HOW TO

Configurazione di base del firewall

Contents

Configurazione di base del firewall

Premessa

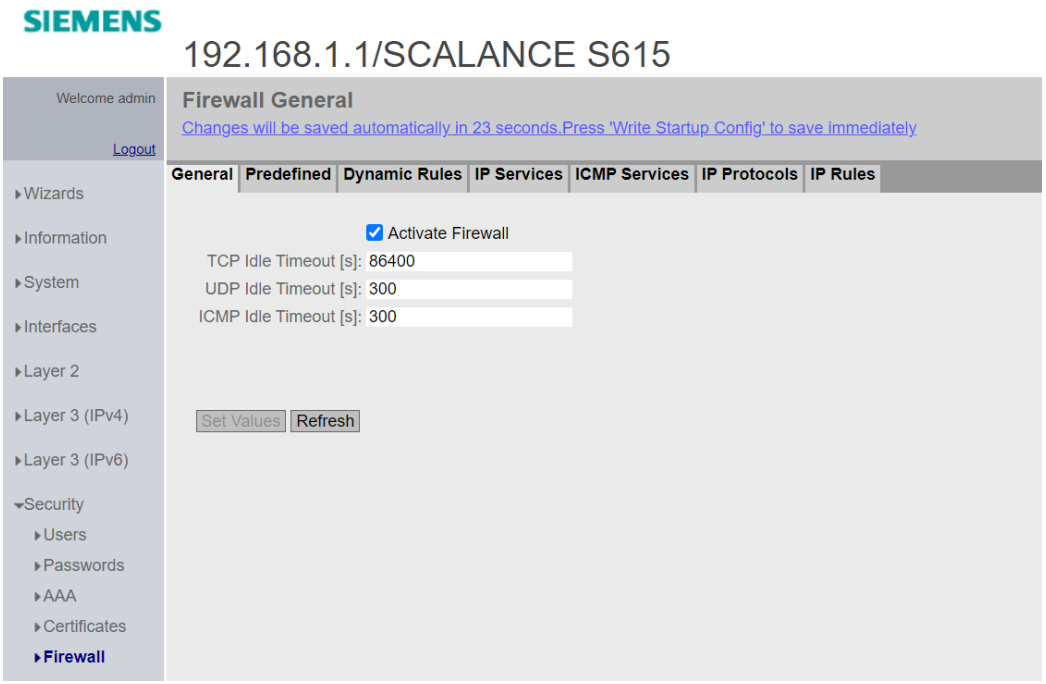
La seguente guida illustra le funzionalità relative ai firewall dei modelli Siemens Scalance S e M e come queste possono essere configurate mediante la gestione web (WBM)

La guida è valida per le versioni firmware fino alla 7.1 per Scalance S615/M800 e 2.3 per Scalance SC600.

