-SW1: Rule 2 allows (VLAN 30 → 10)
11:25:56	PLC_1	192.168.20.10	TCP 102	#1	LIVE **passed** · SEC-SW1: Rule 1 allows (VLAN 10 → 20)

Matrix and log. “LIVE” marks decisions of real traffic, the other entries are tests inside the program.

> **PROFINET**
> PLCSIM Advanced does not simulate PROFINET IO. The check for IO devices therefore only rates the **plan**: are controller and IO device in the same segment and the same IP subnet? If not, the program blocks the I/O data of the IO device in live mode.

7 Live with PLCSIM Advanced

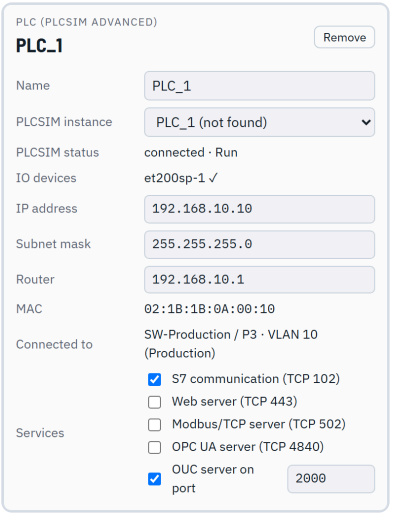
In live mode the real traffic of your PLCSIM instances runs through the simulated switch. The program acts as a router in the PLCSIM network: for every router IP of a VLAN it answers with a MAC address of its own. Packets between different subnets are routed, checked against the firewall rules (with stateful inspection) and forwarded or dropped.

Preparation

1. Set **PLCSIM Advanced** to “TCP/IP Single Adapter” with `<Local>` and start the instances. **Npcap** must be installed.
2. In **TIA Portal** enter the IP address of every PLC and set **“Use router”** to the router IP of the VLAN (as in the plan). For PUT/GET allow access by the remote partner. Download the project to the instance.
3. In **SecNet Labor** choose the **PLCSIM instance** for every PLC in the inspector. A green dot on the PLC shows the connection. An instance only ever belongs to one PLC.
4. The status line at the top should read “Data path active”.



The status indicators at the top: program, PLCSIM instances, data path and configuration check.



Inspector of a PLC: PLCSIM instance, connection status, IP address, router and services.

Example: PUT/GET between two PLCs

PLC_1 reads data from PLC_2 with GET. As long as the firewall rule is **active**, the data arrives at PLC_1. Switch the rule off and the transfer stops, and the log shows “blocked”. Switch it on again and it continues. The log shows every decision with “LIVE” and the rule that made it.

> **TIP**
> The partner address in GET/PUT is the address of the other PLC (here PLC_2). With NAT or NAPT it is the **outer address** (see chapters 9 and 10).

8 TIA Portal through the firewall: connecting the PC

The access of your engineering PC (TIA Portal) can also run through the simulated firewall. There are two ways to do this.

Option 1: two addresses on the adapter (not recommended)

In the Windows adapter “PLCSIM Virtual Ethernet” you add addresses from both networks. The PC then sits directly in both zones and talks to the PLC **past the security switch**. This is useful for downloading a project but does not test the firewall.

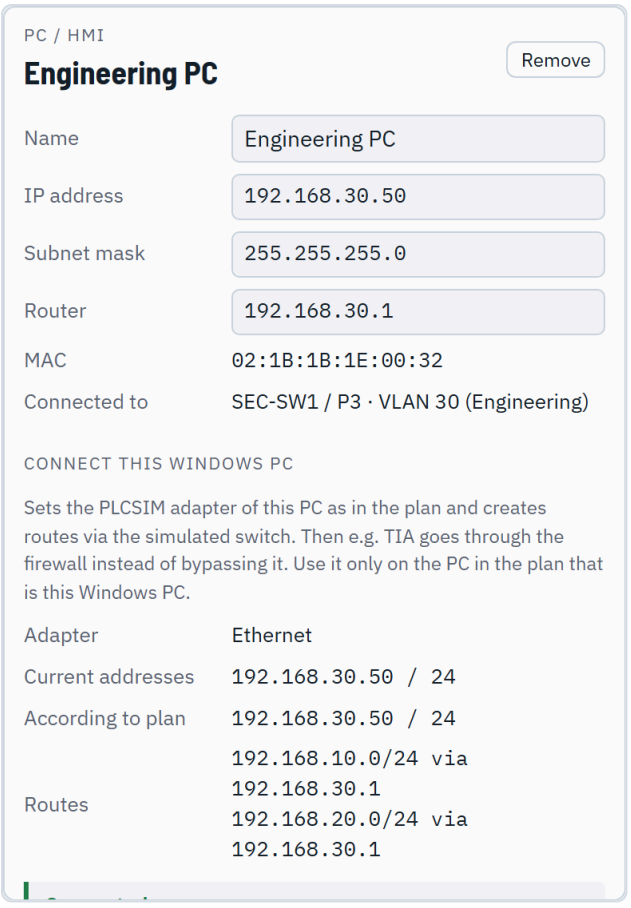
Option 2: “Connect PC” (recommended)

The Windows PC itself becomes a device in the plan (for example “Engineering PC” with IP and router). With the **“Connect PC”** button the program sets the PC’s PLCSIM adapter up as the PC appears in the plan and creates routes to the other networks. TIA then also runs through the firewall and needs matching rules (for example TCP 102 for going online and downloading, ICMP for ping).

