SecNet Labor

Esercitarsi e provare la sicurezza di rete industriale sul PC: VLAN, firewall, NAT e inoltro di porte

Manuale · Versione del 4 novembre 2026

Per Windows · facoltativamente con Siemens PLCSIM Advanced

PLCPrime

Indice

Questo manuale ti guida passo dopo passo attraverso SecNet Labor: dal primo avvio alla pianificazione di una rete, fino a regole firewall, NAT e collegamento di simulazioni PLC reali.

1	Che cos'è SecNet Labor?	2
2	Installazione e avvio	3
3	L'interfaccia in sintesi	4
4	Pianificare una rete	5
5	Firewall e stateful inspection	7
6	Provare le connessioni	9
7	Live con PLCSIM Advanced	11
8	TIA Portal attraverso il firewall: collegare il PC	12
9	NAT 1:1: indirizzi uguali, raggiungibili senza ambiguità	14
10	Inoltro di porte (NAPT) e OPC UA	18
11	Collegare due switch di sicurezza (trunk)	21
12	Progetti, esempi e PDF	23
13	Risoluzione dei problemi	24
14	Note e informazioni legali	25

> **SULL'INTERFACCIA**
> L'interfaccia è disponibile in tedesco, inglese e italiano. Cambia la lingua con **DE**, **EN** o **IT** in alto nella finestra del programma. Le immagini di questo manuale mostrano l'interfaccia in italiano.

1 Che cos'è SecNet Labor?

SecNet Labor è un programma di esercitazione e di prova per la sicurezza di rete nell'automazione. Invece di usare hardware reale, ricostruisci le reti industriali sul PC e le provi. Puoi verificare in sicurezza concetti di zone e regole firewall, risalire agli errori e svolgere corsi di formazione senza mettere a rischio un impianto reale.

Che cosa puoi fare

- **Pianificare la rete:** trascina sull'area di lavoro PLC, dispositivi IO, PC HMI e di engineering, switch normali e switch di sicurezza e collegali con i cavi.
- **Configurare lo switch di sicurezza:** VLAN e zone, porte access e trunk, routing, route statiche, regole firewall con stateful inspection, NAT (1:1, mascheramento, inoltro di porte), sul modello di uno switch di sicurezza industriale.
- **Verificare:** un pacchetto di prova mostra passo dopo passo quale percorso segue e quale regola lo lascia passare o lo blocca. La matrice di comunicazione mostra chi può parlare con chi.
- **Live con PLCSIM Advanced:** i PLC simulati vengono collegati e il loro traffico reale (ad esempio PUT/GET oppure OPC UA) passa attraverso lo switch simulato. Ciò che il firewall blocca non arriva davvero al PLC.

Due modalità

Modalità	Che cosa offre
Modalità modello (senza PLCSIM)	Pianificare e verificare nel programma: tracciamento del percorso, matrice, controllo della configurazione. Non scorre traffico reale.
Modalità live (con PLCSIM Advanced e Npcap)	In più, il traffico reale tra le istanze PLCSIM passa attraverso lo switch simulato, con log firewall live e I/O live sui dispositivi IO.

> **IMPORTANTE**
> Siemens, TIA Portal e PLCSIM Advanced sono marchi di Siemens AG. SecNet Labor è un programma indipendente e non è collegato a Siemens. Serve per imparare e provare, non per l'uso su impianti reali.

2 Installazione e avvio

Requisiti

Che cosa	A che serve	Obbligatorio?
Windows con Microsoft Edge	Il programma apre la sua finestra con Edge (incluso in Windows).	sì
Siemens PLCSIM Advanced	I PLC simulati. Impostazione «TCP/IP Single Adapter» con `<Local>`.	solo per la modalità live
Npcap (`npcap.com`)	Permette al programma di inoltrare il traffico tra le istanze. Spesso è già presente, ad esempio con Wireshark.	solo per la modalità live

Avvio

1. **Decomprimi** il file ZIP in una cartella propria. Non avviare il programma direttamente dal file ZIP.
2. Avvia `SecNetLabor.exe` con un doppio clic. Si apre una finestra propria.
3. Al primo avvio Windows mostra un avviso perché il programma non è firmato: clicca su **«Ulteriori informazioni»** e poi su **«Esegui comunque»**.

Lingua: il programma si avvia nella lingua di Windows (tedesco o italiano; con qualsiasi altra lingua si avvia in inglese). Per cambiarla clicca su **DE**, **EN** o **IT** nell'intestazione in alto nella finestra del programma. Il programma ricorda la scelta.

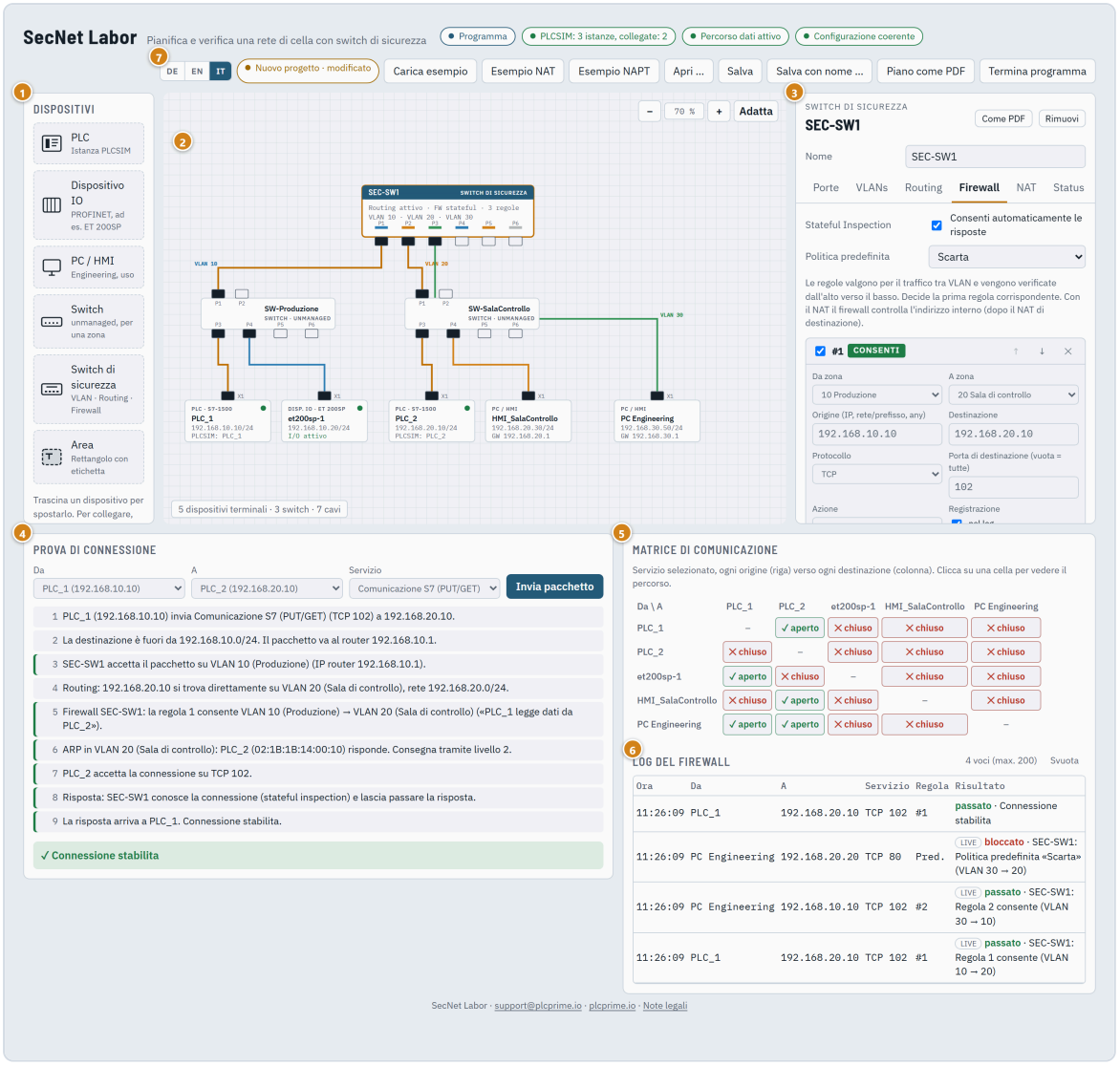
Chiusura

Chiudere la finestra con la **X non** termina il programma: lo switch simulato continua a funzionare in background (icona nell'area di notifica accanto all'orologio), così le connessioni non si interrompono. Per uscire ci sono due modi:

- Clicca in alto nella finestra del programma su **«Termina programma»**.
- Oppure clicca con il tasto destro sull'icona nell'area di notifica e scegli **«Termina SecNet Labor»**.

> **SUGGERIMENTO**
> Dopo la chiusura non esiste più alcun router simulato e le connessioni tra le zone si interrompono. Se avevi collegato il PC con «Collega PC», le route create vengono rimosse automaticamente (vedi capitolo 8).

