SecNet Labor

Industrielle Netzwerksicherheit am PC üben und testen: VLANs, Firewall, NAT und Port-Weiterleitung

Handbuch · Stand 04.11.2026

Für Windows · optional mit Siemens PLCSIM Advanced

PLCPrime

Inhalt

Dieses Handbuch führt Sie Schritt für Schritt durch SecNet Labor: vom ersten Start über das Planen eines Netzes bis zu Firewall-Regeln, NAT und der Anbindung echter SPS-Simulationen.

1 Was ist SecNet Labor? 2

2 Installation und Start 3

3 Die Oberfläche im Überblick 4

4 Ein Netz planen 5

5 Firewall und Stateful Inspection 7

6 Verbindungen testen 9

7 Live mit PLCSIM Advanced 11

8 TIA Portal durch die Firewall: PC anbinden 12

9 NAT 1:1: gleiche Adressen, eindeutig erreichbar 14

10 Port-Weiterleitung (NAPT) und OPC UA 18

11 Zwei Security-Switches verbinden (Trunk) 21

12 Projekte, Beispiele und PDF 23

13 Fehlersuche 24

14 Hinweise und Rechtliches 25

> **ÜBER DIE OBERFLÄCHE**
> Die Oberfläche gibt es auf Deutsch, Englisch und Italienisch. Die Sprache stellen Sie mit **DE**, **EN** oder **IT** oben im Programmfenster um. Die Bilder in diesem Handbuch zeigen die Oberfläche auf Deutsch.

1 Was ist SecNet Labor?

SecNet Labor ist ein Übungs- und Testprogramm für Netzwerksicherheit in der Automatisierungstechnik. Statt mit echter Hardware bauen Sie Industrienetze am PC nach und probieren sie aus. Sie können Zonenkonzepte und Firewall-Regeln gefahrlos testen, Fehler nachvollziehen und Schulungen durchführen, ohne eine reale Anlage zu gefährden.

Was Sie damit tun können

- **Netz planen:** Steuerungen, IO-Devices, HMI- und Engineering-PCs, normale Switches und Security-Switches auf eine Fläche ziehen und verkabeln.
- **Security-Switch einrichten:** VLANs und Zonen, Access- und Trunk-Ports, Routing, statische Routen, Firewall-Regeln mit Stateful Inspection, NAT (1:1, Maskierung, Port-Weiterleitung). Das Vorbild ist ein industrieller Security-Switch.
- **Prüfen:** Ein Testpaket zeigt Schritt für Schritt, welchen Weg es nimmt und welche Regel es durchlässt oder sperrt. Die Kommunikationsmatrix zeigt, wer mit wem sprechen darf.
- **Live mit PLCSIM Advanced:** Die simulierten Steuerungen werden angebunden, und ihr echter Datenverkehr (zum Beispiel PUT/GET oder OPC UA) läuft durch den simulierten Switch. Was die Firewall sperrt, kommt bei der Steuerung tatsächlich nicht an.

Zwei Betriebsarten

Betriebsart	Was geht
Modellmodus (ohne PLCSIM)	Planen und Prüfen im Programm: Wegeverfolgung, Matrix, Konfigurationsprüfung. Es fließt kein echter Datenverkehr.
Live-Modus (mit PLCSIM Advanced und Npcap)	Zusätzlich echter Datenverkehr zwischen PLCSIM-Instanzen durch den simulierten Switch, Live-Firewall-Log, Live-E/A an IO-Devices.

> **WICHTIG**
> Siemens, TIA Portal und PLCSIM Advanced sind Marken der Siemens AG. SecNet Labor ist ein unabhängiges Programm und nicht mit Siemens verbunden. Es dient zum Lernen und Testen, nicht für den Einsatz an echten Anlagen.

2 Installation und Start

Voraussetzungen

Was	Wofür	Pflicht?
Windows mit Microsoft Edge	Das Programm öffnet sein Fenster mit Edge (ist in Windows enthalten).	ja
Siemens PLCSIM Advanced	Die simulierten Steuerungen. Einstellung „TCP/IP Single Adapter“ mit `<Local>`.	nur für den Live-Modus
Npcap (`npcap.com`)	Damit das Programm den Datenverkehr zwischen den Instanzen weiterleiten kann. Oft schon vorhanden, zum Beispiel mit Wireshark installiert.	nur für den Live-Modus

Starten

1. Die ZIP-Datei in einen **eigenen Ordner entpacken**. Nicht aus der ZIP-Datei heraus starten.
2. `SecNetLabor.exe` per Doppelklick starten. Es öffnet sich ein eigenes Fenster.
3. Beim ersten Start warnt Windows, weil das Programm nicht signiert ist: auf **„Weitere Informationen“** und dann auf **„Trotzdem ausführen“** klicken.

Sprache: Das Programm startet in der Sprache von Windows (Deutsch oder Italienisch; bei jeder anderen Sprache auf Englisch). Zum Umstellen oben in der Kopfzeile des Programmfensters auf **DE**, **EN** oder **IT** klicken. Das Programm merkt sich die Wahl.

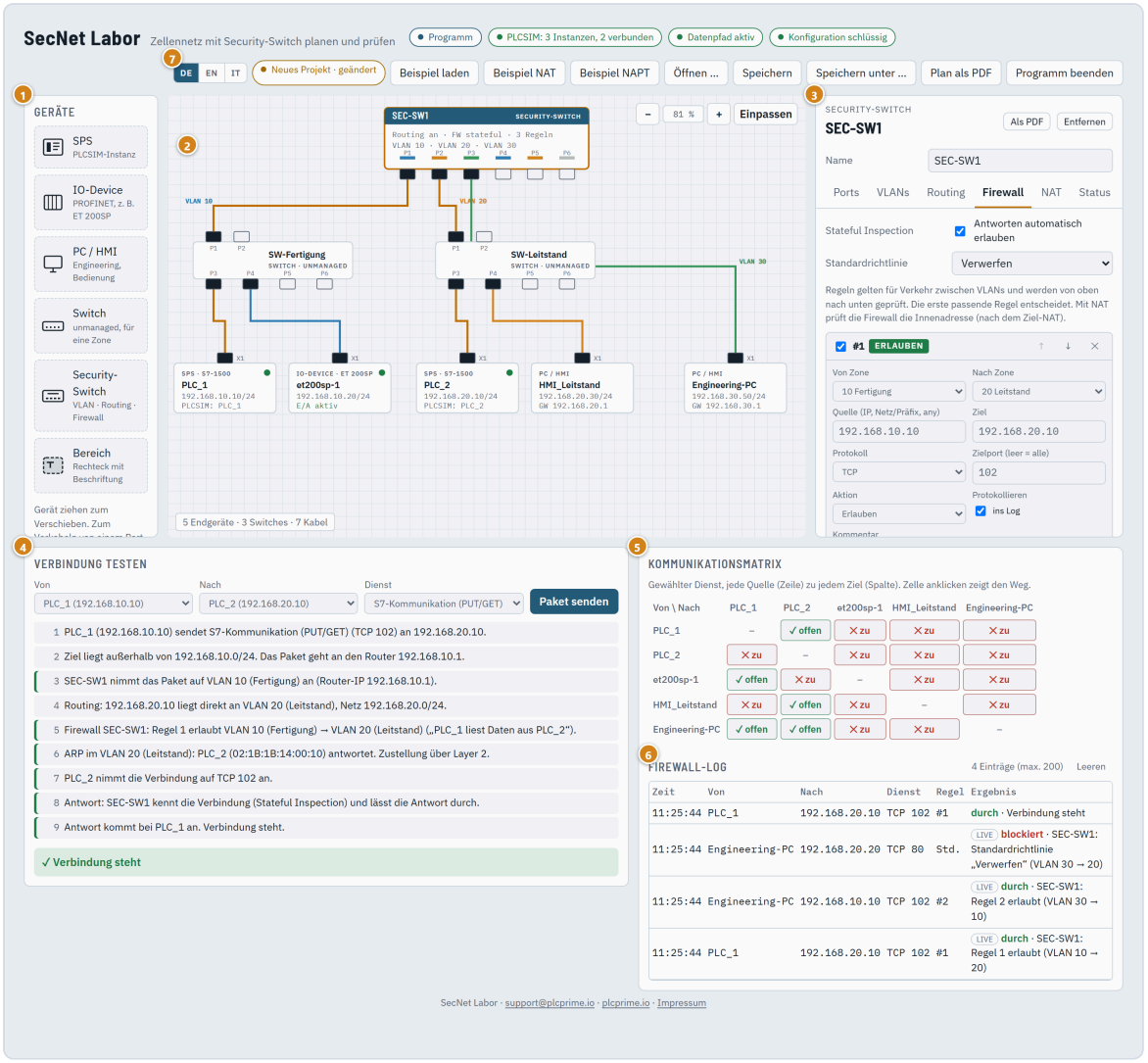
Beenden

Das Schließen des Fensters mit dem **X** beendet das Programm **nicht**: Der simulierte Switch läuft im Hintergrund weiter (Symbol im Infobereich neben der Uhr), damit Verbindungen nicht abbrechen. Zum Beenden gibt es zwei Wege:

- Im Programmfenster oben auf **„Programm beenden“** klicken.
- Oder im Infobereich mit der rechten Maustaste auf das Symbol und **„SecNet Labor beenden“** wählen.

> **TIPP**
> Nach dem Beenden gibt es keinen simulierten Router mehr. Verbindungen zwischen den Zonen brechen dann ab. Wenn Sie den PC über „PC anbinden“ eingebunden hatten, werden die angelegten Routen dabei automatisch entfernt (siehe Kapitel 8).

3 Die Oberfläche im Überblick



Das Programmfenster mit dem Beispiel „Beispiel laden". Die Nummern sind unten erklärt.