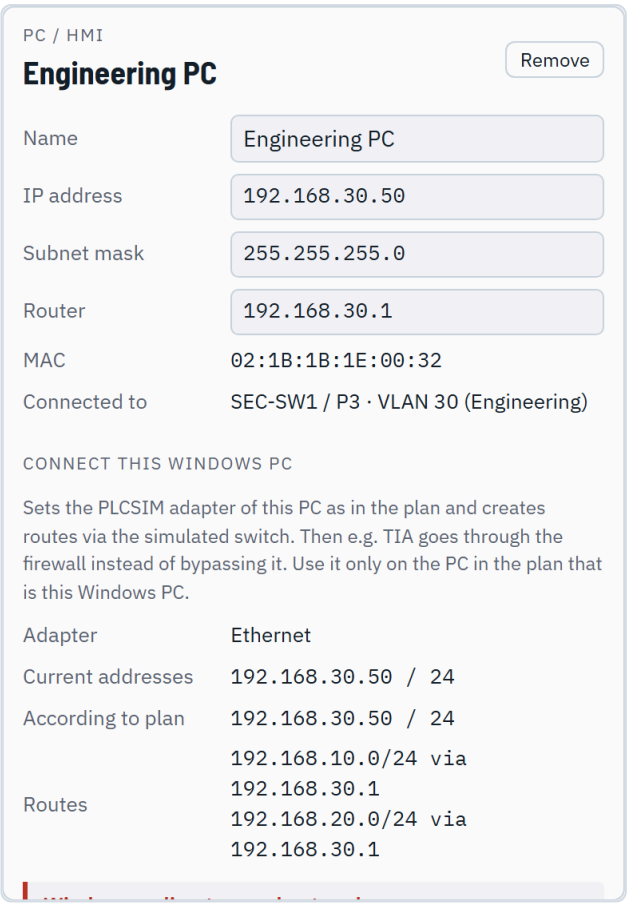
1. Click the PC in the plan (IP address and router as in the network, for example `192.168.30.50` and router `192.168.30.1`).
2. At the bottom of the inspector, under “Connect this Windows PC”, click **“Connect PC”** and confirm the Windows prompt (administrator rights).
3. **Switch the PLCSIM instances off and on once**, because their MAC address depends on the address of the adapter.
4. Go online in TIA. If TIA asks for another IP address (“Assign IP address?”), click **“No”**. Routing is active, no address needs to be added.

What happens to the routes

- Only routes for the networks of the security switch whose router the PC uses are created.
- If a network in the plan overlaps with a **real network of your PC** (for example your WLAN `192.168.1.0/24`), the program creates **no** route for it and tells you. Otherwise your real traffic would go into the simulated switch.
- **When the program quits** the routes it created are removed again (Windows asks for administrator rights). The address on the adapter stays. **“Disconnect again”** restores the state from before the first connection.



The “Connect this Windows PC” block: adapter, addresses, created route and status



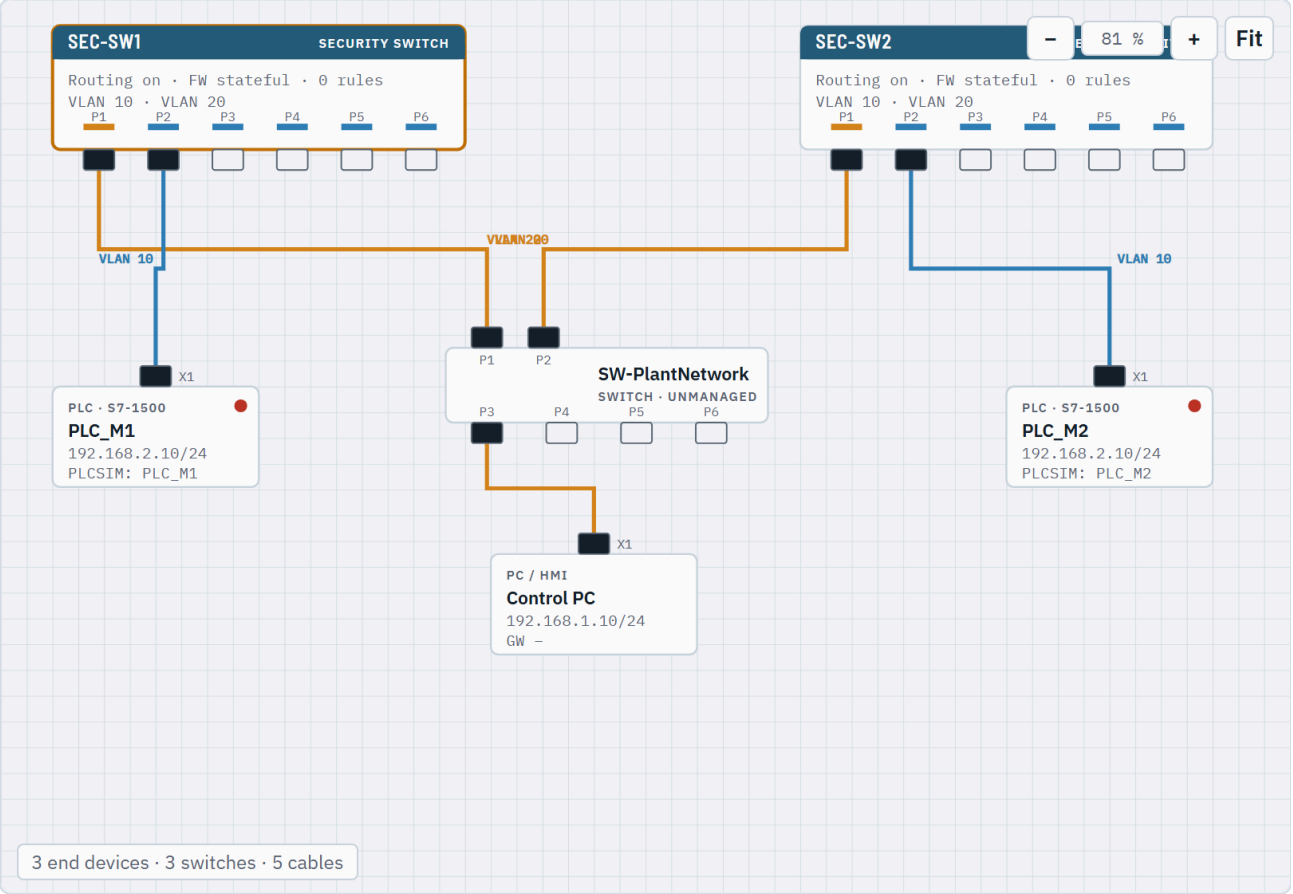
The “Windows redirects a real network” warning with the clean-up button