3 L’interfaccia in sintesi



La finestra del programma con lo scenario «Carica esempio». I numeri sono spiegati sotto.

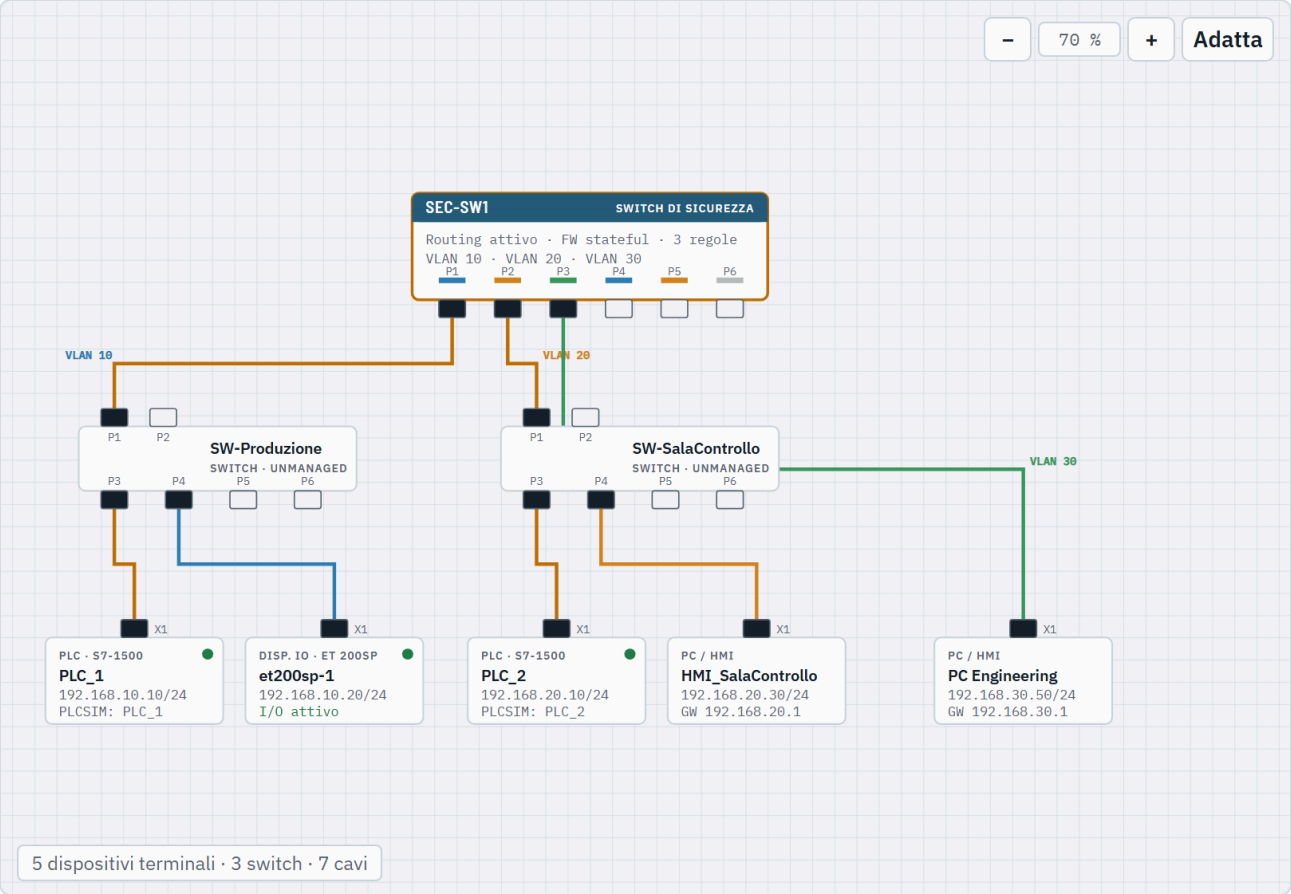
1. **Barra dei dispositivi:** PLC, dispositivo IO, PC/HMI, switch, switch di sicurezza e area. Trascina un dispositivo sull’area di lavoro.
2. **Area di lavoro:** qui costruisci la rete. Rotellina del mouse per lo zoom, trascina su uno spazio libero per spostare la vista.
3. **Ispettore:** mostra le impostazioni del dispositivo selezionato. Per lo switch di sicurezza sono divise in schede.
4. **Prova di connessione:** scegli origine, destinazione e servizio, poi «Invia pacchetto». Il percorso appare passo dopo passo.
5. **Matrice di comunicazione:** chi può parlare con chi? Clicca su una cella per vedere il percorso.
6. **Log del firewall:** ogni decisione del firewall. Le voci con «LIVE» provengono dal traffico reale.
7. **Intestazione:** cambiare la lingua (DE EN IT), caricare esempi, aprire e salvare progetti, piano come PDF, chiudere il programma.

Gli indicatori di stato in alto mostrano il programma, le istanze PLCSIM e il percorso dati. L’ultimo, **«Configurazione coerente»** oppure **«n avvisi»**, controlla di continuo il tuo piano: indirizzi non validi, dispositivi senza router, conflitti IP nello stesso segmento, indicazioni NAT e firewall errate. Clicca su uno switch di sicurezza e sulla scheda «Stato» per leggere gli avvisi in chiaro.

4 Pianificare una rete

Aggiungere e collegare i dispositivi

1. **Trascina un dispositivo** dalla barra a sinistra sull'area di lavoro. In alternativa apri un esempio con «Carica esempio».
2. **Trascina con il mouse da una porta a un'altra porta** per posare un cavo. Funziona anche cliccando due porte una dopo l'altra.
3. Clicca su un dispositivo: a destra, nell'ispettore, imposti nome, indirizzo IP, maschera di sottorete e **router**. Elimina la selezione con il tasto **Canc**.

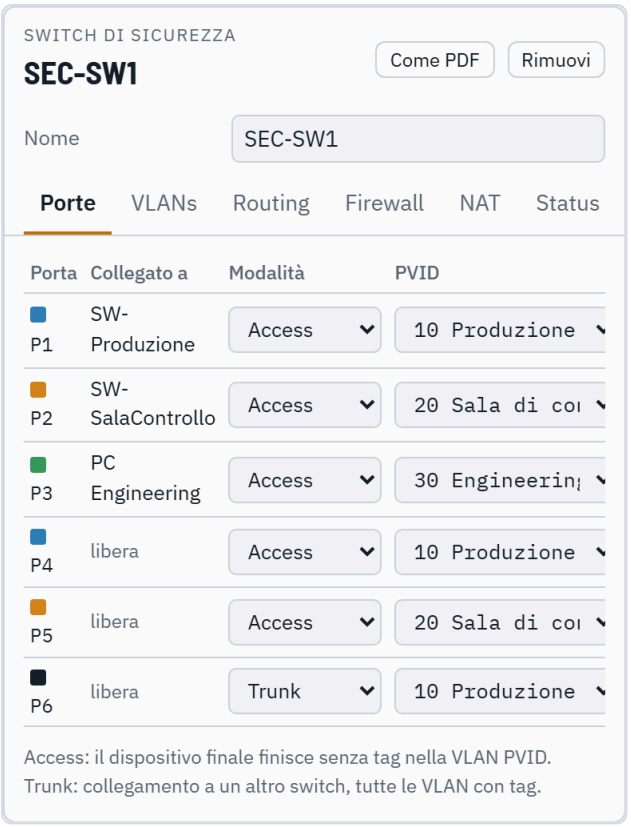


Esempio: due zone (produzione, sala di controllo) e una rete di engineering su uno switch di sicurezza. Arancione e verde sono VLAN diverse.

> **IMPORTANTE**
> Ogni PLC e ogni dispositivo ha bisogno del **router** se deve parlare con un'altra rete. Come router inserisci l'**IP router della VLAN** sullo switch di sicurezza. Altrimenti la risposta non torna mai indietro.

Configurare lo switch di sicurezza

Cliccando sullo switch di sicurezza si aprono sei schede nell'ispettore (Porte, VLANs, Routing, Firewall, NAT, Stato). Le impostazioni principali:



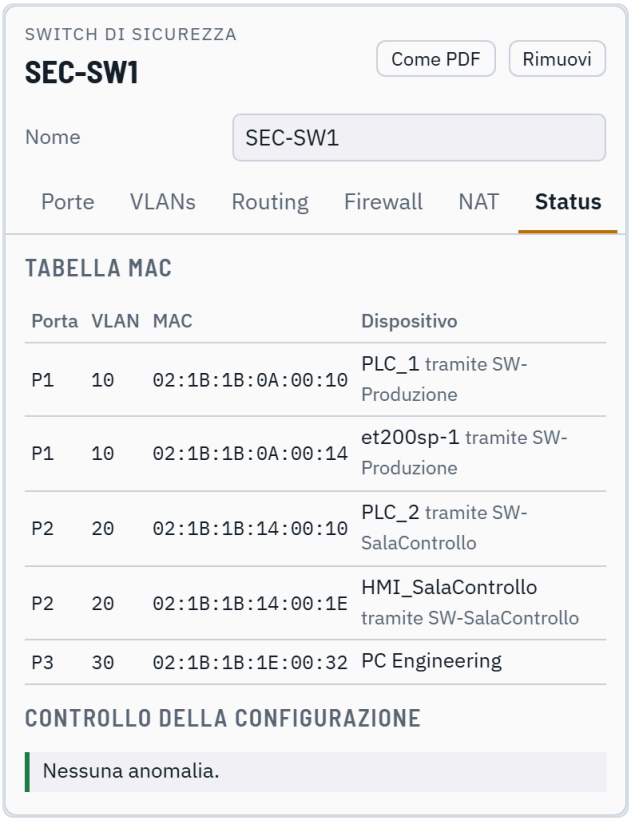
Porte: access (una VLAN) o trunk (tutte le VLAN, per il collegamento a un altro switch)



VLAN: nome, IP router e maschera. Ogni VLAN con IP router è una zona firewall.