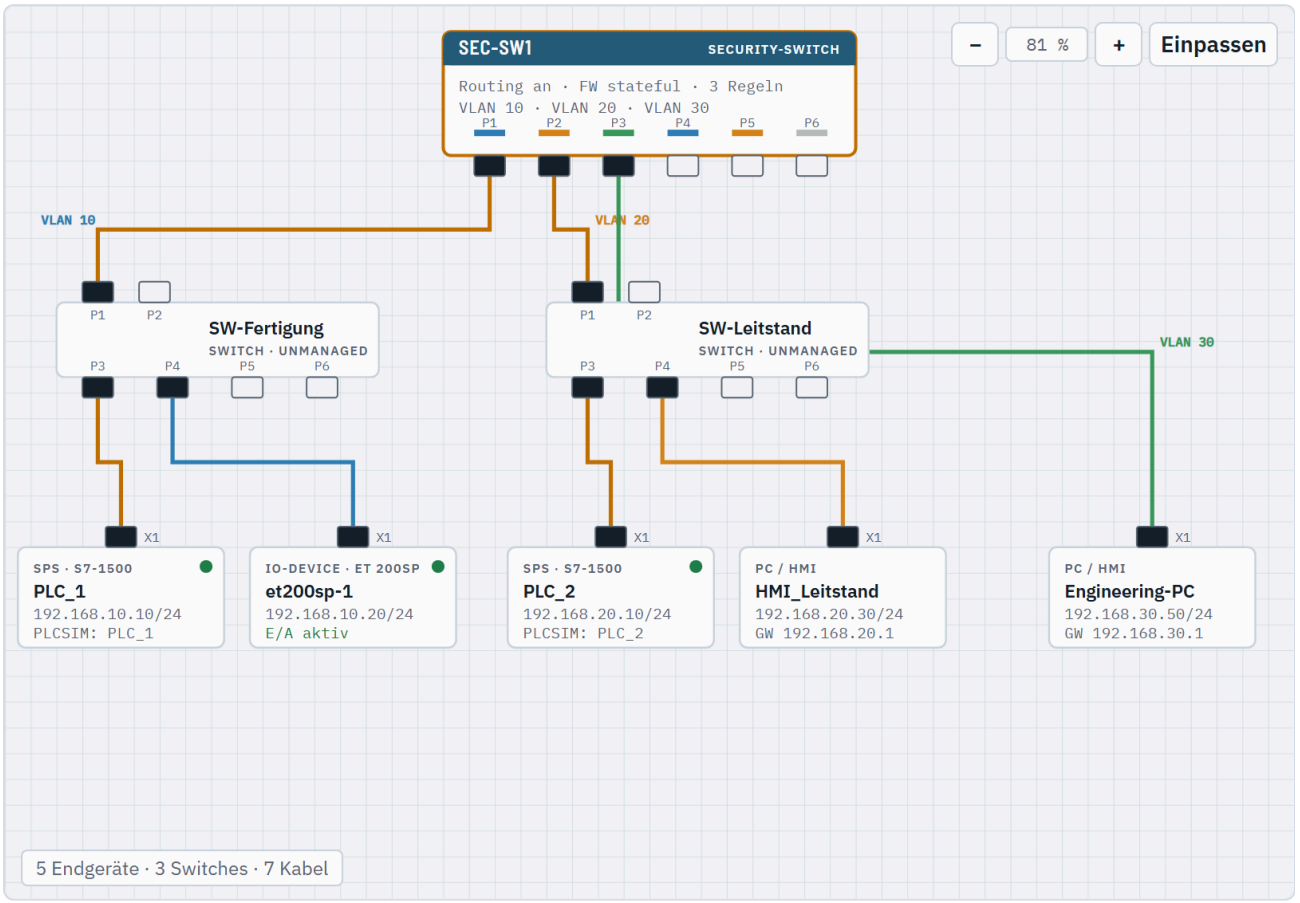
1. **Geräteleiste:** SPS, IO-Device, PC/HMI, Switch, Security-Switch und Bereich. Ziehen Sie ein Gerät auf die Fläche.
2. **Planungsfläche:** Hier bauen Sie das Netz. Mausrad zum Zoomen, Verschieben mit gedrückter Maustaste auf freier Fläche.
3. **Inspektor:** Zeigt die Einstellungen des angeklickten Geräts. Beim Security-Switch in Reitern.
4. **Verbindung testen:** Quelle, Ziel und Dienst wählen, „Paket senden". Der Weg erscheint Schritt für Schritt.
5. **Kommunikationsmatrix:** Wer darf mit wem? Eine Zelle anklicken zeigt den Weg.
6. **Firewall-Log:** Jede Entscheidung der Firewall. Einträge mit „LIVE" stammen vom echten Datenverkehr.
7. **Kopfzeile:** Sprache umschalten (DE EN IT), Beispiele laden, Projekte öffnen und speichern, Plan als PDF, Programm beenden.

Die Statusanzeigen oben zeigen Programm, PLCSIM-Instanzen und Datenpfad. Die letzte Anzeige, **„Konfiguration schlüssig"** oder **„n Hinweise"**, prüft Ihren Plan laufend: ungültige Adressen, fehlende Router bei Geräten, IP-Konflikte im selben Segment, falsche NAT- und Firewall-Angaben. Ein Klick auf einen Security-Switch und den Reiter „Status" zeigt die Hinweise im Klartext.

4 Ein Netz planen

Geräte anlegen und verkabeln

1. Ein Gerät aus der Leiste links **auf die Fläche ziehen**. Alternativ ein Beispiel mit „Beispiel laden“ öffnen.
2. Mit der Maus von einem **Port zu einem anderen Port ziehen**, um ein Kabel zu legen. Auch zwei Ports nacheinander anklicken geht.
3. Ein Gerät anklicken: Rechts im Inspektor stellen Sie Name, IP-Adresse, Subnetzmaske und **Router** ein. Auswahl löschen mit der Taste **Entf**.

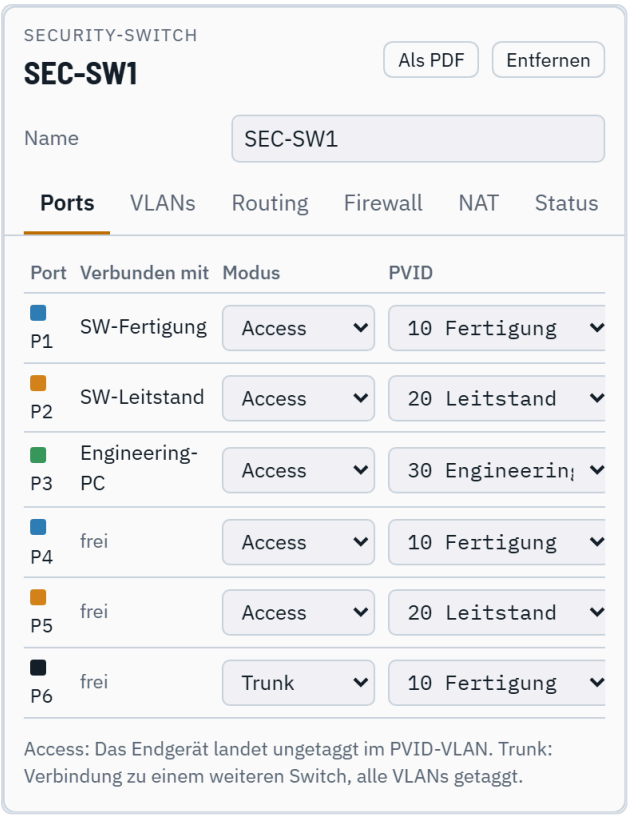


Beispiel: Zwei Zonen (Fertigung, Leitstand) und ein Engineering-Netz an einem Security-Switch. Orange und grün sind verschiedene VLANs.

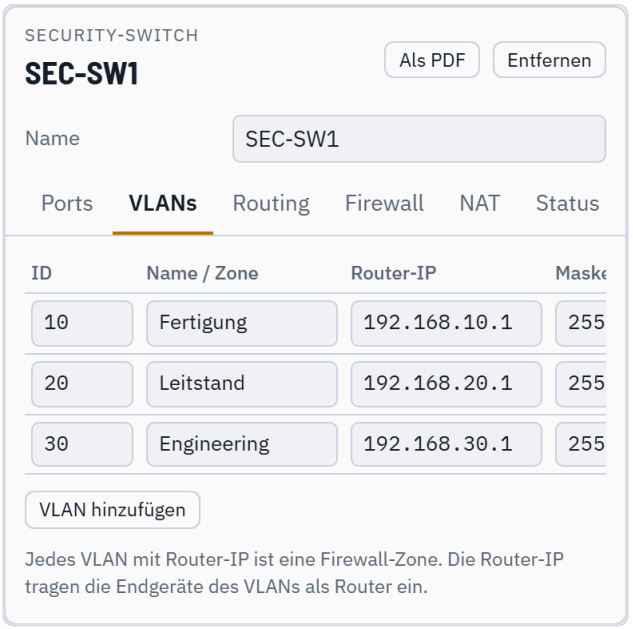
> **WICHTIG**
> Jede Steuerung und jedes Gerät braucht den **Router**, wenn es mit einem anderen Netz sprechen soll. Als Router tragen Sie die **Router-IP des VLANs** am Security-Switch ein. Sonst kommt die Antwort nie zurück.