Checking the routes on the PC

In PowerShell with `route print -4`. After the program has quit, you should find nothing from SecNet Labor under “Persistent Routes”. If a route that redirects a real network into the simulated switch is still there, the program shows a red warning with the **“Remove conflicting routes”** button.

9 NAT 1:1: equal addresses, uniquely reachable

Controllers are often delivered with their default IP address, and it is often not changed afterwards. If a plant has several identical machines, they all have the **same address**. To make them reachable unambiguously you use **NAT**: the security switch in front of each machine gives it an address of its own towards the outside and rewrites the address in the packet.



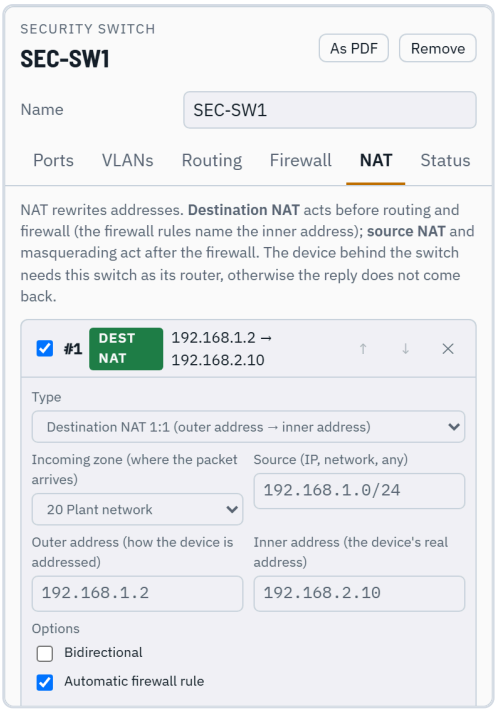
NAT example: PLC_M1 and PLC_M2 both have `192.168.20.10`. The control PC reaches them as `192.168.10.2` and `192.168.10.3`.

How it works

1. The control system sends something to `192.168.10.2` (the outer address of machine 1).
2. The switch writes the real address `192.168.20.10` as the destination into the packet and hands it to the machine. This happens **before** routing and firewall.
3. The machine replies. The switch writes `192.168.10.2` back in as the sender. The control system never notices the translation.