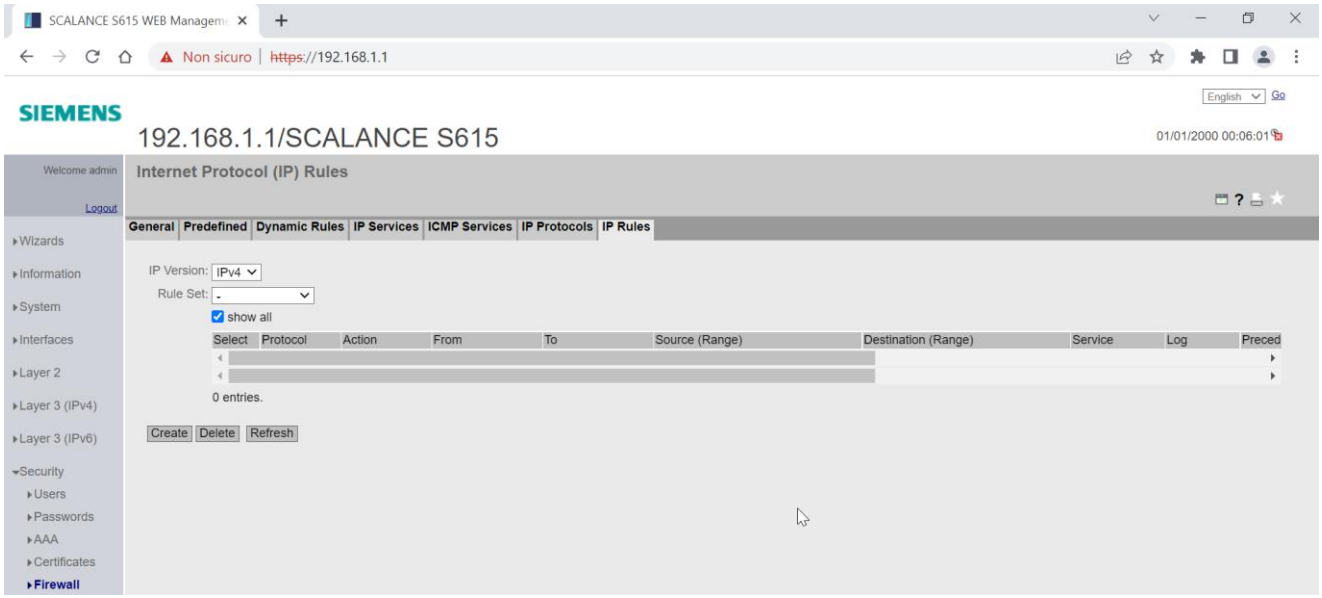
Per funzionalità aggiuntive quali firewall bridge (solo Scalance SC600), regole di firewall su base utente, digital input o trigger temporale così come altre informazioni di base relative agli Scalance, fare riferimento alle guide apposite.

Attivazione del Firewall e parametrizzazione di default

Gli Scalance S/M sono dotati di firewall Stateful Inspection su base L3/L4 (L2 disponibile solo per Scalance SC-600, vedere guida specifica) abilitato di default.
Questo significa che fra le diverse interfacce (es: VLAN1 e VLAN2 per lo Scalance S615) non è possibile comunicare alcun tipo di dato senza una configurazione del firewall che lo permetta.
Il firewall funziona con la politica di Whitelist (tutto è proibito, fuorché ciò che è permesso) e si gestisce dalla schermata Security/Firewall nella pagina web del dispositivo.