Den Security-Switch einrichten

Ein Klick auf den Security-Switch öffnet im Inspektor sechs Reiter (Ports, VLANs, Routing, Firewall, NAT, Status). Die wichtigsten Einstellungen:



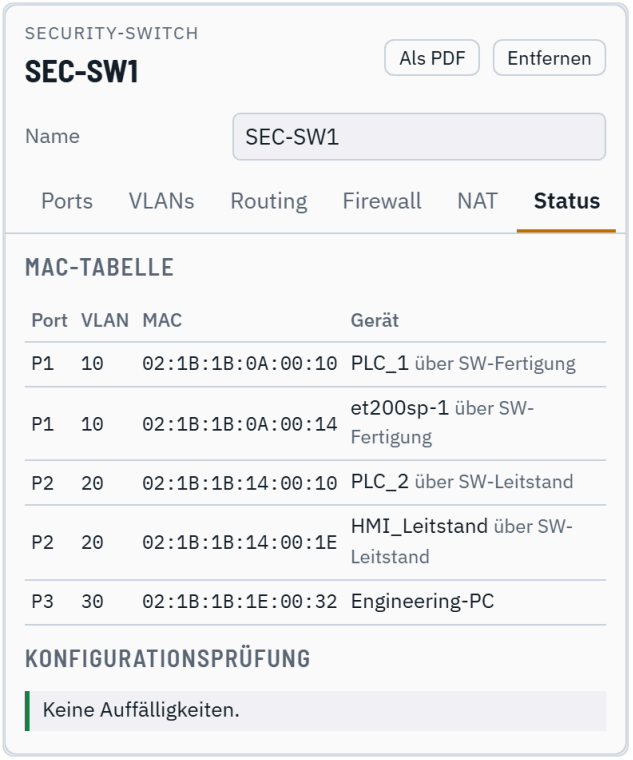
Ports: Access (ein VLAN) oder Trunk (alle VLANs, für die Verbindung zu einem weiteren Switch)



VLANs: Name, Router-IP und Maske. Jedes VLAN mit Router-IP ist eine Firewall-Zone.



Routing: Routing zwischen den VLANs an- oder ausschalten, statische Routen eintragen

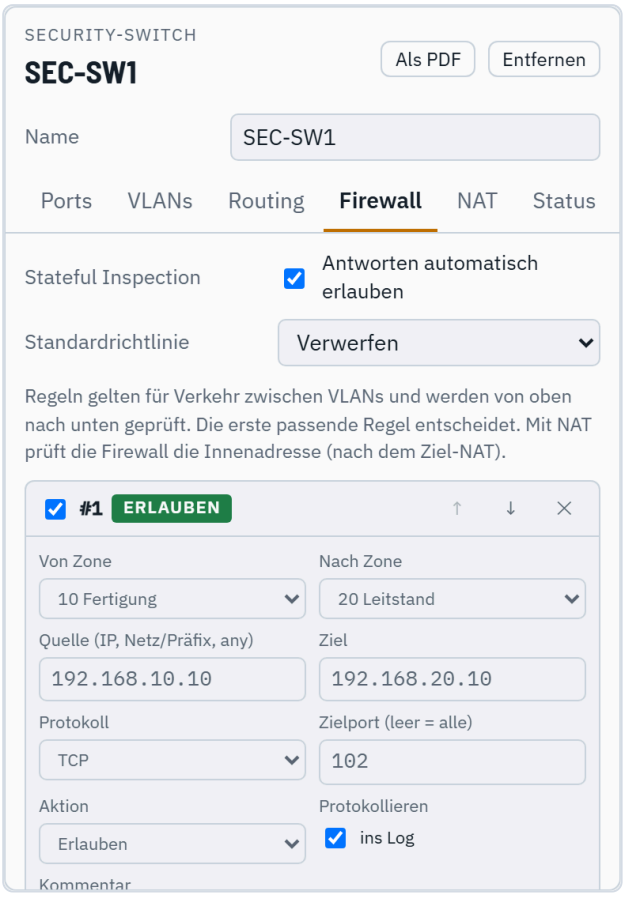


Status: angeschlossene Geräte mit MAC-Adresse und die Konfigurationsprüfung

Mit dem Werkzeug **„Bereich“** legen Sie farbige Rechtecke mit Beschriftung hinter Ihren Plan, zum Beispiel für „Werksnetz“ oder „Maschine 1“. Das macht größere Pläne übersichtlich.

5 Firewall und Stateful Inspection

Die Firewall des Security-Switches prüft Verkehr **zwischen** den VLANs. Innerhalb eines VLANs prüft sie nicht. Die Regeln werden von oben nach unten durchsucht, die **erste passende Regel entscheidet**. Passt keine Regel, gilt die **Standardrichtlinie** (meist „Verwerfen“).



Reiter Firewall: Stateful Inspection, Standardrichtlinie und die Regeln. Jede Regel hat Zonen, Quelle, Ziel, Protokoll, Zielport und Aktion.

Eine Regel anlegen

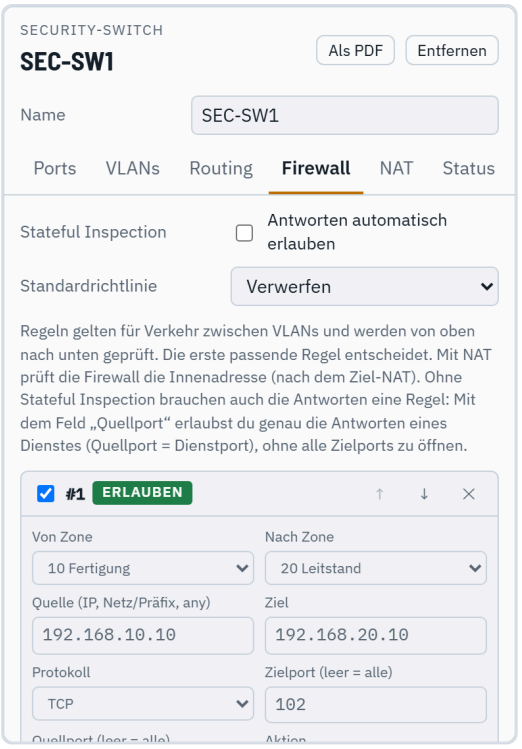
1. Security-Switch anklicken, Reiter **Firewall**, Knopf **„Regel hinzufügen“**.
2. **Von Zone** und **Nach Zone** wählen, Quelle und Ziel als IP-Adresse, Netz (zum Beispiel `192.168.10.0/24`) oder `any` eintragen.
3. **Protokoll** und **Zielport** festlegen (S7 zum Beispiel TCP 102). Ein leerer Port bedeutet alle Ports.
4. **Aktion** „Erlauben“ oder „Verwerfen“, mit „Protokollieren“ erscheint die Entscheidung im Log.

Was Stateful Inspection bedeutet

Mit eingeschalteter **Stateful Inspection** merkt sich die Firewall jede erlaubte Verbindung und lässt die **Antworten** darauf automatisch zurück. Sie brauchen nur eine Regel für die Richtung, in der die Verbindung aufgebaut wird. Schalten Sie die Stateful Inspection aus, braucht auch der Verkehr in die Gegenrichtung eine eigene Regel.

Der Quellport (für Fortgeschrittene)

Eine Regel kann zusätzlich einen **Quellport** verlangen. Das Feld erscheint nur dann, wenn es sinnvoll ist: bei ausgeschalteter Stateful Inspection oder wenn schon ein Quellport eingetragen ist. Die Antwort eines Dienstes kommt mit dem Dienstport als Quellport zurück. Eine Regel mit diesem Quellport erlaubt genau die Antworten dieses Dienstes, ohne alle Zielports zu öffnen.



Ohne Stateful Inspection erscheint bei jeder Regel das Feld „Quellport“.

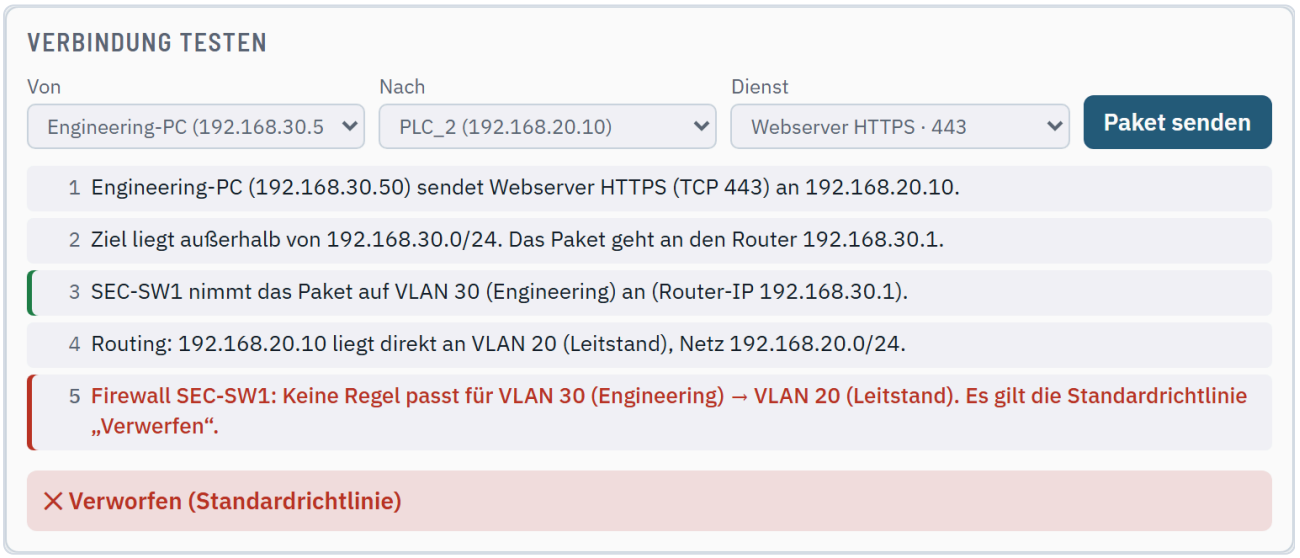
6 Verbindungen testen

Ein Testpaket senden

1. Im Feld **„Von“** das sendende Gerät wählen, bei **„Nach“** das Ziel und bei **„Dienst“** das Protokoll (zum Beispiel S7-Kommunikation, Webserver, OPC UA, Ping).
2. Auf **„Paket senden“** klicken. Darunter erscheint der Weg des Pakets Schritt für Schritt, grün für erlaubte Schritte, rot für den Schritt, an dem das Paket stirbt.



Das Paket von PLC_1 zu PLC_2 kommt durch: Router, Firewall-Regel 1, ARP, Zielport offen, Antwort zurück.