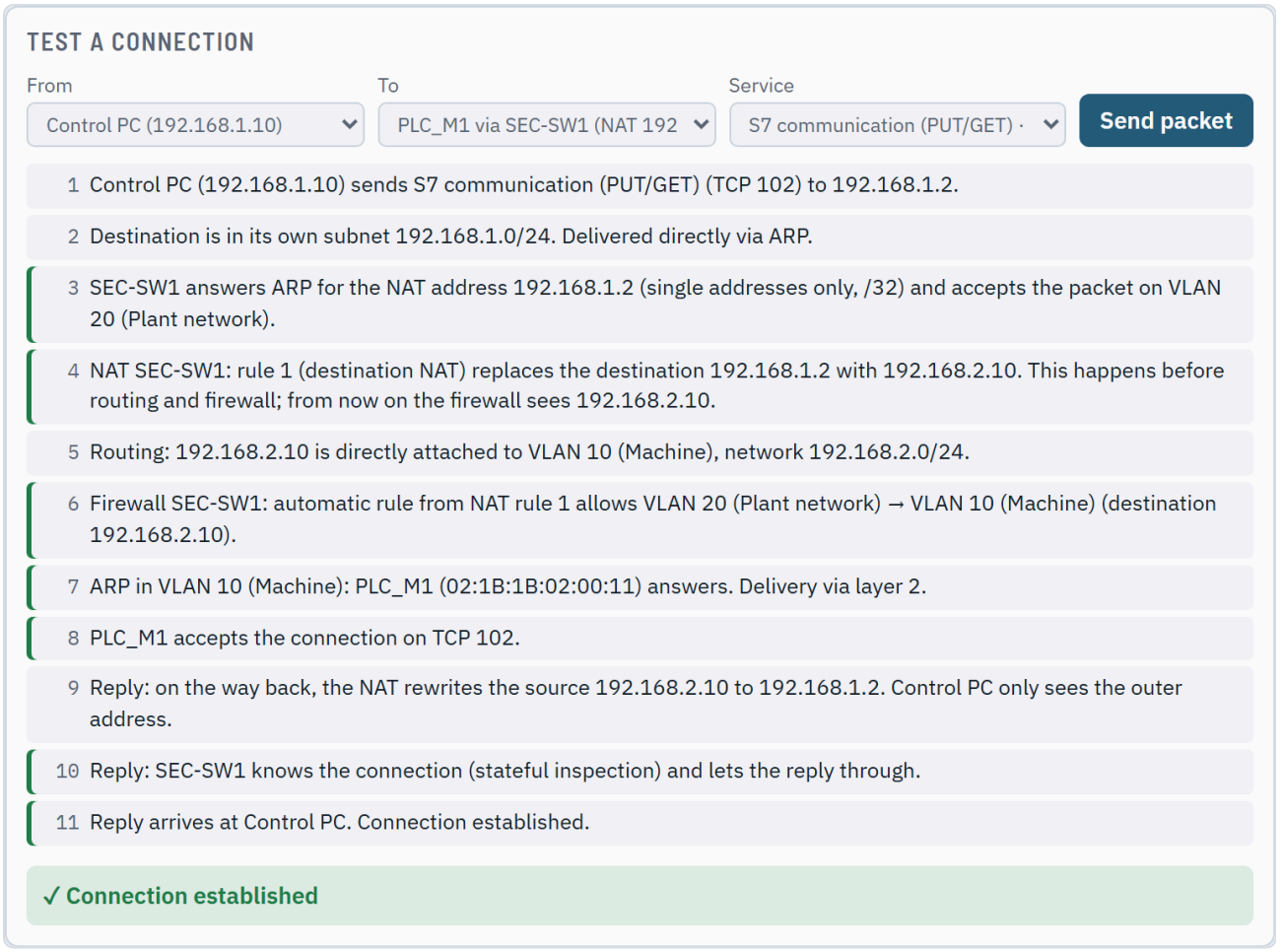
Setting up the NAT rule

Click the security switch, open the **NAT** tab, click “Add NAT rule”, type **“Destination NAT 1:1 (outer address → inner address)”**.



Destination NAT: incoming zone, source, outer address and inner address. The options “Bidirectional” and “Automatic firewall rule” are below.

Field	Meaning
Incoming zone	The packet arrives in this zone (here the plant network).
Source	Who may use the outer address (IP, network or `any`).
Outer address	How the machine is addressed from outside. A single address (`/32`) is also answered by the switch via ARP.
Inner address	The machine’s real address.
Automatic firewall rule	The switch allows the traffic to the inner address automatically. Without the tick you need a firewall rule of your own with the **inner address**.
Bidirectional	Even when the machine itself opens a connection to the outside, it appears with its outer address.



The test from “Control PC” to “PLC_M1 via SEC-SW1 (NAT 192.168.1.2)”: the switch answers ARP for the outer address and rewrites the destination.

Important with NAT

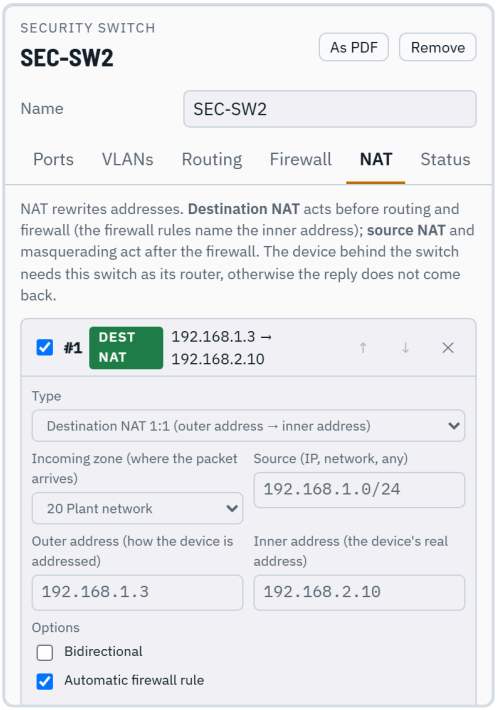
- **Router on the PLC:** the controller must have the security switch (router IP of the machine VLAN) entered as its router, otherwise the reply does not come back.
- **The firewall sees the inner address.** A rule of your own with the outer address never matches, because the destination is rewritten before the firewall.
- **In TIA** you enter the **address changed by NAT** as the partner address (for example for GET), although the PLC actually has a different one. Connections that are configured with the partner IP on both sides do not work with NAT. Use GET/PUT from one side.
- Equal IP addresses behind **different** security switches are allowed. The configuration check only reports an IP conflict in the same segment.