Routing: attivare o disattivare il routing tra le VLAN, inserire route statiche

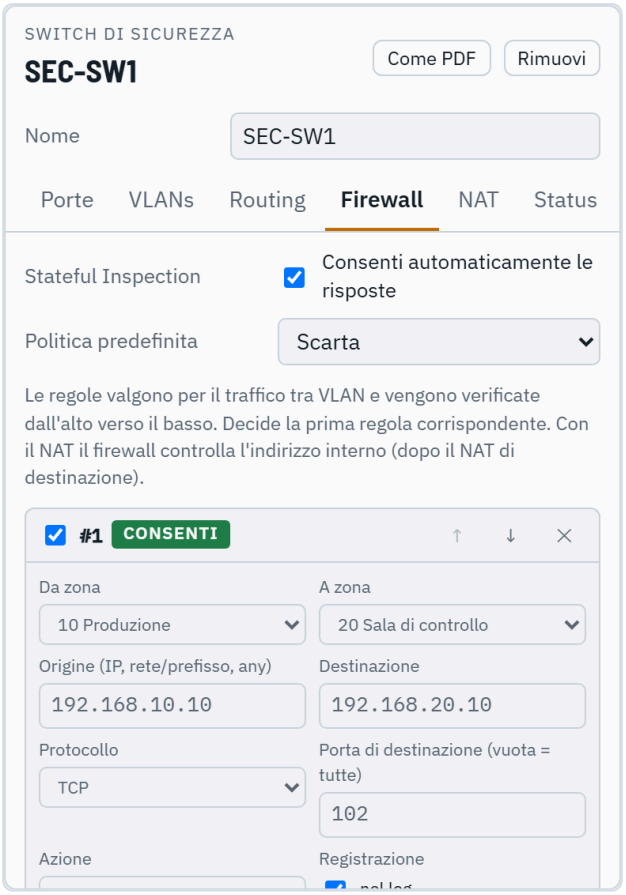


Stato: dispositivi collegati con indirizzo MAC e controllo della configurazione

Con lo strumento **«Area»** posizioni rettangoli colorati con etichetta dietro il tuo piano, ad esempio per «rete di stabilimento» o «macchina 1». Così anche i piani più grandi restano leggibili.

5 Firewall e stateful inspection

Il firewall dello switch di sicurezza controlla il traffico **tra** le VLAN. All'interno di una VLAN non controlla. Le regole vengono lette dall'alto verso il basso e **decide la prima regola corrispondente**. Se nessuna regola corrisponde, vale la **politica predefinita** (di solito «Scarta»).



Scheda «Firewall»: stateful inspection, politica predefinita e regole. Ogni regola ha zone, origine, destinazione, protocollo, porta di destinazione e azione.

Creare una regola

1. Clicca sullo switch di sicurezza, apri la scheda **Firewall** e clicca su **«Aggiungi regola»**.
2. Scegli **Da zona** e **A zona**, inserisci origine e destinazione come indirizzo IP, rete (ad esempio `192.168.10.0/24`) oppure `any`.
3. Imposta **Protocollo** e **Porta di destinazione** (per S7 ad esempio TCP 102). Una porta vuota significa tutte le porte.
4. Scegli l'**Azione** «Consenti» o «Scarta». Con «Registrazione» spuntato la decisione compare nel log.

Che cosa significa stateful inspection

Con la **stateful inspection** attiva il firewall ricorda ogni connessione consentita e lascia rientrare automaticamente le **risposte**. Ti serve una sola regola, per la direzione in cui viene aperta la connessione. Se disattivi la stateful inspection, anche il traffico nella direzione opposta richiede una regola propria.

La porta di origine (per esperti)

Una regola può richiedere inoltre una **porta di origine**. Il campo compare solo dove serve: con la stateful inspection disattivata o quando è già inserita una porta di origine. La risposta di un servizio torna con la porta del servizio come porta di origine. Una regola con questa porta di origine consente esattamente le risposte di quel servizio, senza aprire tutte le porte di destinazione.



Senza stateful inspection ogni regola mostra il campo «Porta di origine».

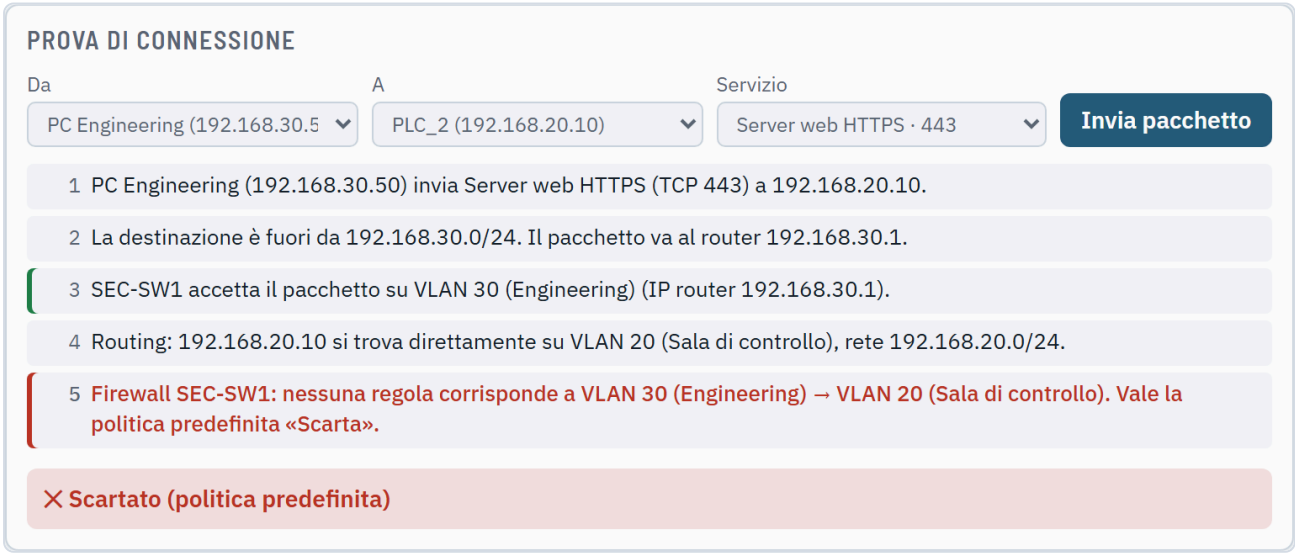
6 Provare le connessioni

Inviare un pacchetto di prova

1. In **«Da»** scegli il dispositivo mittente, in **«A»** la destinazione e in **«Servizio»** il protocollo (ad esempio comunicazione S7, server web, OPC UA, ping).
2. Clicca su **«Invia pacchetto»**. Sotto compare il percorso del pacchetto passo dopo passo: verde per i passi consentiti, rosso per il passo in cui il pacchetto si ferma.



Il pacchetto da PLC_1 a PLC_2 passa: router, regola firewall 1, ARP, porta di destinazione aperta, risposta di ritorno.



La stessa destinazione con un altro servizio: il firewall scarta il pacchetto perché nessuna regola corrisponde. Il risultato è sotto il percorso.

La matrice di comunicazione e il log

Per il servizio scelto la **matrice di comunicazione** mostra a colpo d'occhio chi può parlare con chi («✓ aperto» o «✕ chiuso»). Cliccando su una cella il percorso compare nella casella di prova. Il **log del firewall** raccoglie le decisioni (al massimo 200 voci, «Svuota» lo svuota). Le regole senza spunta su «Registrazione» non vi compaiono.

MATRICE DI COMUNICAZIONE

Servizio selezionato, ogni origine (riga) verso ogni destinazione (colonna). Clicca su una cella per vedere il percorso.