Das gleiche Ziel mit einem anderen Dienst: Die Firewall verwirft das Paket, weil keine Regel passt. Das Ergebnis steht unter dem Weg.

Die Kommunikationsmatrix und das Log

Die **Kommunikationsmatrix** zeigt für den gewählten Dienst auf einen Blick, wer mit wem sprechen darf („offen“ oder „zu“). Eine Zelle anklicken zeigt den Weg im Testfeld. Das **Firewall-Log** sammelt die Entscheidungen (höchstens 200 Einträge, „Leeren“ räumt auf). Regeln ohne Haken bei „Protokollieren“ erscheinen dort nicht.

KOMMUNIKATIONSMATRIX

Gewählter Dienst, jede Quelle (Zeile) zu jedem Ziel (Spalte). Zelle anklicken zeigt den Weg.

Von \ Nach	PLC_1	PLC_2	et200sp-1	HMI_Leitstand	Engineering-PC
PLC_1	–	✓ offen	✕ zu	✕ zu	✕ zu
PLC_2	✕ zu	–	✕ zu	✕ zu	✕ zu
et200sp-1	✓ offen	✕ zu	–	✕ zu	✕ zu
HMI_Leitstand	✕ zu	✓ offen	✕ zu	–	✕ zu
Engineering-PC	✓ offen	✓ offen	✕ zu	✕ zu	–

FIREWALL-LOG

4 Einträge (max. 200) Leeren

Zeit	Von	Nach	Dienst	Regel	Ergebnis
11:25:44	PLC_1	192.168.20.10	TCP 102	#1	**durch** · Verbindung steht
11:25:44	Engineering-PC	192.168.20.20	TCP 80	Std.	LIVE **blockiert** · SEC-SW1: Standardrichtlinie „Verwerfen“ (VLAN 30 → 20)
11:25:44	Engineering-PC	192.168.10.10	TCP 102	#2	LIVE **durch** · SEC-SW1: Regel 2 erlaubt (VLAN 30 → 10)
11:25:44	PLC_1	192.168.20.10	TCP 102	#1	LIVE **durch** · SEC-SW1: Regel 1 erlaubt (VLAN 10 → 20)

Matrix und Log. „LIVE“ kennzeichnet Entscheidungen des echten Datenverkehrs, die anderen Einträge sind Tests im Programm.

PROFINET

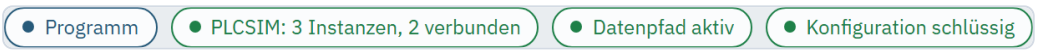
PLCSIM Advanced simuliert kein PROFINET IO. Die Prüfung bei IO-Devices bewertet deshalb nur die **Planung**: Liegen Controller und IO-Device im selben Segment und im selben IP-Subnetz? Stimmt das nicht, sperrt das Programm im Live-Modus die E/A-Daten des IO-Devices.

7 Live mit PLCSIM Advanced

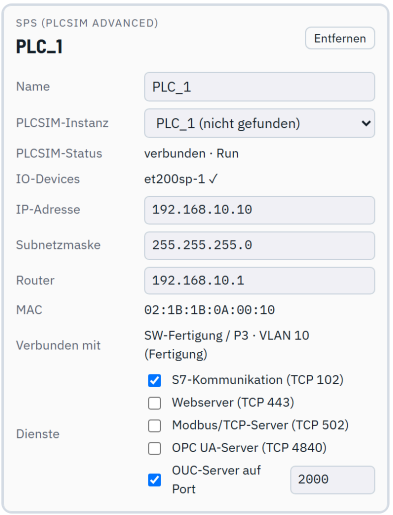
Im Live-Modus läuft der echte Datenverkehr Ihrer PLCSIM-Instanzen durch den simulierten Switch. Das Programm tritt im PLCSIM-Netz als Router auf: Für jede Router-IP eines VLANs antwortet es mit einer eigenen MAC-Adresse. Pakete zwischen verschiedenen Subnetzen werden geroutet, gegen die Firewall-Regeln geprüft (mit Stateful Inspection) und weitergeleitet oder verworfen.

Vorbereitung

1. **PLCSIM Advanced** auf „TCP/IP Single Adapter“ mit `<Local>` stellen und die Instanzen starten. **Npcap** muss installiert sein.
2. In **TIA Portal** bei jeder SPS die IP-Adresse eintragen und **„Router verwenden“** mit der Router-IP des VLANs setzen (so wie im Plan). Für PUT/GET den Zugriff durch den entfernten Partner erlauben. Das Projekt in die Instanz laden.
3. Im **SecNet Labor** bei jeder SPS im Inspektor die **PLCSIM-Instanz** auswählen. Ein grüner Punkt an der SPS zeigt die Verbindung. Eine Instanz gehört immer nur zu einer SPS.
4. Oben in der Statuszeile sollte „Datenpfad aktiv“ stehen.



Die Statusanzeigen oben: Programm, PLCSIM-Instanzen, Datenpfad und Konfigurationsprüfung.



Inspektor einer SPS: PLCSIM-Instanz, Verbindungsstatus, IP-Adresse, Router und Dienste.

Beispiel: PUT/GET zwischen zwei SPS

PLC_1 liest per GET Daten aus PLC_2. Solange die Firewall-Regel **aktiv** ist, kommen die Daten bei PLC_1 an. Schalten Sie die Regel aus, bricht die Übertragung ab, und das Log zeigt „blockiert“. Schalten Sie sie wieder ein, läuft sie weiter. Im Log erscheint jede Entscheidung mit „LIVE“ und der Regel, die sie getroffen hat.

> **TIPP**
> Die Partneradresse im GET/PUT ist die Adresse der anderen SPS (hier PLC_2). Bei NAT oder NAPT ist es die **Außenadresse** (siehe Kapitel 9 und 10).

8 TIA Portal durch die Firewall: PC anbinden

Auch der Zugriff Ihres Engineering-PCs (TIA Portal) kann durch die simulierte Firewall laufen. Dafür gibt es zwei Möglichkeiten.

Möglichkeit 1: zwei Adressen am Adapter (nicht empfohlen)

Im Windows-Adapter „PLCSIM Virtual Ethernet“ tragen Sie zusätzlich Adressen aus beiden Netzen ein. Der PC sitzt dann direkt in beiden Zonen und spricht **am Security-Switch vorbei** mit der SPS. Das ist zum Laden eines Projekts nützlich, testet die Firewall aber nicht.

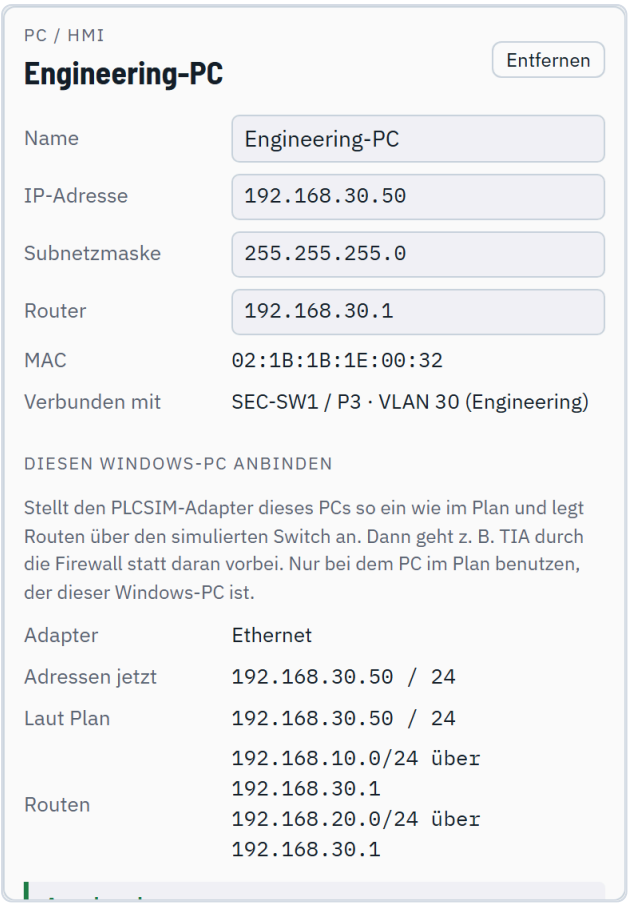
Möglichkeit 2: „PC anbinden“ (empfohlen)

Der Windows-PC wird selbst ein Gerät im Plan (zum Beispiel „Engineering-PC“ mit IP und Router). Mit dem Knopf **„PC anbinden“** stellt das Programm den PLCSIM-Adapter des PCs so ein, wie der PC im Plan steht, und legt Routen zu den anderen Netzen an. Dann läuft auch TIA durch die Firewall und braucht passende Regeln (zum Beispiel TCP 102 für Online und Laden, ICMP für Ping).