> **LIMIT IN LIVE MODE**
> On one PLCSIM adapter there can only be one instance per address. Two identical machines with the same IP can therefore only be shown **in the plan**. For a live test give the second machine a different inner address.

Communication between machines

If two identical machines are to talk to each other (machine 2 calls machine 1), you additionally need a **source NAT** on the switch of the calling machine. Otherwise machine 1 would see its own address as the sender. A firewall rule with the **real** source address is needed as well, because source NAT only takes effect

after the firewall.

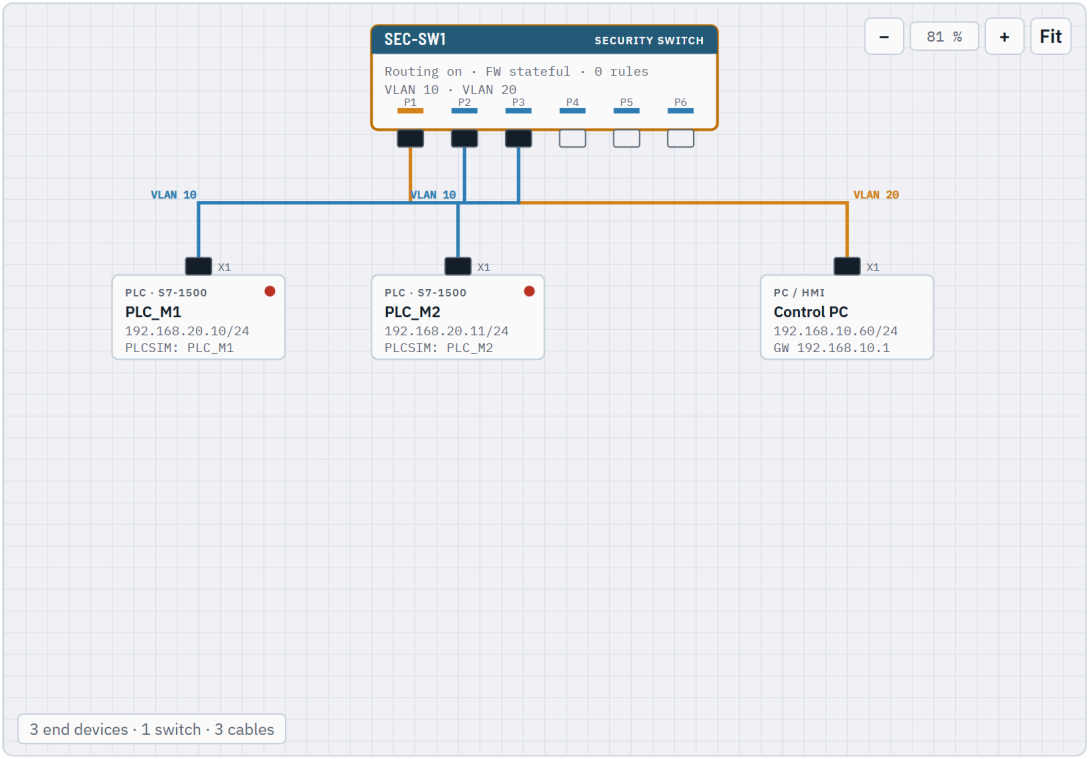


On the switch of the calling machine: source NAT from 192.168.2.10 to 192.168.1.3.

10 Port forwarding (NAPT) and OPC UA

With **NAPT** the switch has **a single outer address** (its router IP). It tells the devices behind it apart only by the **port**. The advantage: you do not need a free IP address of its own for each device, a single one is enough.

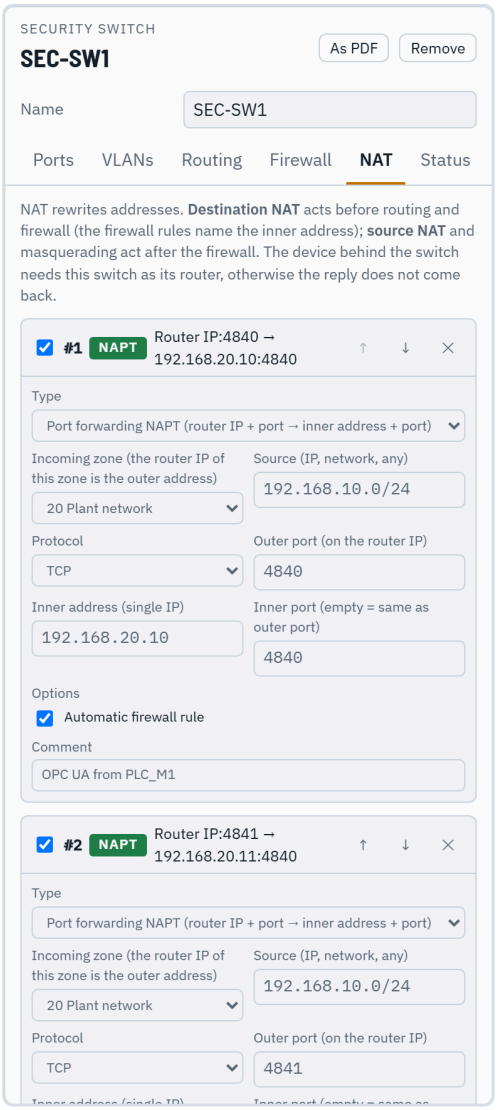
Request from outside	Forwarded to
`192.168.10.1`, port `4840`	PLC 1: `192.168.20.10`, port `4840`
`192.168.10.1`, port `4841`	PLC 2: `192.168.20.11`, port `4840`
`192.168.10.1`, port `8443`	Web server of PLC 1: `192.168.20.10`, port `443`