Da \ A	PLC_1	PLC_2	et200sp-1	HMI_SalaControllo	PC Engineering
PLC_1	–	✓ aperto	✕ chiuso	✕ chiuso	✕ chiuso
PLC_2	✕ chiuso	–	✕ chiuso	✕ chiuso	✕ chiuso
et200sp-1	✓ aperto	✕ chiuso	–	✕ chiuso	✕ chiuso
HMI_SalaControllo	✕ chiuso	✓ aperto	✕ chiuso	–	✕ chiuso
PC Engineering	✓ aperto	✓ aperto	✕ chiuso	✕ chiuso	–

LOG DEL FIREWALL

4 voci (max. 200) Svuota

Ora	Da	A	Servizio	Regola	Risultato
11:26:09	PLC_1	192.168.20.10	TCP 102	#1	**passato** · Connessione stabilita
11:26:09	PC Engineering	192.168.20.20	TCP 80	Pred.	LIVE **bloccato** · SEC-SW1: Politica predefinita «Scarta» (VLAN 30 → 20)
11:26:09	PC Engineering	192.168.10.10	TCP 102	#2	LIVE **passato** · SEC-SW1: Regola 2 consente (VLAN 30 → 10)
11:26:09	PLC_1	192.168.20.10	TCP 102	#1	LIVE **passato** · SEC-SW1: Regola 1 consente (VLAN 10 → 20)

Matrice e log. «LIVE» indica le decisioni del traffico reale, le altre voci sono prove nel programma.

PROFINET

PLCSIM Advanced non simula PROFINET IO. Il controllo per i dispositivi IO valuta quindi solo la **pianificazione**: controller e dispositivo IO sono nello stesso segmento e nella stessa sottorete IP? In caso contrario, in modalità live il programma blocca i dati I/O del dispositivo IO.

7 Live con PLCSIM Advanced

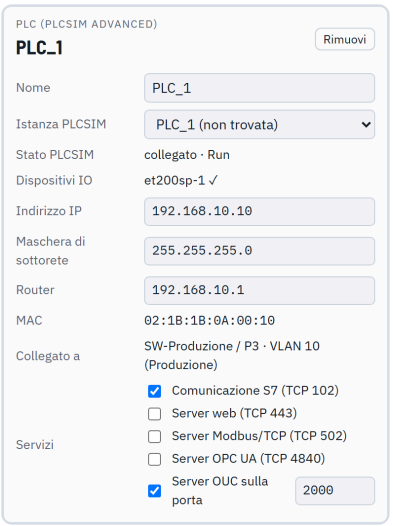
In modalità live il traffico reale delle tue istanze PLCSIM passa attraverso lo switch simulato. Il programma agisce come router nella rete PLCSIM: per ogni IP router di una VLAN risponde con un proprio indirizzo MAC. I pacchetti tra sottoreti diverse vengono instradati, controllati con le regole firewall (con stateful inspection) e inoltrati o scartati.

Preparazione

1. Imposta **PLCSIM Advanced** su «TCP/IP Single Adapter» con `<Local>` e avvia le istanze. **Npcap** deve essere installato.
2. In **TIA Portal** inserisci l'indirizzo IP di ogni PLC e imposta **«Usa router»** con l'IP router della VLAN (come nel piano). Per PUT/GET consenti l'accesso da parte del partner remoto. Carica il progetto nell'istanza.
3. In **SecNet Labor** scegli per ogni PLC nell'ispettore l'**istanza PLCSIM**. Un punto verde sul PLC indica la connessione. Un'istanza appartiene sempre a un solo PLC.
4. La riga di stato in alto dovrebbe indicare «Percorso dati attivo».



Gli indicatori di stato in alto: programma, istanze PLCSIM, percorso dati e controllo della configurazione.



Ispettore di un PLC: istanza PLCSIM, stato della connessione, indirizzo IP, router e servizi.

Esempio: PUT/GET tra due PLC

PLC_1 legge dati da PLC_2 con GET. Finché la regola firewall è **attiva**, i dati arrivano a PLC_1. Se disattivi la regola, la trasmissione si interrompe e il log mostra «bloccato». Se la riattivi, riprende. Nel log ogni decisione compare con «LIVE» e la regola che l'ha presa.

> **SUGGERIMENTO**
> L'indirizzo del partner in GET/PUT è l'indirizzo dell'altro PLC (qui PLC_2). Con NAT o NAPT è l'**indirizzo esterno** (vedi capitoli 9 e 10).

8 TIA Portal attraverso il firewall: collegare il PC

Anche l'accesso del tuo PC di engineering (TIA Portal) può passare attraverso il firewall simulato. Ci sono due possibilità.

Possibilità 1: due indirizzi sull'adattatore (sconsigliata)

Nell'adattatore Windows «PLCSIM Virtual Ethernet» inserisci indirizzi di entrambe le reti. Il PC si trova così direttamente in entrambe le zone e parla con il PLC **aggirando lo switch di sicurezza**. È utile per caricare un progetto, ma non mette alla prova il firewall.

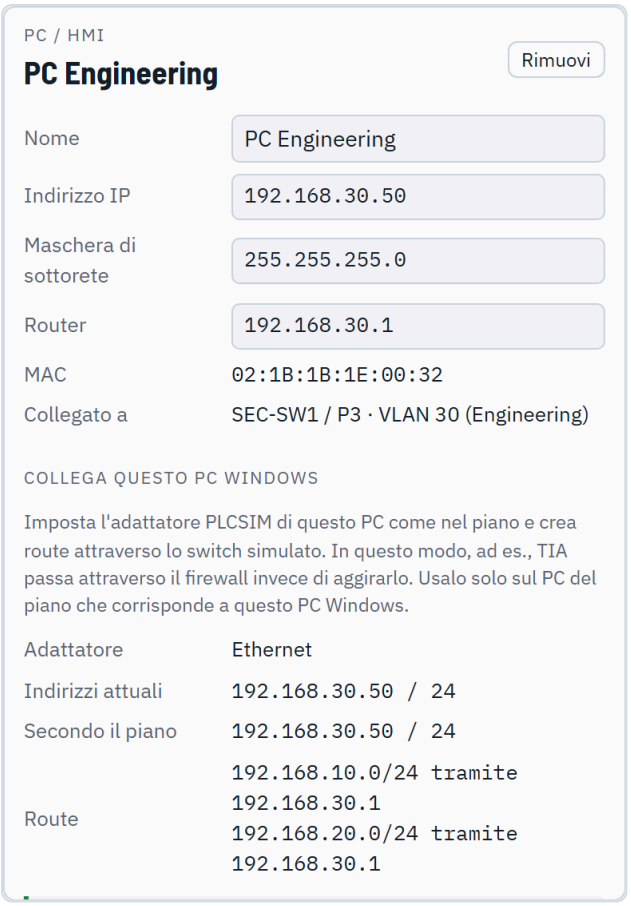
Possibilità 2: «Collega PC» (consigliata)

Il PC Windows diventa esso stesso un dispositivo nel piano (ad esempio «PC Engineering» con IP e router). Con il pulsante **«Collega PC»** il programma imposta l'adattatore PLCSIM del PC come il PC compare nel piano e crea route verso le altre reti. Allora anche TIA passa attraverso il firewall e richiede regole adatte (ad esempio TCP 102 per online e caricamento, ICMP per il ping).

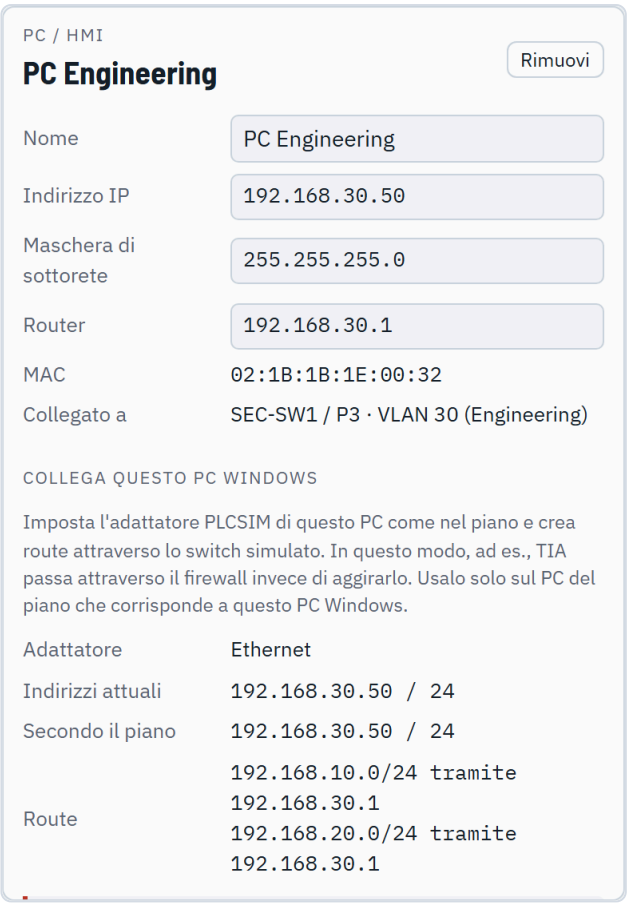
1. Clicca sul PC nel piano (indirizzo IP e router come nella rete, ad esempio `192.168.30.50` e router `192.168.30.1`).
2. In basso nell'ispettore, sotto «Collega questo PC Windows», clicca su **«Collega PC»** e conferma la richiesta di Windows (diritti di amministratore).
3. **Spegni e riaccendi una volta le istanze PLCSIM**, perché il loro indirizzo MAC dipende dall'indirizzo dell'adattatore.
4. Vai online in TIA. Se TIA chiede un altro indirizzo IP («Assegnare indirizzo IP?»), clicca su **«No»**. Il routing è attivo, non serve aggiungere alcun indirizzo.

