HOW TO

Gestione delle porte su Sinema Remote Connect

SIEMENS

Contents

Gestione delle porte su Sinema Remote Connect

La seguente guida illustra quali porte di trasporto (TCP/UDP) vengono utilizzate dal software Siemens Sinema RC Server, come gestirle e cosa è possibile configurare sul server stesso.

La guida è redatta con la versione Sinema RC 3.1

Considerazioni sulle porte e il port forwarding

Come illustrato in altre guide, per il corretto funzionamento del Sinema RC interfacciato su internet è necessario che dall'indirizzo IP o dall'hostname pubblico configurato sul router siano inoltrate le seguenti porte:

- 443 TCP (per HTTPS: configurazione pagina web e auto-enrollment dei device)
- 1194 UDP (OpenVPN su UDP)
- 5443 TCP (OpenVPN su TCP)
- 6220 TCP (procedura di fallback per rinnovo automatico dei certificati in caso di connessione successiva alla scadenza).

Le ultime due porte sono in backup per cui è possibile far funzionare il Sinema RC Server anche solo con la 443 e una fra la 1194 e 5443 ma in caso di problemi non scatterebbero le soluzioni alternative automatiche.
Questo significa che se per esempio avessimo:

- IP pubblico Sinema RC Server (gestito da provider TLC e/o dal proprio router): 1.1.1.1
- IP privato (configurato in fase di installazione o modificato successivamente): 192.168.1.1

Nel router proprio o del provider andranno inserite ad esempio le regole:

- *1.1.1.1:443 TCP -> 192.168.1.1 TCP*
- *1.1.1.1:1194 UDP -> 192.168.1.1:1194 UDP*
- .....

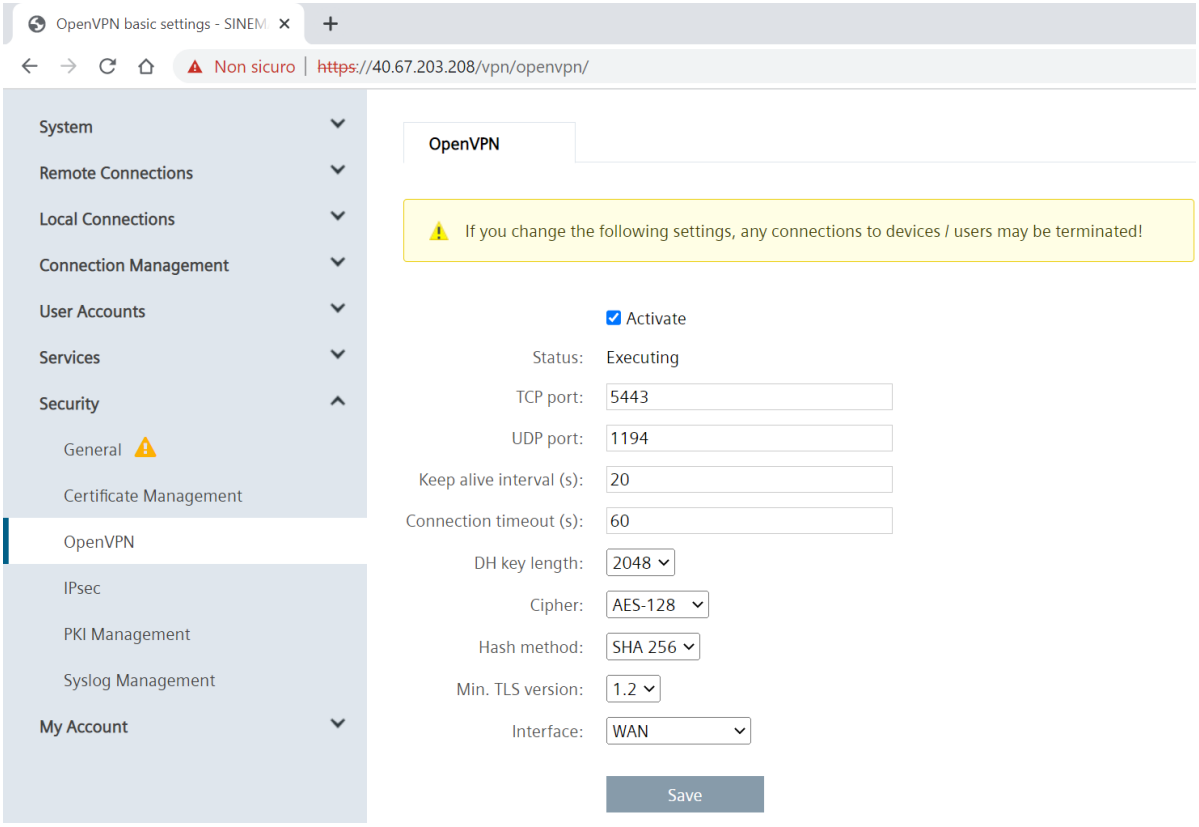
Ovvero tutte le connessioni in ingresso sull'IP pubblico sulle porte specificate sono inoltrate internamente all'IP privato.
L'eventuale firewall sul router va configurato in accordo con queste regole qualora tale impostazione non sia automatica.
Inoltre se il Sinema RC Server è allocato dietro un firewall che blocca le connessioni in uscita, oltre alle suddette porte si raccomanda di permettere la connessione uscente su:

- 53 UDP -> per le connessioni DNS e quindi il raggiungimento del server delle licenze
- 123 UDP -> per le connessioni NTP e quindi la sincronizzazione dell'orologio

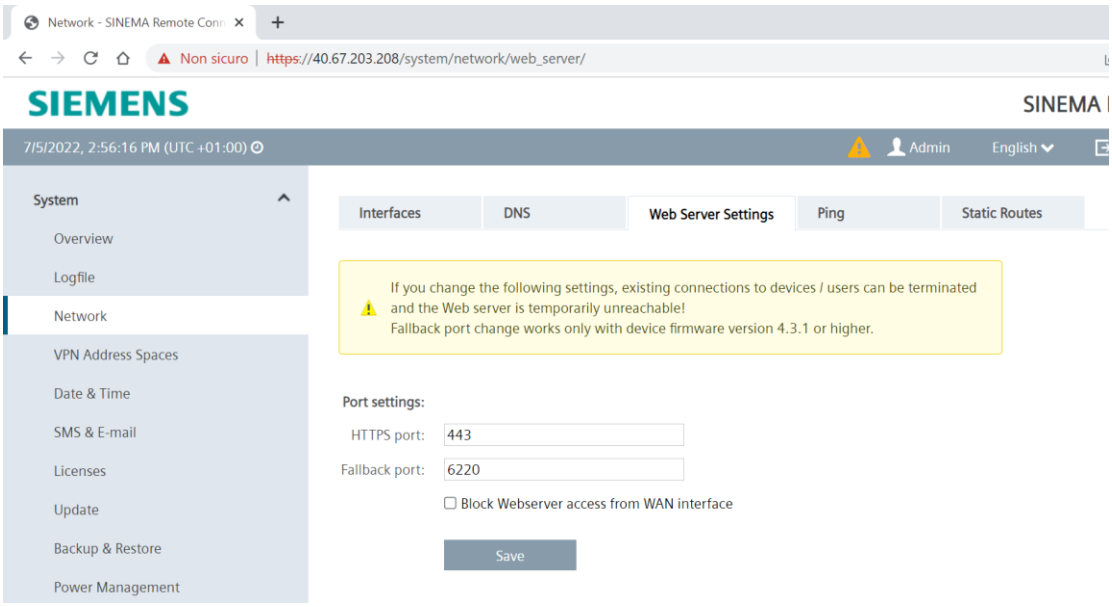
Anche l'uso dell'hostname dinamico (DynDNS) deve essere configurato direttamente sul router.

Configurazione sulle porte

È possibile cambiare le porte di comunicazione per OpenVPN (default 1194UDP e 5443TCP) dal menù Security → OpenVPN

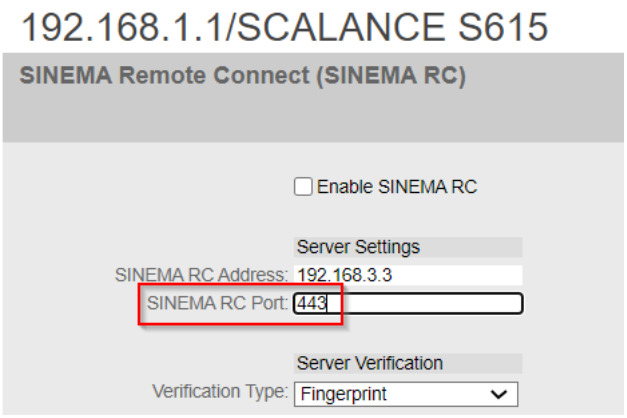


Allo stesso modo è possibile configurare le porte per il Web Server (443) e per la procedura di Fallback (6220) accedendo dal menu "System" → "Network" e selezionando il tab "Web Server Settings"



Notate che una volta cambiata la porta UDP o TCP questa impostazione è valida per tutti i device e client che si debbano connettere al Sinema RC Server

Se ad esempio cambio la 1194 UDP in 1195 UDP i device remoti tenteranno tutti di connettersi tramite quest'ultima porta (anche quelli che si erano connessi in precedenza).
Fa eccezione la porta per HTTPS, essa infatti è configurabile sia sui web browser del dispositivo e su Sinema RC Client mediante la scrittura IP:porta (es: https://1.1.1.1:444 per aprire la porta 444 su indirizzo 1.1.1.1) ma anche sui device con auto-enrollment come lo Scalance S615.



Questo permette di poter utilizzare molteplici porte per la connessione su HTTPS a patto che siano tutte correttamente inoltrate (port forwarding) verso il server che ascolta su un'unica porta.

Con riserva di modifiche e salvo errori.
Il presente documento contiene solo descrizioni generali o informazioni su caratteristiche non sempre applicabili, nella forma descritta, al caso concreto o che possono cambiare a seguito di un ulteriore sviluppo dei prodotti. Le caratteristiche desiderate sono vincolanti solo se espressamente concordate all'atto di stipula del contratto.
Tutte le denominazioni dei prodotti possono essere marchi oppure denominazioni di prodotti della Siemens AG o di altre ditte fornitrici, il cui utilizzo da parte di terzi per propri scopi può violare il diritto dei proprietari.