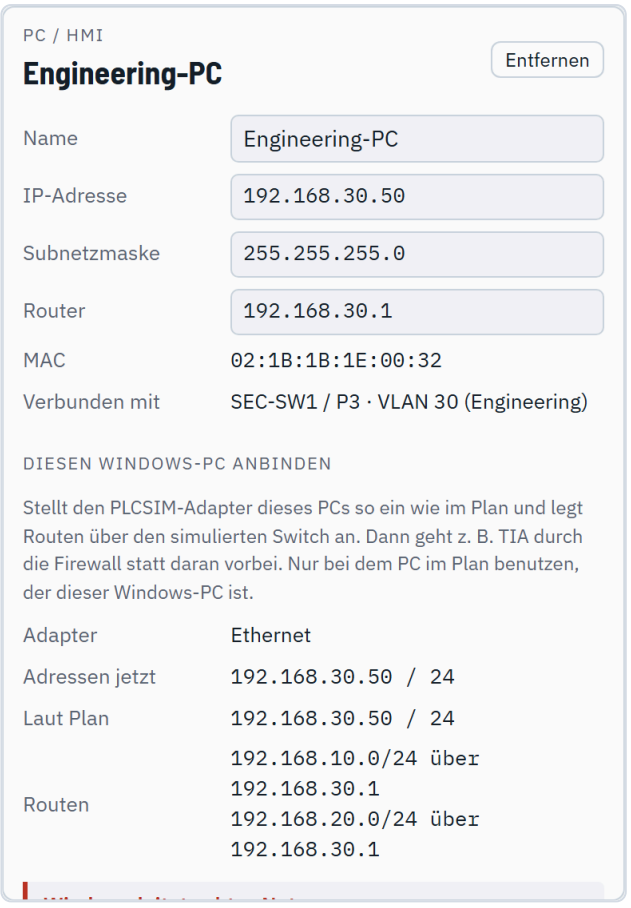
1. Im Plan den PC anklicken (IP-Adresse und Router wie im Netz, zum Beispiel `192.168.30.50` und Router `192.168.30.1`).
2. Unten im Inspektor bei „Diesen Windows-PC anbinden“ auf **„PC anbinden“** klicken und die Windows-Abfrage (Administratorrechte) bestätigen.
3. Die **PLCSIM-Instanzen einmal aus- und wieder einschalten**, denn ihre MAC-Adresse hängt an der Adresse des Adapters.
4. In TIA online gehen. Fragt TIA nach einer weiteren IP-Adresse („IP-Adresse zuweisen?“), auf **„Nein“** klicken. Das Routing ist aktiv, es muss keine Adresse hinzugefügt werden.

Was mit den Routen passiert

- Es werden nur Routen für die Netze des Security-Switches angelegt, dessen Router der PC benutzt.
- Überschneidet sich ein Netz im Plan mit einem **echten Netz Ihres PCs** (zum Beispiel dem WLAN `192.168.1.0/24`), legt das Programm dafür **keine** Route an und meldet das. Sonst ginge Ihr echter Verkehr in den simulierten Switch.
- **Beim Beenden des Programms** werden die angelegten Routen wieder entfernt (Windows fragt nach Administratorrechten). Die Adresse am Adapter bleibt. **„Wieder trennen“** stellt den Zustand von vor dem ersten Anbinden wieder her.



Der Block „Diesen Windows-PC anbinden“: Adapter, Adressen, angelegte Route und Status



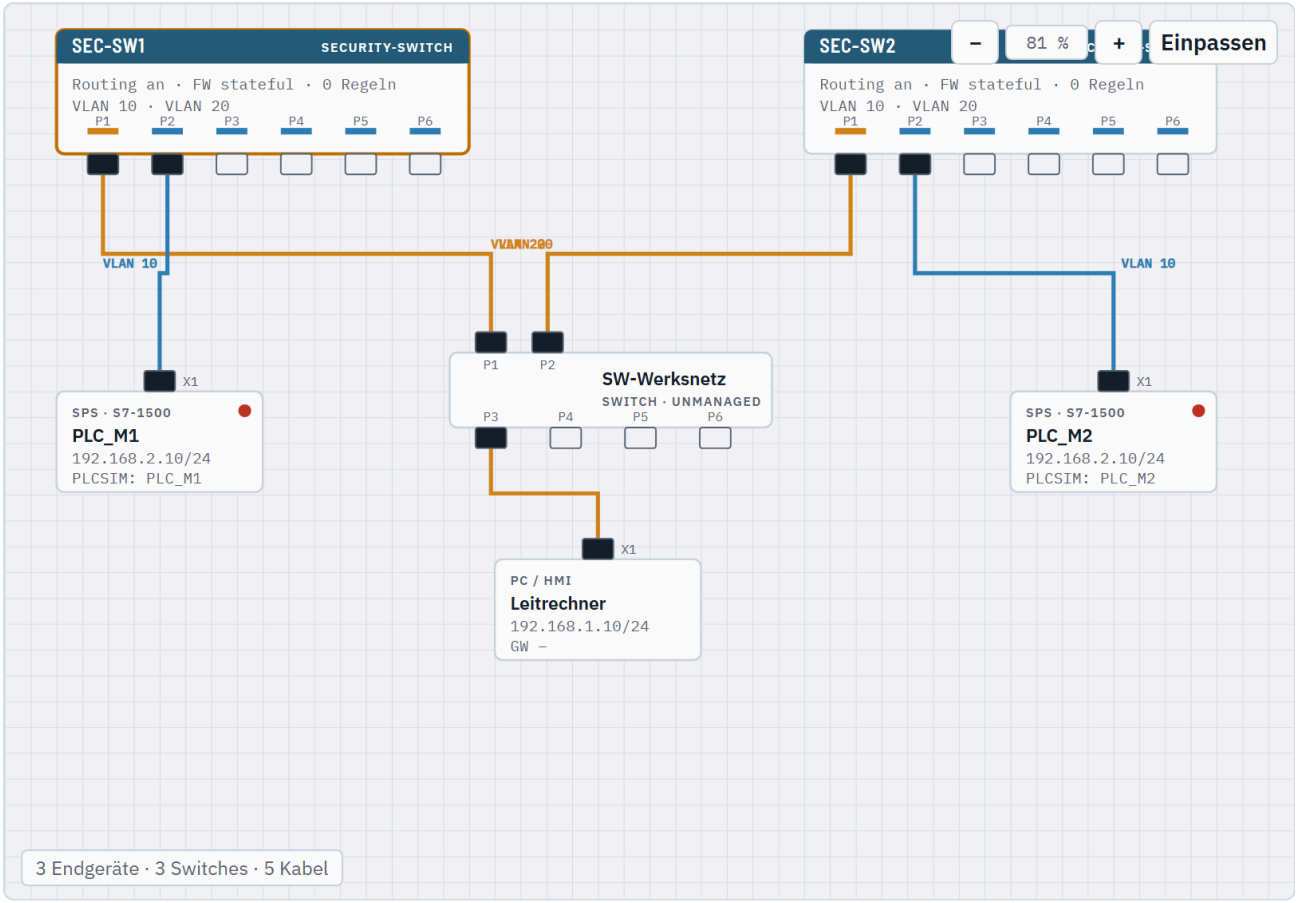
Der Hinweis „Windows leitet echtes Netz um“ mit dem Knopf zum Aufräumen

Routen am PC prüfen

In PowerShell mit `route print -4`. Nach dem Beenden des Programms sollten Sie unter „Ständige Routen“ nichts mehr von SecNet Labor finden. Steht noch eine Route, die ein echtes Netz in den simulierten Switch umleitet, zeigt das Programm einen roten Hinweis mit dem Knopf **„Störende Routen entfernen“**.

9 NAT 1:1: gleiche Adressen, eindeutig erreichbar

Steuerungen werden oft mit ihrer Standard-IP-Adresse ausgeliefert und nach der Auslieferung nicht geändert. Hat eine Anlage mehrere gleiche Maschinen, haben alle **dieselbe Adresse**. Damit sie trotzdem eindeutig erreichbar sind, nutzt man **NAT**: Der Security-Switch vor jeder Maschine gibt ihr nach außen eine eigene Adresse und schreibt die Adresse im Paket um.



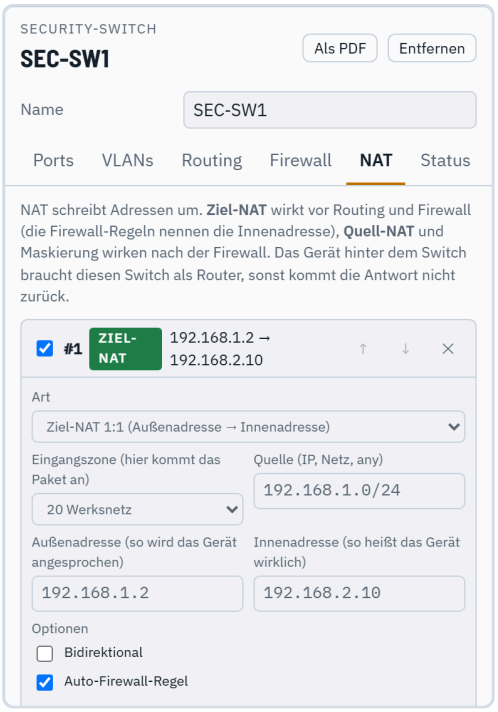
Beispiel NAT: PLC_M1 und PLC_M2 haben beide `192.168.20.10`. Der Leitrechner erreicht sie unter `192.168.10.2` und `192.168.10.3`.

So funktioniert es

1. Das Leitsystem schickt etwas an `192.168.10.2` (die Außenadresse von Maschine 1).
2. Der Switch schreibt als Ziel die echte Adresse `192.168.20.10` ins Paket und gibt es der Maschine. Das geschieht **vor** Routing und Firewall.
3. Die Maschine antwortet. Der Switch schreibt wieder `192.168.10.2` als Absender hinein. Das Leitsystem merkt nichts von der Übersetzung.