Che cosa succede alle route

- Vengono create solo route per le reti dello switch di sicurezza il cui router è usato dal PC.
- Se una rete del piano si sovrappone a una **rete reale del tuo PC** (ad esempio il WLAN `192.168.1.0/24`), il programma **non** crea alcuna route per essa e te lo segnala. Altrimenti il tuo traffico reale finirebbe nello switch simulato.
- **Alla chiusura del programma** le route create vengono rimosse di nuovo (Windows chiede i diritti di amministratore). L'indirizzo sull'adattatore resta. **«Scollega di nuovo»** ripristina lo stato precedente al primo collegamento.



Il blocco «Collega questo PC Windows»: adattatore, indirizzi, route creata e stato



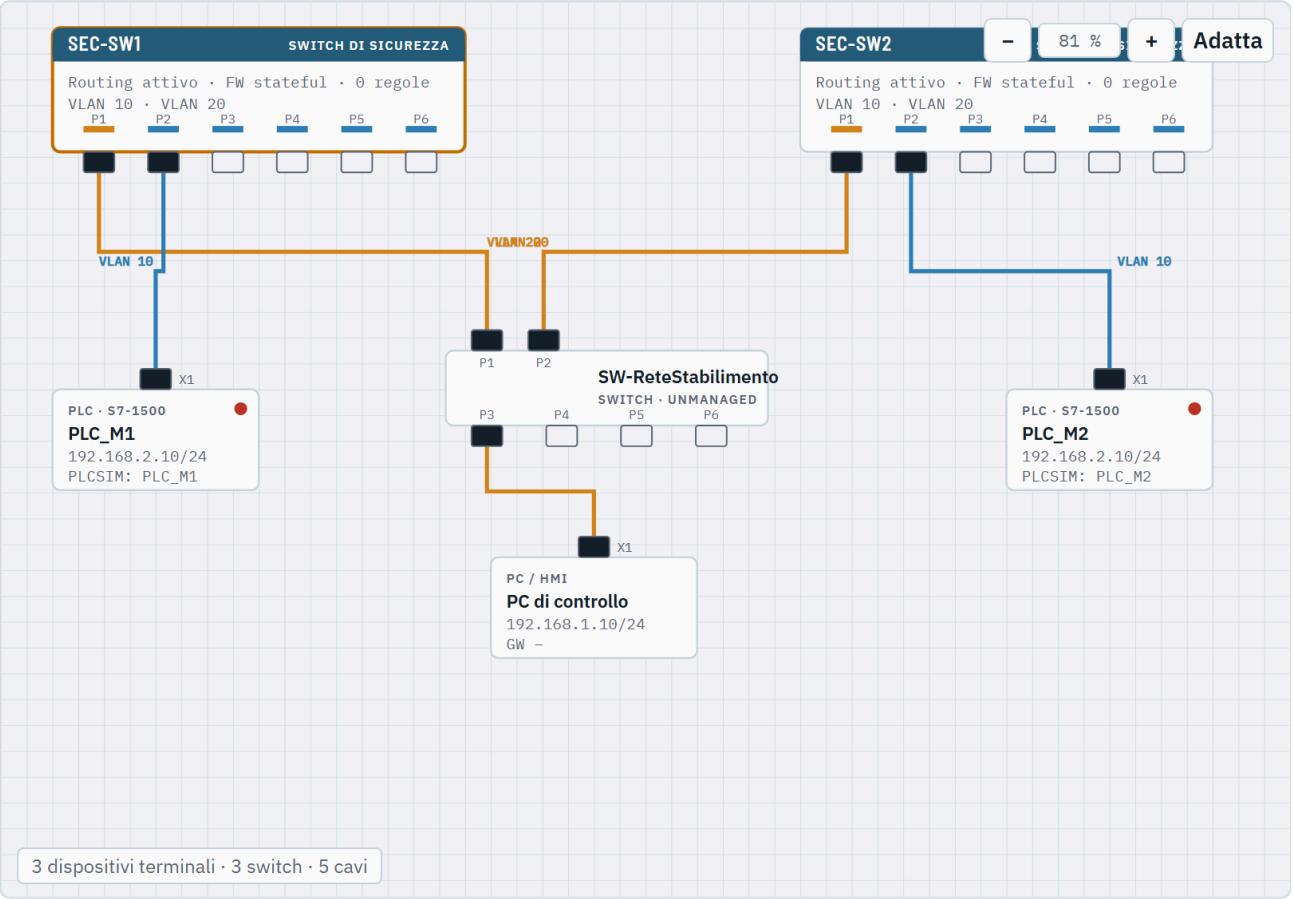
L'avviso «Windows reindirizza una rete reale» con il pulsante per ripulire

Controllare le route sul PC

In PowerShell con `route print -4`. Dopo la chiusura del programma sotto «Route permanenti» non dovresti trovare più nulla di SecNet Labor. Se è ancora presente una route che reindirizza una rete reale nello switch simulato, il programma mostra un avviso rosso con il pulsante **«Rimuovi route in conflitto»**.

9 NAT 1:1: indirizzi uguali, raggiungibili senza ambiguità

I PLC vengono spesso forniti con il loro indirizzo IP predefinito e dopo la consegna spesso non viene cambiato. Se un impianto ha più macchine uguali, tutte hanno lo **stesso indirizzo**. Per renderle raggiungibili in modo univoco si usa il **NAT**: lo switch di sicurezza davanti a ogni macchina le assegna verso l'esterno un indirizzo proprio e riscrive l'indirizzo nel pacchetto.



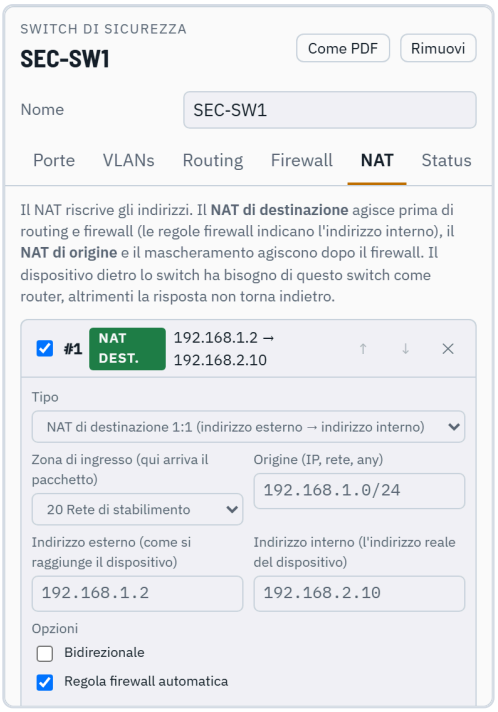
Esempio NAT: PLC_M1 e PLC_M2 hanno entrambi `192.168.20.10`. Il PC di controllo li raggiunge come `192.168.10.2` e `192.168.10.3`.

Come funziona

1. Il sistema di controllo invia qualcosa a `192.168.10.2` (l'indirizzo esterno della macchina 1).
2. Lo switch scrive nel pacchetto come destinazione l'indirizzo reale `192.168.20.10` e lo consegna alla macchina. Ciò avviene **prima** di routing e firewall.
3. La macchina risponde. Lo switch riscrive `192.168.10.2` come mittente. Il sistema di controllo non si accorge della traduzione.