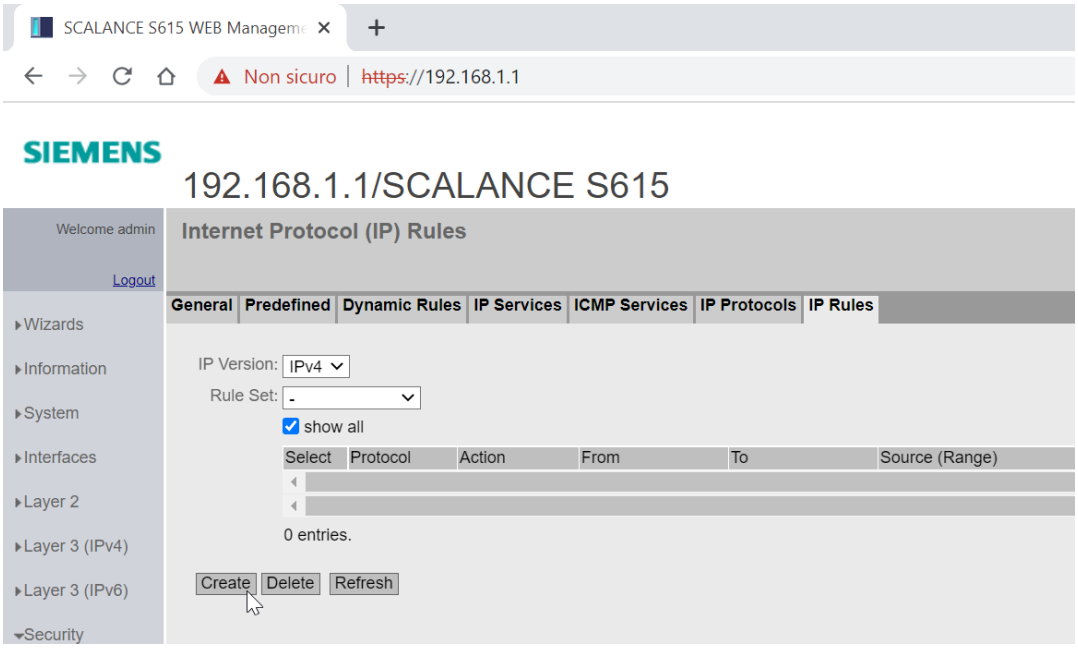


È possibile, disabilitando la spunta nel tab “General”, disattivare il firewall e permettere qualsiasi tipo di comunicazione fra le interfacce, se necessario. **Questa disabilitazione del firewall è fortemente sconsigliata!**
In fase di prima configurazione non sono inserite regole, di conseguenza nessuna comunicazione è permessa a firewall attivo.