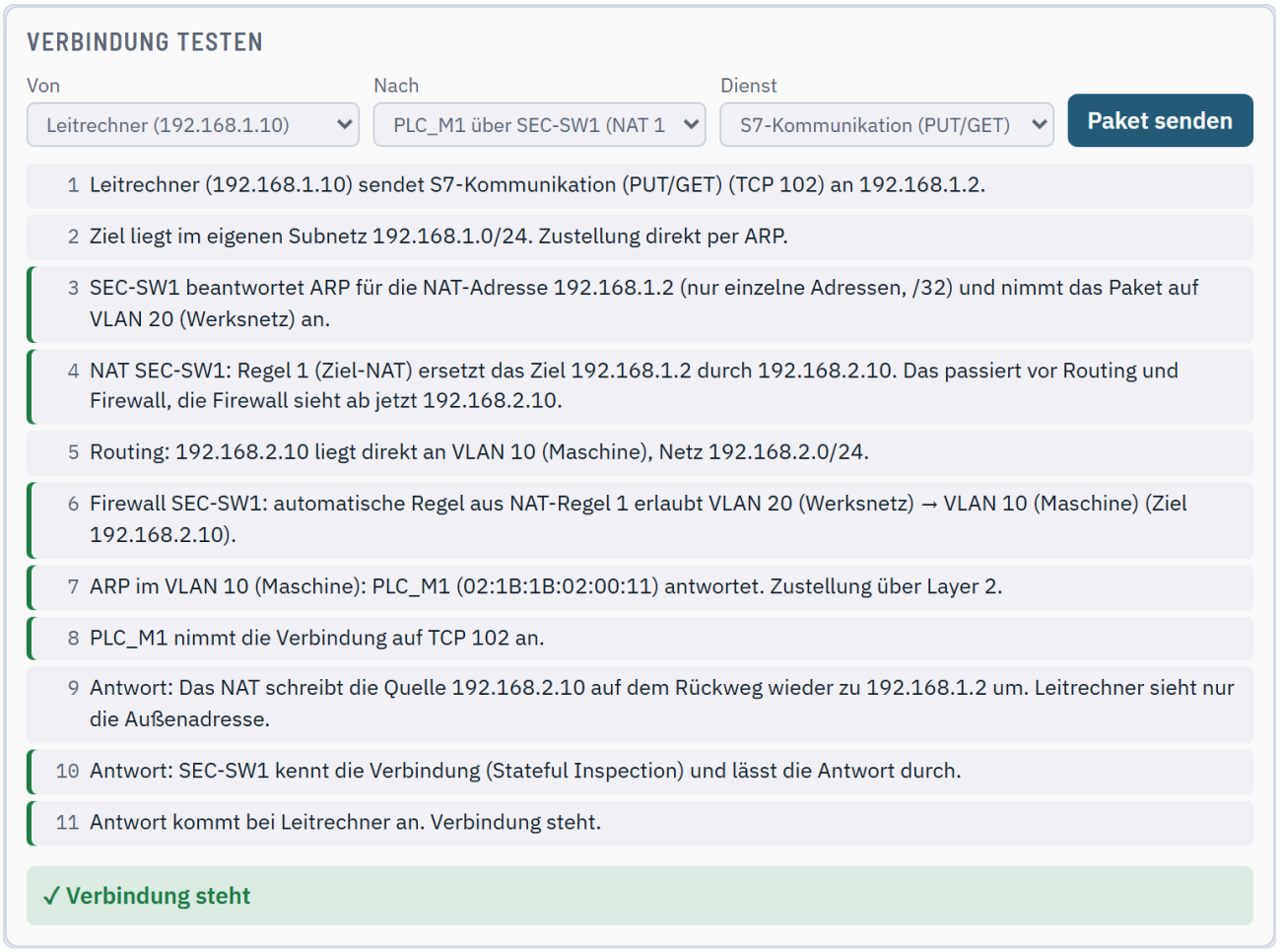
Die NAT-Regel einrichten

Security-Switch anklicken, Reiter **NAT**, Knopf „NAT-Regel hinzufügen“, Art **„Ziel-NAT 1:1“**.



Ziel-NAT: Eingangszone, Quelle, Außenadresse und Innenadresse. Die Optionen „Bidirektional“ und „Auto-Firewall-Regel“ stehen darunter.

Feld	Bedeutung
Eingangszone	In dieser Zone kommt das Paket an (hier das Werksnetz).
Quelle	Wer darf die Außenadresse benutzen (IP, Netz oder `any`).
Außenadresse	So wird die Maschine von außen angesprochen. Eine einzelne Adresse (`/32`) wird vom Switch auch per ARP beantwortet.
Innenadresse	So heißt die Maschine wirklich.
Auto-Firewall-Regel	Der Switch erlaubt den Verkehr zur Innenadresse automatisch. Ohne das Häkchen brauchen Sie eine eigene Firewall-Regel mit der **Innenadresse**.
Bidirektional	Auch wenn die Maschine selbst eine Verbindung nach außen aufbaut, erscheint sie mit ihrer Außenadresse.



Der Test von „Leitrechner“ zu „PLC_M1 über SEC-SW1 (NAT 192.168.1.2)“: Der Switch beantwortet ARP für die Außenadresse und schreibt das Ziel um.

Wichtig bei NAT

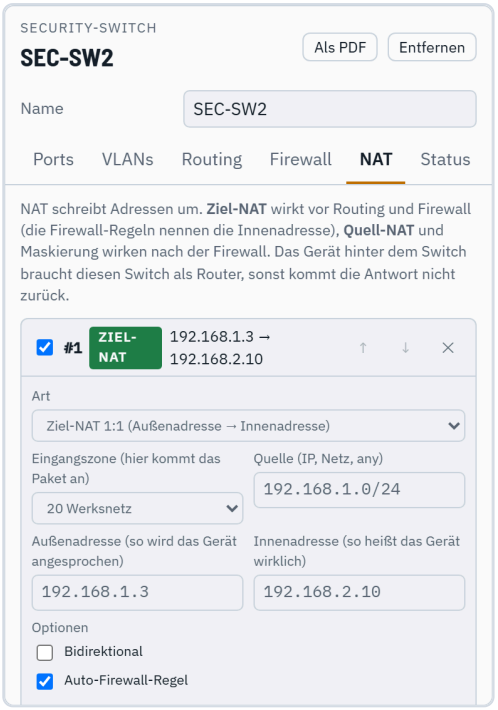
- **Router bei der SPS:** Die Steuerung muss den Security-Switch (Router-IP des Maschinen-VLANs) als Router eingetragen haben, sonst kommt die Antwort nicht zurück.
- **Die Firewall sieht die Innenadresse.** Eine eigene Regel mit der Außenadresse greift nie, denn das Ziel wird vor der Firewall umgeschrieben.
- **In TIA** tragen Sie als Partneradresse (zum Beispiel bei GET) die **durch NAT geänderte Adresse** ein, obwohl die SPS eigentlich eine andere hat. Verbindungen, die auf beiden Seiten fest mit der Partner-IP projektiert sind, funktionieren mit NAT nicht. Nehmen Sie GET/PUT von einer Seite aus.
- Gleiche IP-Adressen hinter **verschiedenen** Security-Switches sind erlaubt. Einen IP-Konflikt meldet die Konfigurationsprüfung nur im selben Segment.

> **GRENZE IM LIVE-MODUS**
> Auf einem PLCSIM-Adapter kann es zu einer Adresse nur eine Instanz geben. Zwei gleiche Maschinen mit derselben IP lassen sich deshalb nur **in der Planung** zeigen. Für einen Live-Test geben Sie der zweiten Maschine eine andere Innenadresse.

Querkommunikation zwischen Maschinen

Wenn zwei gleiche Maschinen miteinander sprechen sollen (Maschine 2 ruft Maschine 1), braucht es zusätzlich einen **Quell-NAT** beim Switch der anrufenden Maschine. Sonst würde Maschine 1 als Absender ihre eigene Adresse sehen. Dazu kommt eine Firewall-Regel mit der **echten** Quelladresse, denn der Quell-

NAT wirkt erst nach der Firewall.

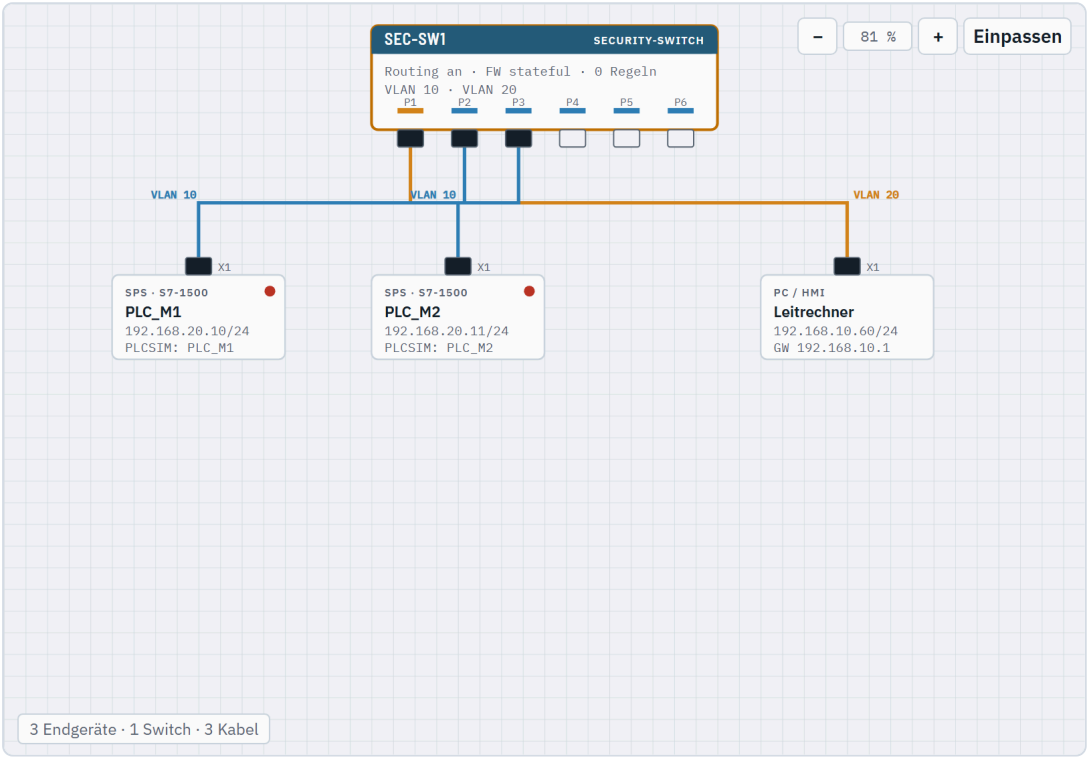


Beim Switch der anrufenden Maschine: Quell-NAT von 192.168.2.10 auf 192.168.1.3.