NAPT example: two PLCs with OPC UA behind one switch, reachable via its router IP.

The NAPT rules

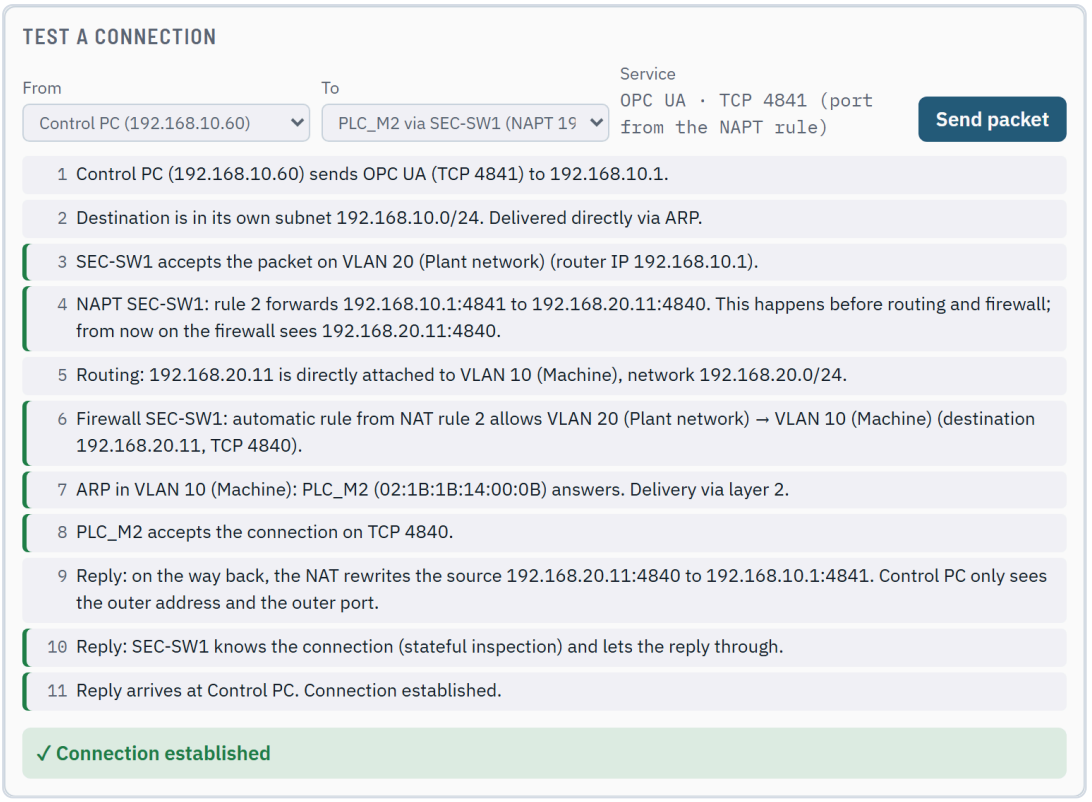
“NAT” tab, type **“Port forwarding NAPT (router IP + port → inner address + port)”**. You enter the **Outer port** (on the router IP), the **Inner address** and the **Inner port** (empty means: same as the outer port). With “Automatic firewall rule” the switch allows exactly this combination of protocol and inner port.



NAPT rules: two OPC UA servers (outer ports 4840 and 4841); the third rule (web server, 8443 to 443) follows below.

Testing

Under **“To”** there is an entry of its own for every forwarding, for example “PLC_M2 via SEC-SW1 (NAPT 192.168.10.1:4841)”. Address and port are then already correct in the test, and the service choice disappears.



Test through the forwarding: the destination is rewritten to 192.168.20.11:4840, and the firewall sees this inner address with the inner port.

OPC UA with UA Expert (live)

1. In TIA **activate the OPC UA server** on the PLC, enter address and router as in the plan and download. Assign the instance in SecNet Labor.
2. Connect the PC (chapter 8) and switch the instances off and on.
3. In UA Expert enter the **router IP of the switch** as the server: `opc.tcp://192.168.10.1:4840`. Not the address of the PLC.
4. The firewall log shows “NAPT: 192.168.10.1:4840 → 192.168.20.10:4840”. UA Expert finds the PLC and shows its application.