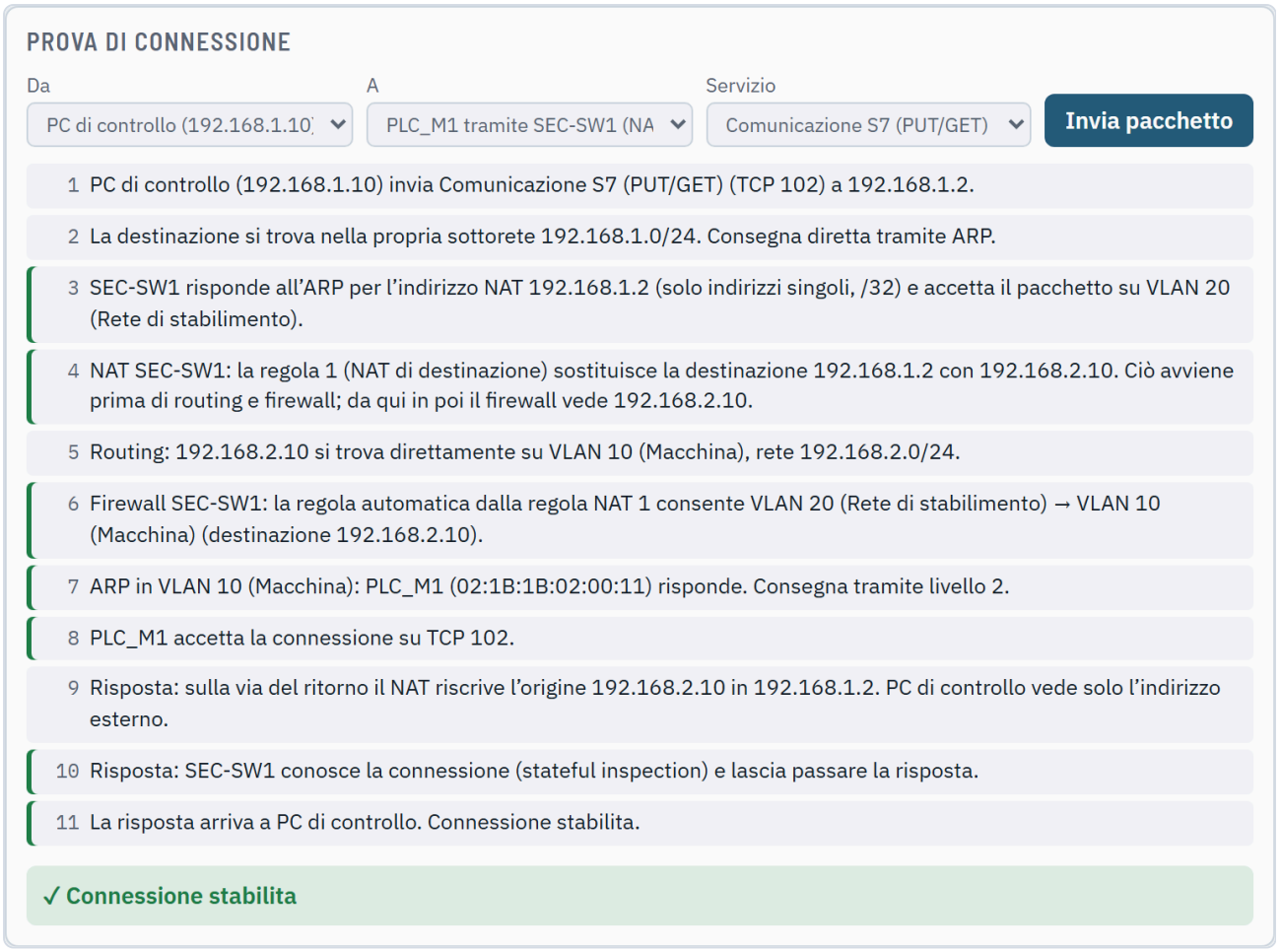
Impostare la regola NAT

Clicca sullo switch di sicurezza, apri la scheda **NAT**, clicca su «Aggiungi regola NAT», tipo **«NAT di destinazione 1:1 (indirizzo esterno → indirizzo interno)»**.



NAT di destinazione: zona di ingresso, origine, indirizzo esterno e indirizzo interno. Le opzioni «Bidirezionale» e «Regola firewall automatica» sono sotto.

Campo	Significato
Zona di ingresso	In questa zona arriva il pacchetto (qui la rete di stabilimento).
Origine	Chi può usare l’indirizzo esterno (IP, rete oppure `any`).
Indirizzo esterno	Come la macchina viene indirizzata dall’esterno. Un indirizzo singolo (`/32`) viene soddisfatto dallo switch anche tramite ARP.
Indirizzo interno	L’indirizzo reale della macchina.
Regola firewall automatica	Lo switch consente automaticamente il traffico verso l’indirizzo interno. Senza la spunta serve una regola firewall propria con l’**indirizzo interno**.
Bidirezionale	Anche quando la macchina stessa apre una connessione verso l’esterno, compare con il suo indirizzo esterno.



La prova da «PC di controllo» a «PLC_M1 tramite SEC-SW1 (NAT 192.168.1.2)»: lo switch risponde all'ARP per l'indirizzo esterno e riscrive la destinazione.

Importante con il NAT

- **Router sul PLC:** il PLC deve avere lo switch di sicurezza (IP router della VLAN della macchina) inserito come router, altrimenti la risposta non torna indietro.
- **Il firewall vede l'indirizzo interno.** Una regola propria con l'indirizzo esterno non scatta mai, perché la destinazione viene riscritta prima del firewall.
- **In TIA** inserisci come indirizzo del partner (ad esempio per GET) l'**indirizzo modificato dal NAT**, anche se il PLC in realtà ne ha un altro. Le connessioni configurate su entrambi i lati con l'IP del partner non funzionano con il NAT. Usa GET/PUT da un solo lato.
- Indirizzi IP uguali dietro switch di sicurezza **diversi** sono consentiti. Il controllo della configurazione segnala un conflitto IP solo nello stesso segmento.

> **LIMITE IN MODALITÀ LIVE**
> Su un adattatore PLCSIM può esserci una sola istanza per indirizzo. Due macchine uguali con lo stesso IP si possono quindi mostrare solo **nel piano**. Per una prova live assegna alla seconda macchina un altro indirizzo interno.

Comunicazione tra macchine

Se due macchine uguali devono parlare tra loro (la macchina 2 chiama la macchina 1), serve inoltre un **NAT di origine** sullo switch della macchina che chiama. Altrimenti la macchina 1 vedrebbe come mittente il proprio indirizzo. Serve anche una regola firewall con l'indirizzo di origine **reale**, perché il NAT di origine agisce solo

dopo il firewall.

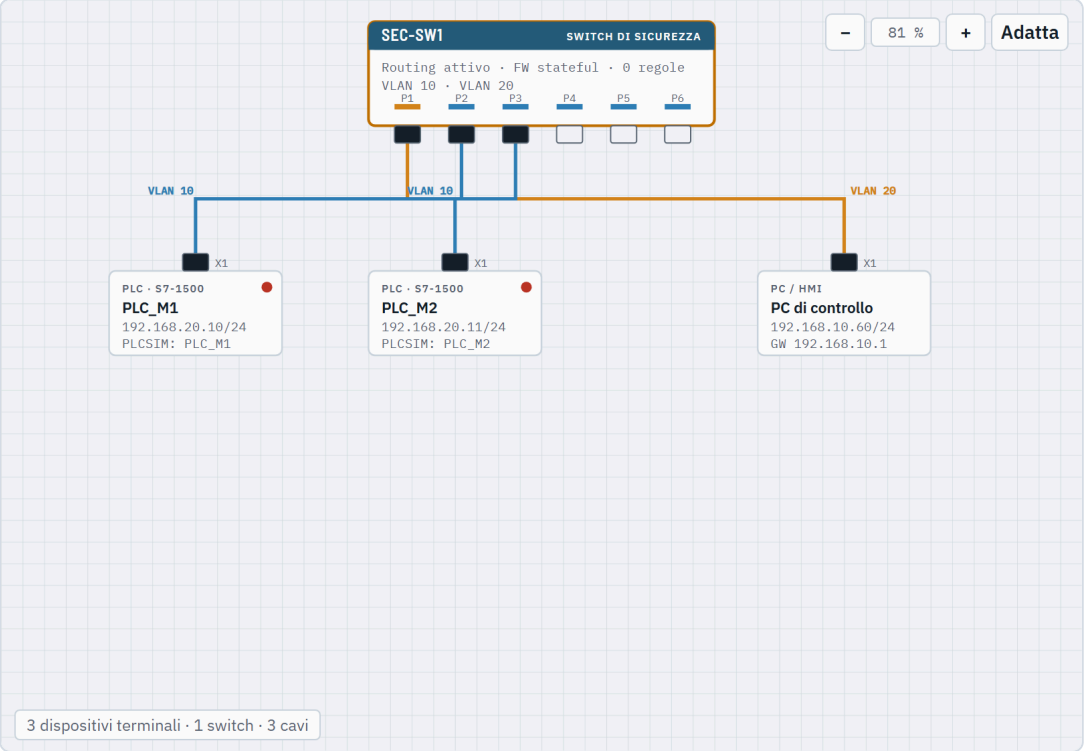


Sullo switch della macchina che chiama: NAT di origine da 192.168.2.10 a 192.168.1.3.

10 Inoltro di porte (NAPT) e OPC UA

Con il **NAPT** lo switch ha **un solo indirizzo esterno** (il suo IP router). I dispositivi dietro di esso li distingue soltanto in base alla **porta**. Il vantaggio: non serve un indirizzo IP libero per ogni dispositivo, ne basta uno solo.