10 Port-Weiterleitung (NAPT) und OPC UA

Bei **NAPT** hat der Switch **eine einzige Außenadresse** (seine Router-IP). Die Geräte dahinter unterscheidet er nur durch den **Port**. Der Vorteil: Man braucht für jedes Gerät keine eigene freie IP-Adresse, eine einzige genügt.

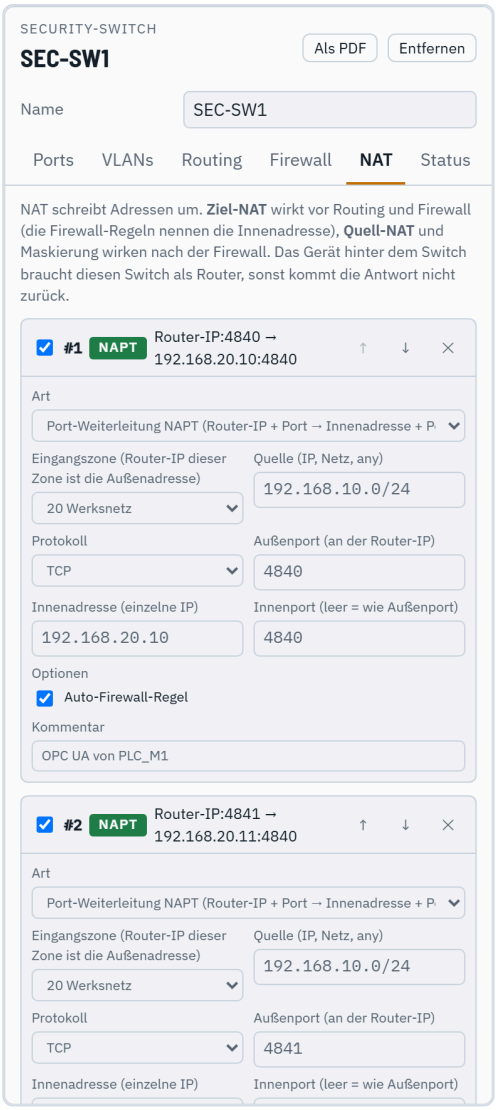
Anfrage von außen	Weiterleitung an
`192.168.10.1` , Port `4840`	SPS 1: `192.168.20.10` , Port `4840`
`192.168.10.1` , Port `4841`	SPS 2: `192.168.20.11` , Port `4840`
`192.168.10.1` , Port `8443`	Webserver von SPS 1: `192.168.20.10` , Port `443`



Beispiel NAPT: zwei SPS mit OPC UA hinter einem Switch, erreichbar über dessen Router-IP.

Die NAPT-Regeln

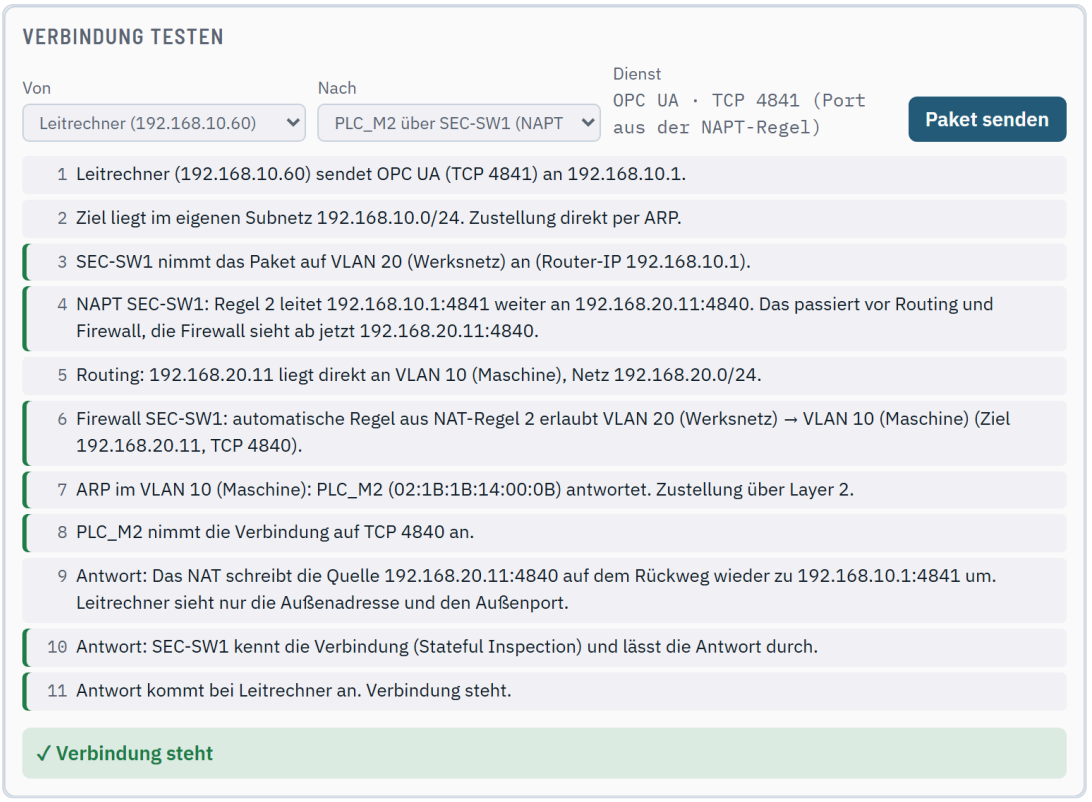
Reiter **NAT**, Art **„Port-Weiterleitung NAPT“**. Sie tragen den **Außenport** (an der Router-IP), die **Innenadresse** und den **Innenport** ein (leer bedeutet: wie der Außenport). Mit „Auto-Firewall-Regel“ erlaubt der Switch genau diese Kombination aus Protokoll und Innenport.



NAPT-Regeln: zwei OPC-UA-Server (Außenports 4840 und 4841); die dritte Regel (Webserver, 8443 auf 443) folgt darunter.

Testen

Unter **„Nach“** gibt es für jede Weiterleitung einen eigenen Eintrag, zum Beispiel „PLC_M2 über SEC-SW1 (NAPT 192.168.10.1:4841)“. Dann stehen Adresse und Port schon richtig im Test, die Dienstauswahl entfällt.



Test über die Weiterleitung: Das Ziel wird auf 192.168.20.11:4840 umgeschrieben, die Firewall sieht diese Innenadresse mit Innenport.

OPC UA mit UA Expert (Live)

1. In TIA bei der SPS den **OPC-UA-Server aktivieren**, Adresse und Router wie im Plan eintragen und laden. Im SecNet Labor die Instanz zuordnen.
2. Den PC anbinden (Kapitel 8) und die Instanzen aus- und einschalten.
3. In UA Expert als Server die **Router-IP des Switches** eintragen: `opc.tcp://192.168.10.1:4840`. Nicht die Adresse der SPS.
4. Im Firewall-Log erscheint „NAPT: 192.168.10.1:4840 → 192.168.20.10:4840“. UA Expert findet die SPS und zeigt deren Anwendung an.

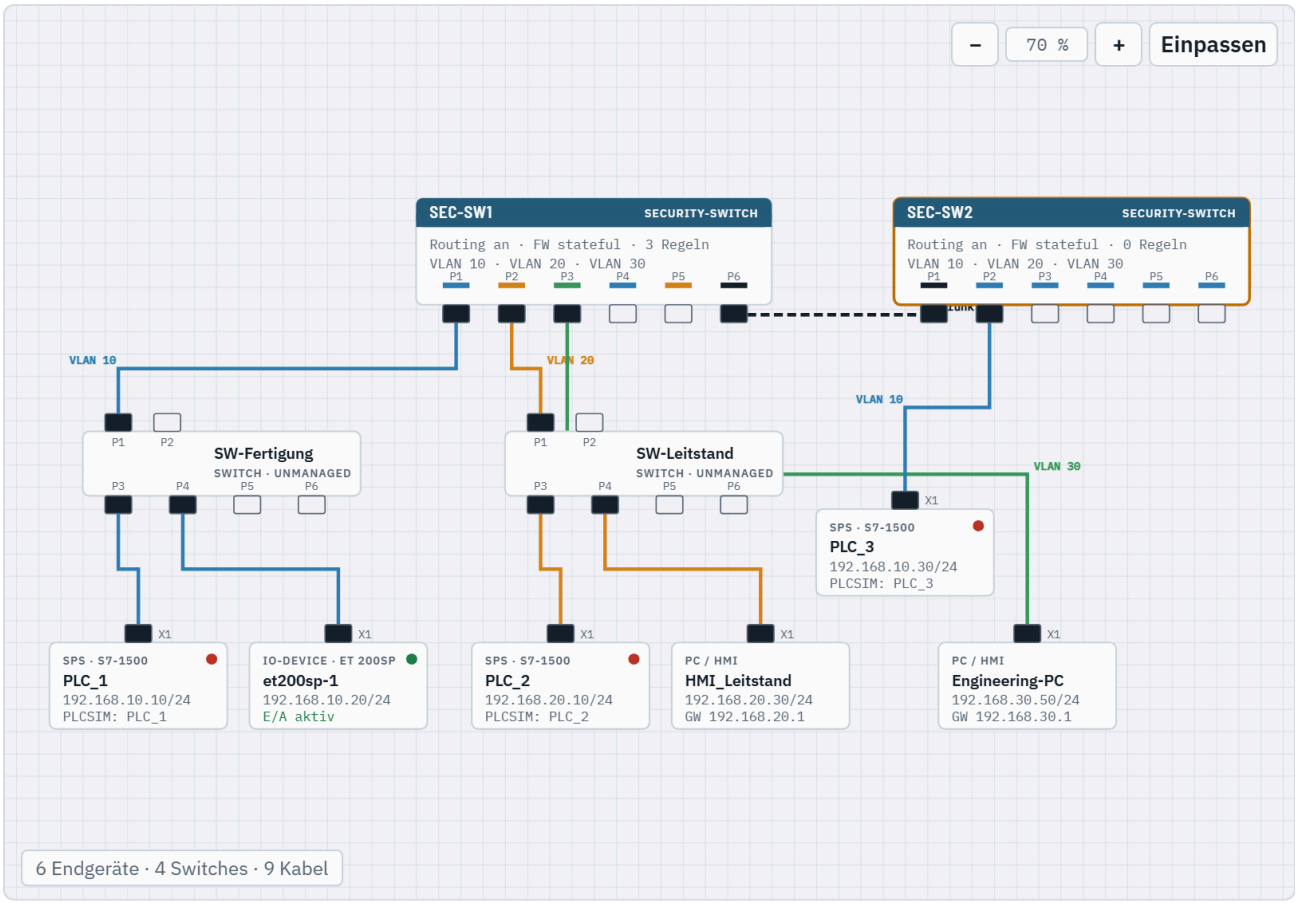
> **GUT ZU WISSEN**
> Die SPS meldet dem Client als Endpunkt ihre **eigene** Adresse (`192.168.20.10`). Die eigentliche Sitzung baut UA Expert deshalb oft direkt zu dieser Adresse auf. Das klappt, wenn der PC eine Route ins Maschinennetz hat (wie nach „PC anbinden“). Dann läuft diese Sitzung normal geroutet durch die Firewall, ohne NAPT. Im Log erkennen Sie das daran, dass der Eintrag **ohne** den NAPT-Hinweis erscheint. In echten Anlagen ohne Route ins Maschinennetz muss man den Endpunkt am Client oder an der SPS anpassen.