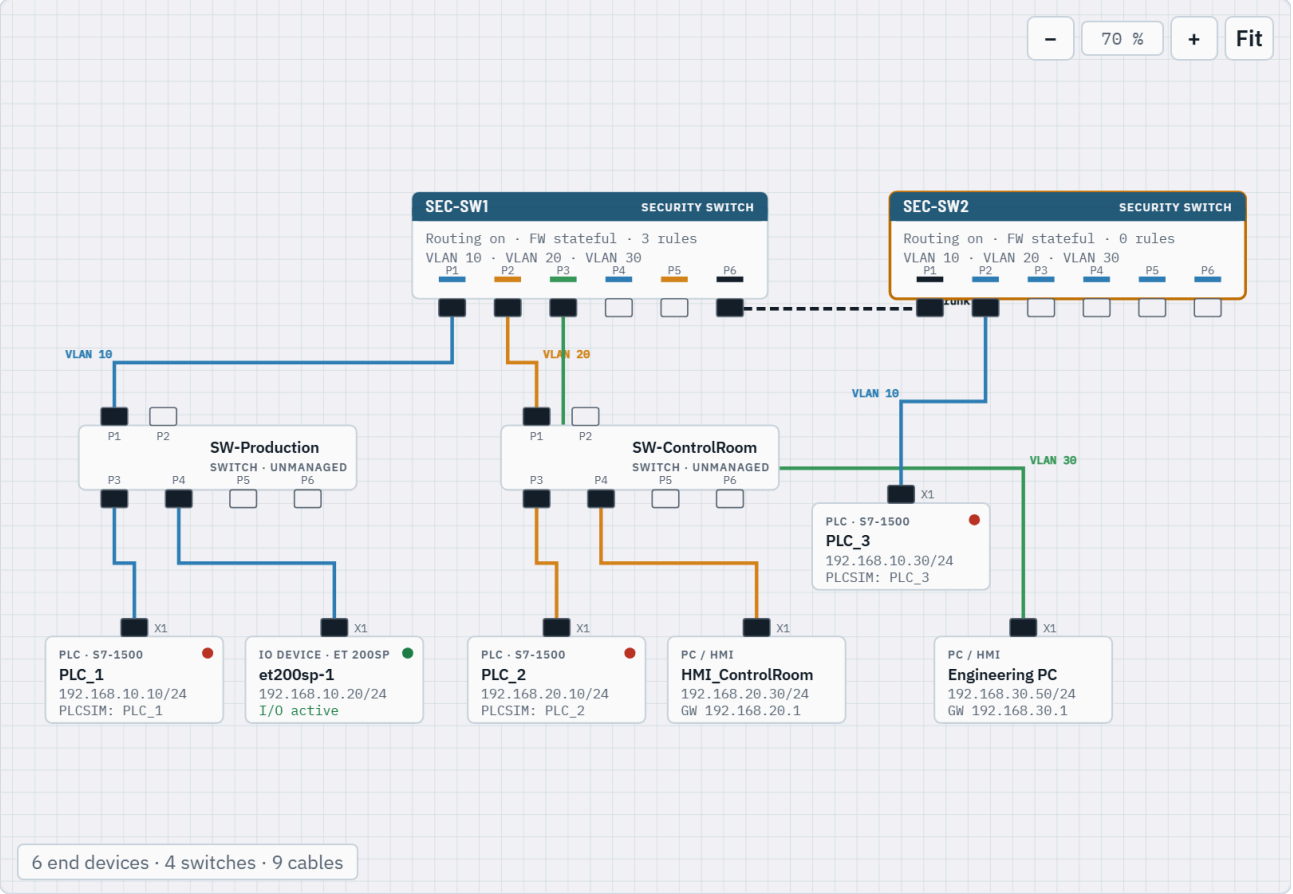
> **GOOD TO KNOW**
> The PLC reports **its own** address (`192.168.20.10`) to the client as the endpoint. UA Expert therefore often opens the actual session directly to that address. This works if the PC has a route into the machine network (as after “Connect PC”). That session then runs routed normally through the firewall, without NAPT. In the log you recognise it because the entry appears **without** the NAPT note. In real plants without a route into the machine network you have to adjust the endpoint on the client or on the PLC.

Limits of NAPT

- Every outer port can only be forwarded once. A forwarded port can no longer be used on the switch itself (for example 443 for its web management).
- Services with a **fixed port**, for example S7 (port 102), can only be forwarded for **one** device over **one** address. For several identical machines with S7 use 1:1 NAT.

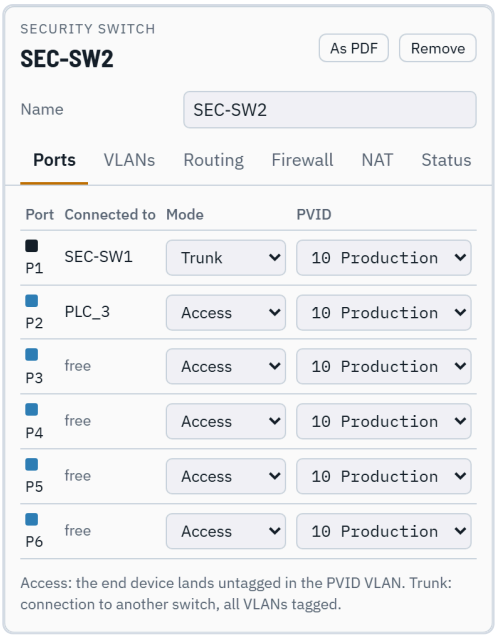
11 Connecting two security switches (trunk)

Two security switches can be connected through a **trunk**. All VLANs run tagged on the trunk. This lets a PLC on the second switch sit in the same network as a PLC on the first.