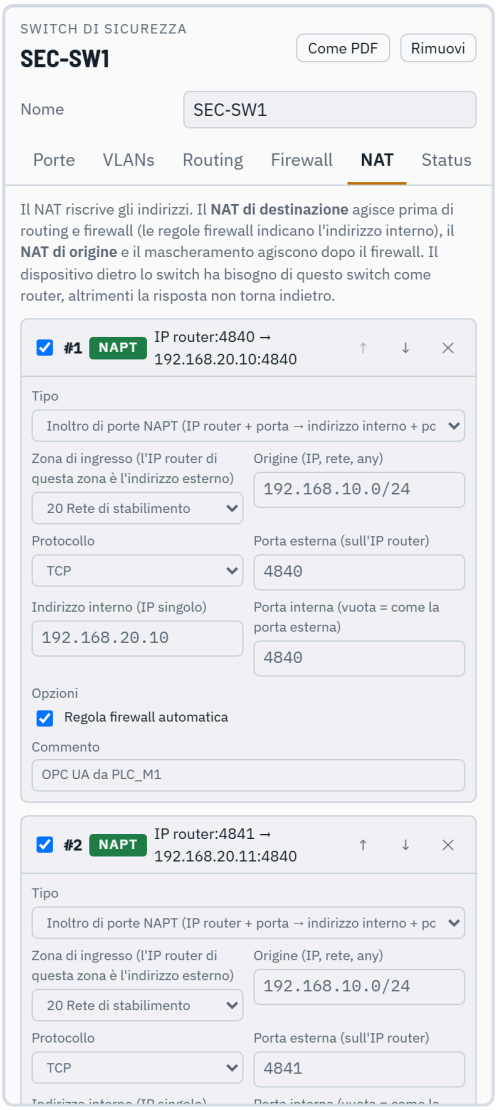
Richiesta dall'esterno	Inoltrata a
`192.168.10.1` , porta `4840`	PLC 1: `192.168.20.10` , porta `4840`
`192.168.10.1` , porta `4841`	PLC 2: `192.168.20.11` , porta `4840`
`192.168.10.1` , porta `8443`	Server web del PLC 1: `192.168.20.10` , porta `443`



Esempio NAPT: due PLC con OPC UA dietro uno switch, raggiungibili tramite il suo IP router.

Le regole NAPT

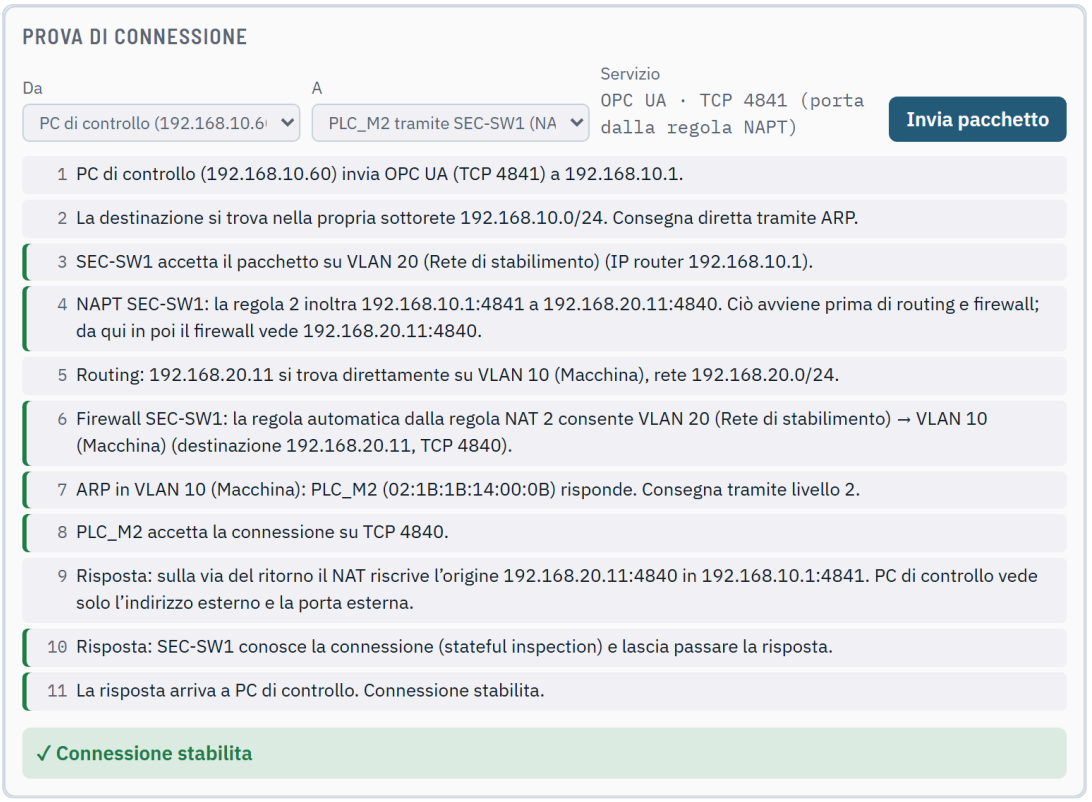
Scheda «NAT», tipo **«Inoltro di porte NAPT (IP router + porta → indirizzo interno + porta)»**. Inserisci la **porta esterna** (sull'IP router), l'**indirizzo interno** e la **porta interna** (vuota significa: uguale alla porta esterna). Con «Regola firewall automatica» lo switch consente esattamente questa combinazione di protocollo e porta interna.



Regole NAPT: due server OPC UA (porte esterne 4840 e 4841); la terza regola (server web, 8443 su 443) segue sotto.

Provare

Sotto **«A»** c'è una voce propria per ogni inoltro, ad esempio «PLC_M2 tramite SEC-SW1 (NAPT 192.168.10.1:4841)». Indirizzo e porta sono così già corretti nella prova e la scelta del servizio scompare.



Prova attraverso l'inoltro: la destinazione viene riscritta in 192.168.20.11:4840 e il firewall vede questo indirizzo interno con la porta interna.

OPC UA con UA Expert (live)

1. In TIA **attiva il server OPC UA** sul PLC, inserisci indirizzo e router come nel piano e carica. In SecNet Labor assegna l'istanza.
2. Collega il PC (capitolo 8) e spegni e riaccendi le istanze.
3. In UA Expert inserisci come server l'**IP router dello switch**: `opc.tcp://192.168.10.1:4840`. Non l'indirizzo del PLC.
4. Nel log del firewall compare «NAPT: 192.168.10.1:4840 → 192.168.20.10:4840». UA Expert trova il PLC e mostra la sua applicazione.

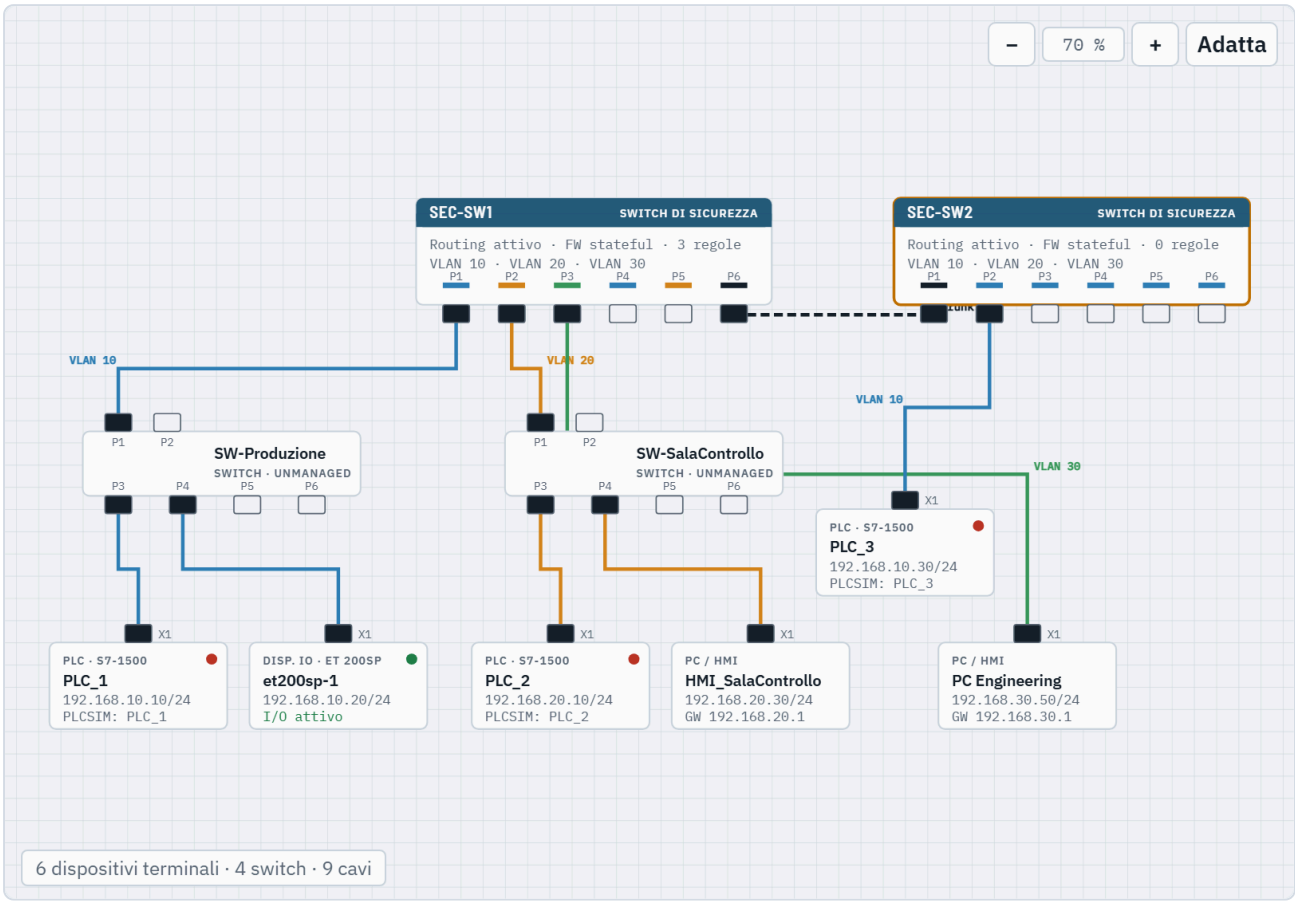
> **DA SAPERE**
> Il PLC comunica al client come endpoint il **proprio** indirizzo (`192.168.20.10`). UA Expert apre quindi spesso la sessione vera e propria direttamente verso quell'indirizzo. Funziona se il PC ha una route verso la rete delle macchine (come dopo «Collega PC»). Quella sessione passa allora instradata normalmente attraverso il firewall, senza NAPT. Nel log lo riconosci perché la voce compare **senza** la nota NAPT. Negli impianti reali senza route verso la rete delle macchine bisogna adattare l'endpoint sul client o sul PLC.