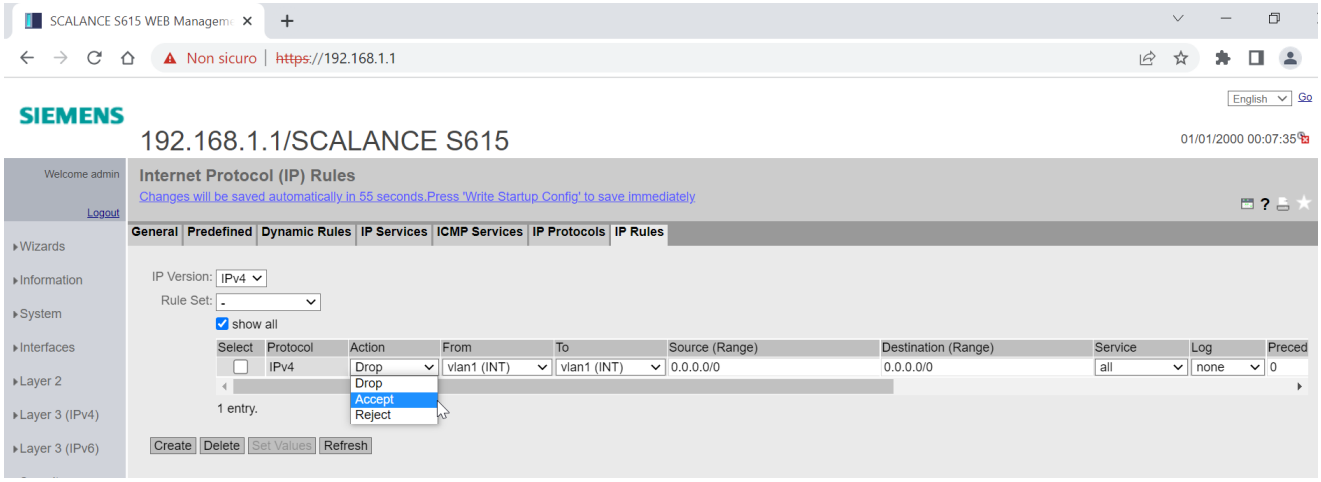


Creazione di regole di comunicazione IP

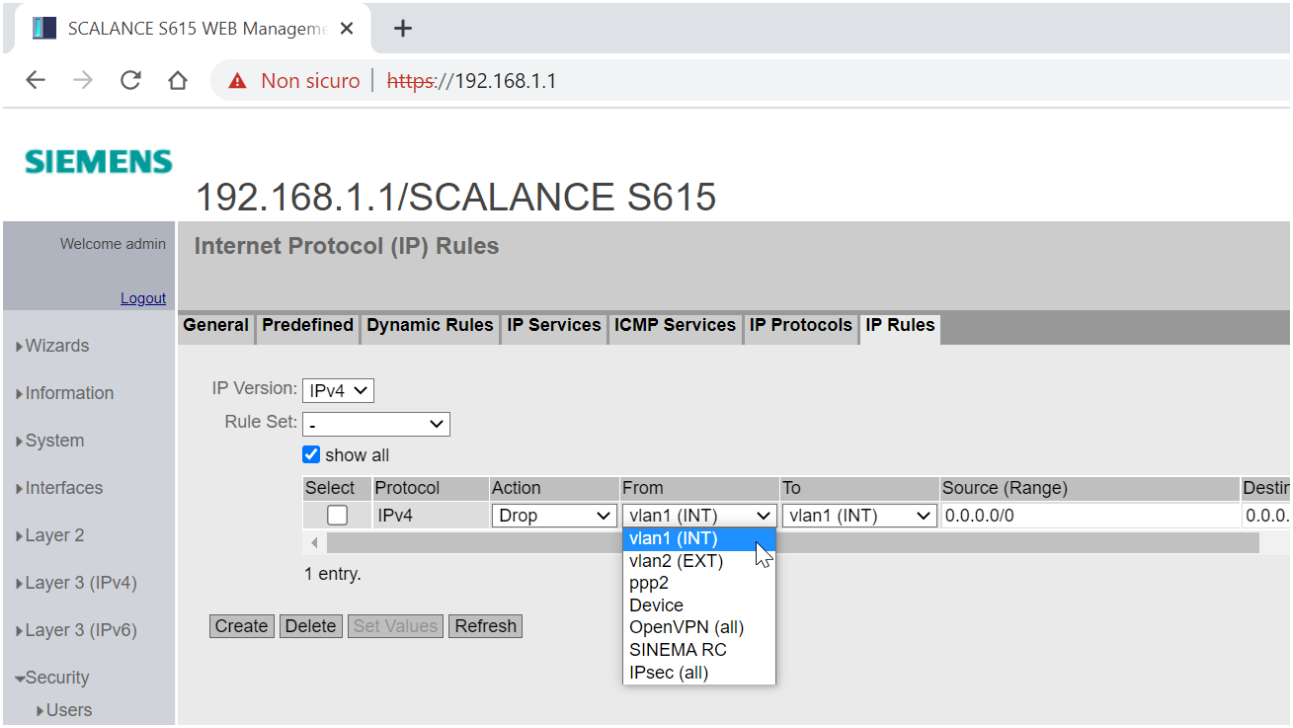
Le regole di comunicazione vanno inserite nella tab **“IP Rules”.** Per inserire la prima regola bisogna cliccare su **“Create”**.



Viene quindi inserita automaticamente una regola dummy di default che può essere poi modificata