Grenzen von NAPT

- Jeder Außenport lässt sich nur einmal weiterleiten. Ein weitergeleiteter Port ist am Switch selbst nicht mehr nutzbar (zum Beispiel 443 für sein Web-Management).
- Dienste mit **festem Port**, zum Beispiel S7 (Port 102), lassen sich über **eine** Adresse nur für **ein** Gerät weiterleiten. Für mehrere gleiche Maschinen mit S7 nehmen Sie NAT 1:1.

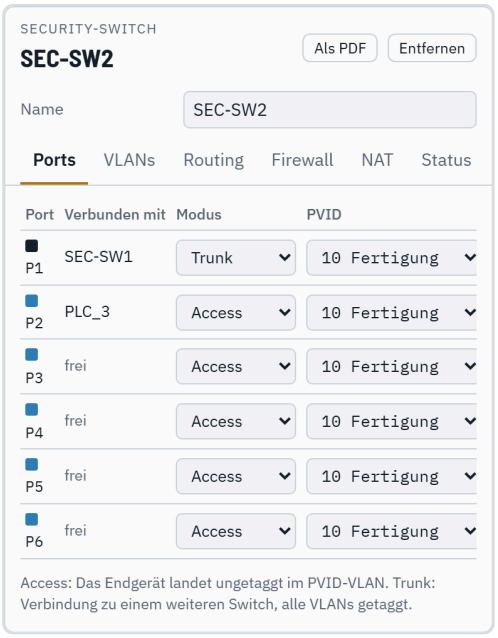
11 Zwei Security-Switches verbinden (Trunk)

Zwei Security-Switches lassen sich über einen **Trunk** verbinden. Auf dem Trunk laufen alle VLANs getaggt. So kann eine SPS am zweiten Switch im selben Netz liegen wie eine SPS am ersten.



SEC-SW1 und SEC-SW2 sind über einen Trunk verbunden (gestrichelt). PLC_3 hängt am VLAN 10 des zweiten Switches und spricht mit PLC_1 am ersten.

1. Bei **beiden** Switches den Port der Verbindung im Reiter „Ports“ auf **Trunk** stellen und aktivieren.
2. Die beiden Trunk-Ports mit einem Kabel verbinden.
3. Beim zweiten Switch die gleichen VLANs anlegen (gleiche ID). Die **Router-IP bleibt dort leer** („nur Layer 2“). Der Router des Netzes bleibt der erste Switch.
4. Die SPS am zweiten Switch bekommt die Adresse aus dem Netz des VLANs und als Router die Router-IP des **ersten** Switches.

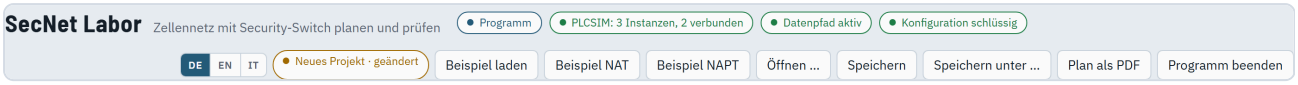


Ports des zweiten Switches: P1 ist der Trunk, die übrigen sind Access-Ports im VLAN 10.

TIPP

Die Router-IP für Switch 2 muss frei bleiben. Zwei Geräte mit derselben Router-IP im selben Netz würden einen IP-Konflikt verursachen.

12 Projekte, Beispiele und PDF



Die Kopfzeile: Beispiele, Projekte, PDF-Ausgabe und Beenden.

Knopf	Was er macht
Beispiel laden	Ein fertiges Netz mit drei Zonen, zwei SPS und einer Firewall.
Beispiel NAT	Zwei gleiche Maschinen mit derselben Adresse hinter je einem Security-Switch, erreichbar über NAT.
Beispiel NAPT	Zwei SPS mit OPC UA hinter einer Außenadresse, erreichbar über verschiedene Ports.
Öffnen, Speichern, Speichern unter	Projekte als `.json`-Datei mit den Windows-Dialogen (Strg+S speichert). Der Plan bleibt zusätzlich im Programm erhalten und ist beim nächsten Start wieder da.
Plan als PDF	Der Netzplan auf Seite 1 (A4 quer), danach die Liste der Geräte und Bereiche.
Als PDF (beim Security-Switch)	Alle Einstellungen des Switches auf A4: Ports, VLANs, Routing, Firewall-Regeln, NAT, angeschlossene Geräte und Konfigurationsprüfung.

> **HINWEIS**
> Die PDF-Dateien erzeugt das Programm im Hintergrund mit Edge. Das kann einige Sekunden dauern. Danach öffnet sich die Datei.

13 Fehlersuche

Problem	Mögliche Ursache und Lösung
Das Paket wird „verworfen“ (Standardrichtlinie)	Keine Regel passt. Im Reiter Firewall eine Regel mit den richtigen Zonen, Adressen und dem richtigen Zielport anlegen. Bei NAT zählt die **Innenadresse**.
Der Weg endet mit „Rückweg fehlt“ oder „ohne Router“	Beim Zielgerät fehlt der Router. Die Router-IP des VLANs eintragen (auch in TIA: „Router verwenden“).
Die SPS hat einen roten Punkt	Keine PLCSIM-Instanz ausgewählt oder die Instanz läuft nicht. Im Inspektor die Instanz wählen, in PLCSIM starten.
„Datenpfad aus“ oben	Npcap fehlt oder der PLCSIM-Adapter wurde nicht gefunden. Npcap installieren, PLCSIM auf „TCP/IP Single Adapter“ mit `<Local>` stellen.
TIA findet die SPS nicht	Beim Laden „Erweiterten Download“ wählen, als Schnittstelle den PLCSIM Virtual Ethernet Adapter und die IP von Hand eintragen. Der PC-Adapter braucht eine Adresse im Netz der SPS. Danach die Instanzen aus- und einschalten. Auf alte Routen prüfen (`route print -4`).
Im Log steht dauernd „blockiert“ für TCP 102	TIA fragt regelmäßig nach der SPS, und Port 102 ist nicht erlaubt. Eine Regel für TCP 102 anlegen oder die Online-Verbindung in TIA trennen.
Nach „PC anbinden“ ist das WLAN oder Internet gestört	Eine Route leitet ein echtes Netz in den Switch um. Beim PC „Störende Routen entfernen“ klicken oder das Programm beenden. Mit `route print -4` kontrollieren.
NAT: keine Verbindung	Router bei der SPS eingetragen? Quelle in der NAT-Regel passt? Außenadresse als einzelne Adresse (`/32`)? Firewall-Regel mit der **Innenadresse** oder „Auto-Firewall-Regel“?
NAPT/OPC UA findet nichts	Die Router-IP des Switches und den **Außenport** eintragen, nicht die Adresse der SPS. Regel eingeschaltet? Protokoll TCP? OPC-UA-Server in der SPS aktiv?
Das Programmfenster ist leer oder reagiert nicht	Mit **Strg+R** neu laden. Hilft das nicht, das Programm beenden und neu starten.

SUPPORT

Bei Fragen oder Fehlern erreichen Sie uns unter **support@plcprime.io**. Schicken Sie am besten einen Screenshot und den Eintrag aus dem Firewall-Log mit.

14 Hinweise und Rechtliches

- **Marken:** Siemens, TIA Portal, SIMATIC und PLCSIM Advanced sind Marken der Siemens AG. SecNet Labor ist ein unabhängiges Programm von PLCPrime und nicht mit Siemens verbunden.
- **Nutzung:** Das Programm wird ohne Gewähr und auf eigene Verantwortung genutzt. Es dient dem Lernen und Testen und ist nicht für den Einsatz an echten Anlagen gedacht.
- **Npcap:** Für den Live-Modus wird Npcap benötigt. Es ist nicht im Paket enthalten, Sie installieren es selbst von `npcap.com`. Die Lizenzbedingungen von Npcap gelten für Ihre Nutzung.
- **Datenschutz:** Das Programm lauscht nur auf dem eigenen Rechner (`127.0.0.1`), braucht kein Internet und überträgt keine Daten. Die Schriften sind im Programm enthalten (SIL Open Font License).
- **Systemänderungen:** „PC anbinden“ ändert die Adresse des PLCSIM-Adapters und legt Routen an. Dafür fragt Windows nach Administratorrechten. Beim Beenden werden die Routen wieder entfernt.

Kontakt: support@plcprime.io · plcprime.io · Impressum