Limiti del NAPT

- Ogni porta esterna può essere inoltrata una sola volta. Una porta inoltrata non è più utilizzabile sullo switch stesso (ad esempio 443 per la sua gestione web).
- I servizi con **porta fissa**, ad esempio S7 (porta 102), possono essere inoltrati su **un** indirizzo solo per **un** dispositivo. Per più macchine uguali con S7 usa il NAT 1:1.

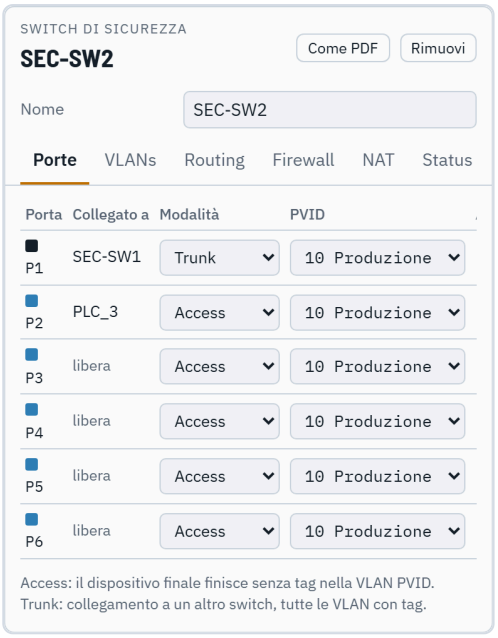
11 Collegare due switch di sicurezza (trunk)

Due switch di sicurezza si possono collegare tramite un **trunk**. Sul trunk tutte le VLAN viaggiano con tag. Così un PLC sul secondo switch può trovarsi nella stessa rete di un PLC sul primo.



SEC-SW1 e SEC-SW2 sono collegati da un trunk (tratteggiato). PLC_3 è sulla VLAN 10 del secondo switch e parla con PLC_1 sul primo.

1. Su **entrambi** gli switch imposta la porta del collegamento su **trunk** nella scheda «Porte» e attivala.
2. Collega le due porte trunk con un cavo.
3. Crea sul secondo switch le stesse VLAN (stesso ID). L'**IP router resta vuoto** ("solo livello 2"). Il router della rete resta il primo switch.
4. Il PLC sul secondo switch riceve un indirizzo della rete della VLAN e come router l'IP router del **primo** switch.



Porte del secondo switch: P1 è il trunk, le altre sono porte access nella VLAN 10.

SUGGERIMENTO

L’IP router per lo switch 2 deve restare libero. Due dispositivi con lo stesso IP router nella stessa rete causerebbero un conflitto IP.

12 Progetti, esempi e PDF



L'intestazione: esempi, progetti, uscita PDF e chiusura.

Pulsante	Che cosa fa
Carica esempio	Una rete pronta con tre zone, due PLC e un firewall.
Esempio NAT	Due macchine uguali con lo stesso indirizzo, ciascuna dietro il proprio switch di sicurezza, raggiungibili tramite NAT.
Esempio NAPT	Due PLC con OPC UA dietro un indirizzo esterno, raggiungibili tramite porte diverse.
Apri ..., Salva, Salva con nome ...	Progetti come file `.json` con le finestre di dialogo di Windows (Ctrl+S salva). Il piano resta anche nel programma ed è di nuovo disponibile al prossimo avvio.
Piano come PDF	Il piano di rete a pagina 1 (A4 orizzontale), poi l'elenco di dispositivi e aree.
Come PDF (sullo switch di sicurezza)	Tutte le impostazioni dello switch su A4: porte, VLAN, routing, regole firewall, NAT, dispositivi collegati e controllo della configurazione.

> **NOTA**
> I file PDF vengono creati dal programma in background con Edge. Può richiedere alcuni secondi. Poi il file si apre.

13 Risoluzione dei problemi

Problema	Possibile causa e soluzione
Il pacchetto risulta «Scartato (politica predefinita)»	Nessuna regola corrisponde. Nella scheda Firewall crea una regola con le zone, gli indirizzi e la porta di destinazione giusti. Con il NAT conta l'**indirizzo interno**.
Il percorso termina con «Percorso di ritorno mancante» o «PLC_2 senza router» (con il nome del dispositivo)	Il dispositivo di destinazione non ha il router. Inserisci l'IP router della VLAN (anche in TIA: «Usa router»).
Il PLC ha un punto rosso	Nessuna istanza PLCSIM scelta o l'istanza non è in esecuzione. Scegli l'istanza nell'ispettore, avviala in PLCSIM.
«Percorso dati spento» in alto	Manca Npcap oppure l'adattatore PLCSIM non è stato trovato. Installa Npcap, imposta PLCSIM su «TCP/IP Single Adapter» con `<Local>`.
TIA non trova il PLC	Nel caricamento scegli «Caricamento esteso», come interfaccia l'adattatore PLCSIM Virtual Ethernet e inserisci l'IP a mano. L'adattatore del PC ha bisogno di un indirizzo nella rete del PLC. Poi spegni e riaccendi le istanze. Controlla le route vecchie (`route print -4`).
Il log mostra continuamente «bloccato» per TCP 102	TIA chiede regolarmente del PLC e la porta 102 non è consentita. Crea una regola per TCP 102 oppure termina la connessione online in TIA.
Dopo «Collega PC» WLAN o Internet sono disturbati	Una route reindirizza una rete reale nello switch. Clicca su «Rimuovi route in conflitto» sul PC oppure chiudi il programma. Controlla con `route print -4`.
NAT: nessuna connessione	Router inserito sul PLC? L'origine nella regola NAT corrisponde? Indirizzo esterno come indirizzo singolo (`/32`)? Regola firewall con l'**indirizzo interno** oppure «Regola firewall automatica»?
NAPT/OPC UA non trova nulla	Inserisci l'IP router dello switch e la **porta esterna**, non l'indirizzo del PLC. Regola attivata? Protocollo TCP? Server OPC UA attivo nel PLC?
La finestra del programma è vuota o non risponde	Ricarica con **Ctrl+R**. Se non basta, chiudi il programma e riavvialo.

ASSISTENZA

Per domande o errori puoi scriverci a **support@plcprime.io**. Allega possibilmente uno screenshot e la voce del log del firewall.

14 Note e informazioni legali

- **Marchi:** Siemens, TIA Portal, SIMATIC e PLCSIM Advanced sono marchi di Siemens AG. SecNet Labor è un programma indipendente di PLCPrime e non è collegato a Siemens.
- **Utilizzo:** il programma è fornito senza garanzia e usato a proprio rischio. Serve per imparare e provare e non è pensato per l'uso su impianti reali.
- **Npcap:** la modalità live richiede Npcap. Non è incluso nel pacchetto, lo installi tu da `npcap.com`. Per il tuo utilizzo valgono le condizioni di licenza di Npcap.
- **Privacy:** il programma ascolta solo sul tuo computer (`127.0.0.1`), non richiede Internet e non trasmette dati. I caratteri sono inclusi nel programma (SIL Open Font License).
- **Modifiche al sistema:** «Collega PC» modifica l'indirizzo dell'adattatore PLCSIM e crea route. Per questo Windows chiede i diritti di amministratore. Alla chiusura del programma le route vengono rimosse di nuovo.

Contatto: support@plcprime.io · plcprime.io · Note legali