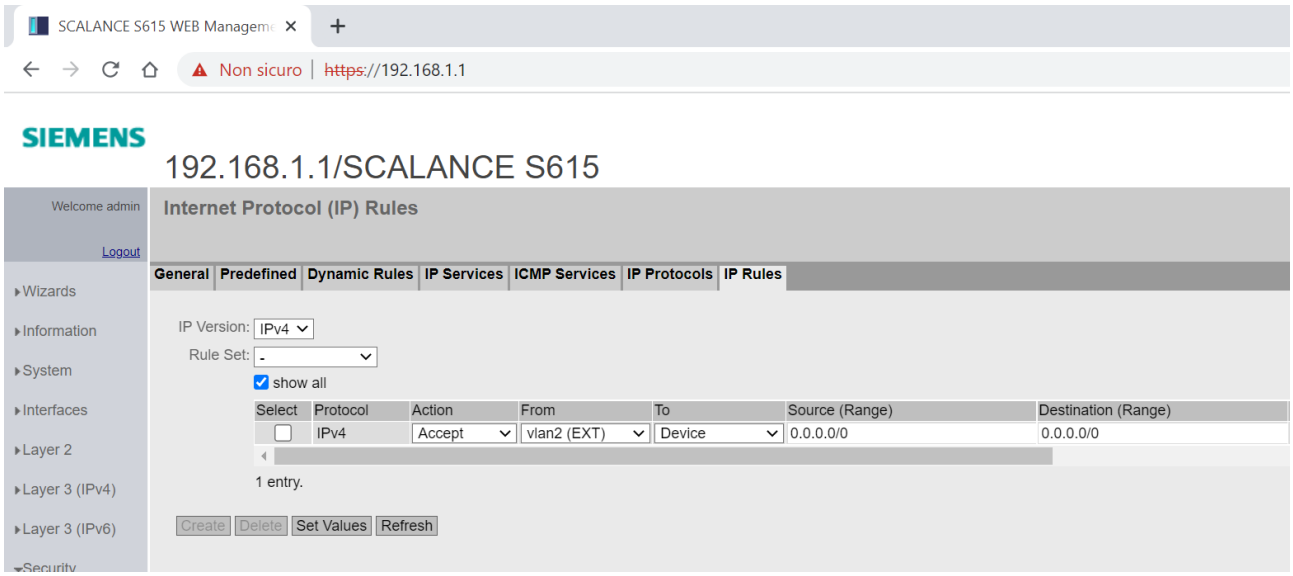


Per creare una regola di comunicazione in genere si seleziona l’Action su “Accept”, dopodiché si modificano gli altri parametri per realizzare la comunicazione desiderata.
Selezionando le interfacce in corrispondenza delle voci “From” e “To”, è possibile definire fra quali di queste stabilire le regole di comunicazione.

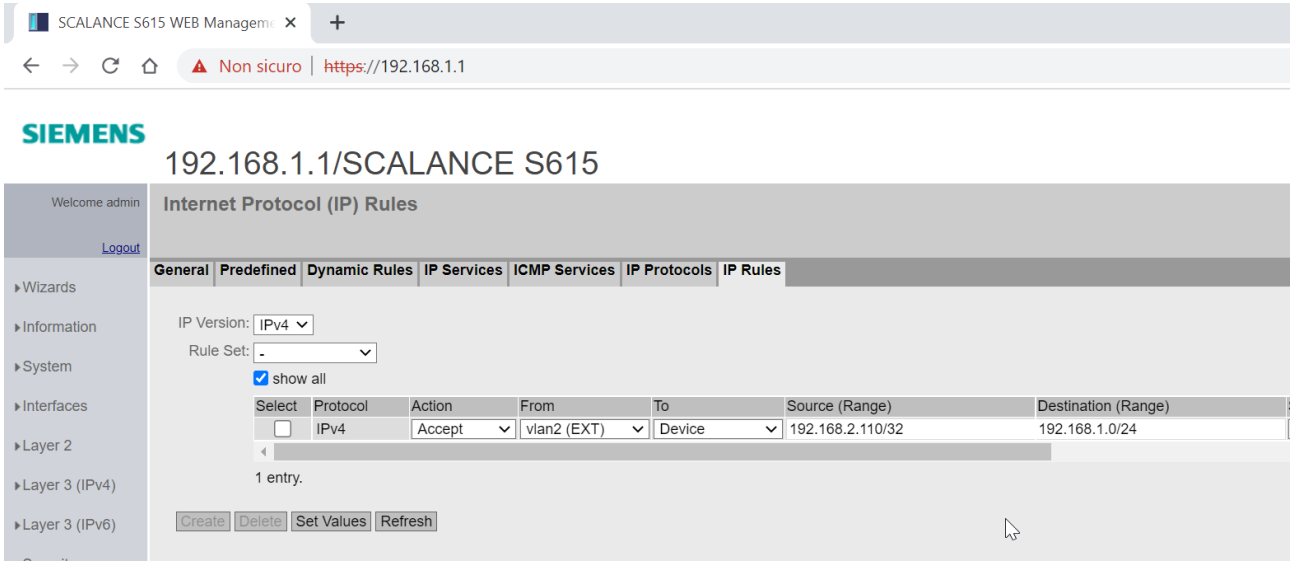


N.B.: oltre alle VLAN/Subnet **è possibile utilizzare anche la stessa interfaccia del device, le interfacce mobili** su Scalance M(usb0) **e le interfacce VPN** come "SINEMA RC" per filtrare il traffico in entrata e in uscita dalla VPN.
In questo ultimo caso, occorre però disabilitare l'auto firewall (vedere capitolo successivo relativo all'argomento).