SEC-SW1 and SEC-SW2 are connected through a trunk (dashed). PLC_3 is on VLAN 10 of the second switch and talks to PLC_1 on the first.

1. On **both** switches set the port of the link to **trunk** in the “Ports” tab and enable it.
2. Connect the two trunk ports with a cable.
3. Create the same VLANs on the second switch (same ID). The **router IP stays empty** there (“Layer 2 only”). The router of the network remains the first switch.
4. The PLC on the second switch gets an address from the VLAN’s network and the router IP of the **first** switch as its router.

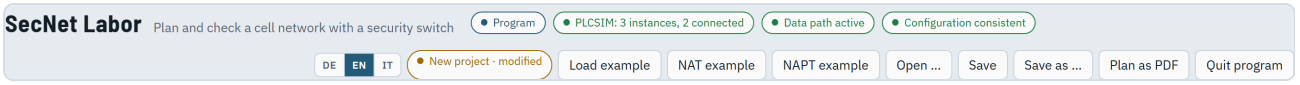


Ports of the second switch: P1 is the trunk, the others are access ports in VLAN 10.

TIP

The router IP for switch 2 must stay free. Two devices with the same router IP in the same network would cause an IP conflict.

12 Projects, examples and PDF



The header: examples, projects, PDF output and quit.

Button	What it does
Load example	A ready-made network with three zones, two PLCs and a firewall.
NAT example	Two identical machines with the same address, each behind its own security switch, reachable through NAT.
NAPT example	Two PLCs with OPC UA behind one outer address, reachable through different ports.
Open ..., Save, Save as ...	Projects as a `.json` file with the Windows dialogs (Ctrl+S saves). The plan is also kept in the program and is there again at the next start.
Plan as PDF	The network plan on page 1 (A4 landscape), then the list of devices and areas.
As PDF (on the security switch)	All settings of the switch on A4: ports, VLANs, routing, firewall rules, NAT, connected devices and configuration check.

> **NOTE**
> The program creates the PDF files in the background with Edge. This can take a few seconds. Then the file opens.

13 Troubleshooting

Problem	Possible cause and solution
The packet is “Dropped (default policy)”	No rule matches. In the Firewall tab create a rule with the right zones, addresses and destination port. With NAT the **inner address** counts.
The path ends with “Return path missing” or “PLC_2 without router” (with the name of the device)	The destination device has no router. Enter the router IP of the VLAN (in TIA too: “Use router”).
The PLC has a red dot	No PLCSIM instance chosen or the instance is not running. Choose the instance in the inspector, start it in PLCSIM.
“Data path off” at the top	Npcap is missing or the PLCSIM adapter was not found. Install Npcap, set PLCSIM to “TCP/IP Single Adapter” with `<Local>`.
TIA does not find the PLC	When downloading choose “Extended download”, as the interface the PLCSIM Virtual Ethernet Adapter, and enter the IP by hand. The PC adapter needs an address in the PLC’s network. Then switch the instances off and on. Check for old routes (`route print -4`).
The log keeps showing “blocked” for TCP 102	TIA asks for the PLC regularly and port 102 is not allowed. Create a rule for TCP 102 or end the online connection in TIA.
After “Connect PC” WLAN or internet is disturbed	A route redirects a real network into the switch. Click “Remove conflicting routes” at the PC or quit the program. Check with `route print -4`.
NAT: no connection	Router entered on the PLC? Source in the NAT rule matches? Outer address as a single address (`/32`)? Firewall rule with the **inner address** or “Automatic firewall rule”?
NAPT/OPC UA finds nothing	Enter the router IP of the switch and the **outer port**, not the PLC’s address. Rule switched on? Protocol TCP? OPC UA server active in the PLC?
The program window is empty or does not respond	Reload with **Ctrl+R**. If that does not help, quit the program and start it again.

SUPPORT

For questions or errors you can reach us at **support@plcprime.io**. Please include a screenshot and the entry from the firewall log.

14 Notes and legal information

- **Trademarks:** Siemens, TIA Portal, SIMATIC and PLCSIM Advanced are trademarks of Siemens AG. SecNet Labor is an independent program by PLCPrime and is not affiliated with Siemens.
- **Use:** the program is provided without warranty and used at your own risk. It is meant for learning and testing and not for use on real plants.
- **Npcap:** live mode needs Npcap. It is not part of the package, you install it yourself from `npcap.com`. The licence terms of Npcap apply to your use.
- **Privacy:** the program only listens on your own computer (`127.0.0.1`), needs no internet connection and transmits no data. The fonts are included in the program (SIL Open Font License).
- **System changes:** “Connect PC” changes the address of the PLCSIM adapter and creates routes. Windows asks for administrator rights for this. When the program quits the routes are removed again.

Contact: support@plcprime.io · plcprime.io · Legal notice