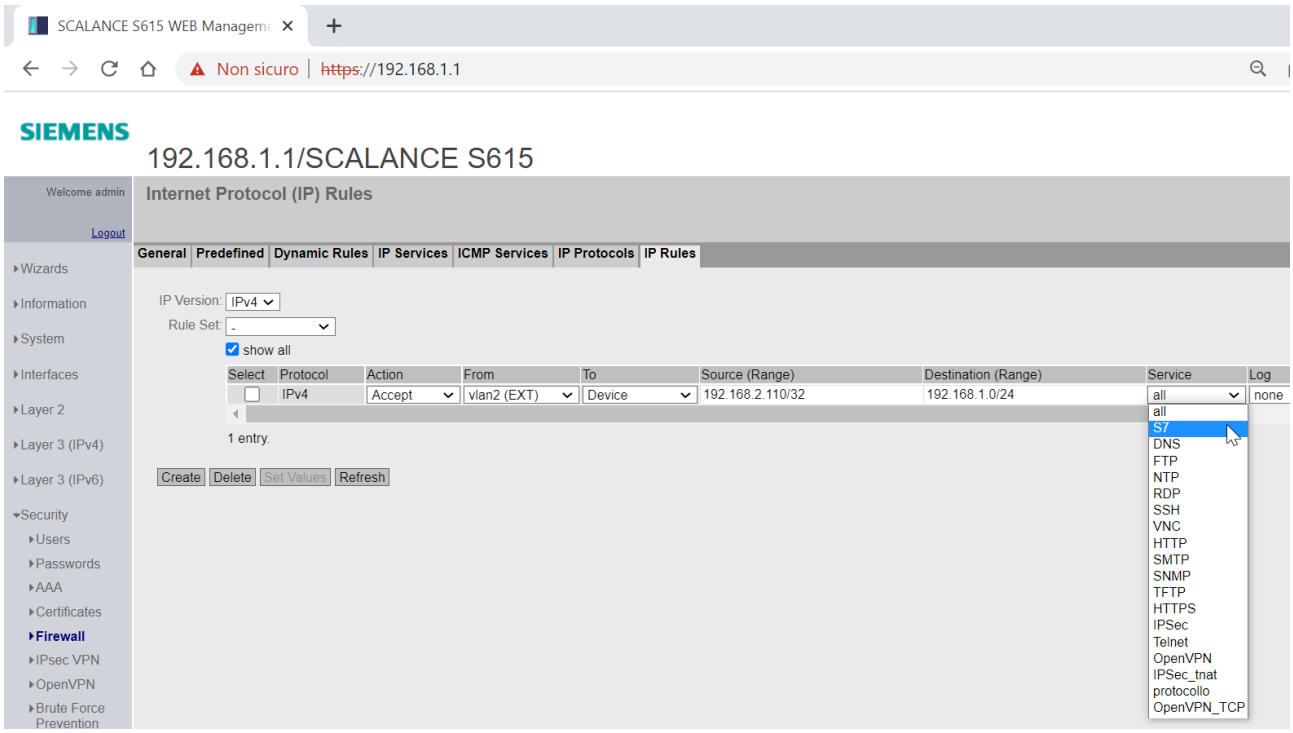
Ad esempio, se si vuole permettere qualsiasi trasmissione (accesso web, ping…) dalla rete esterna verso il device è necessario stabilire una regola dalla VLAN 2 al "Device".



Sul campo "Source (Range)" e "Destination (Range)" è invece possibile restringere il campo degli indirizzi che possono comunicare fra le 2 interfacce utilizzando la notazione CIDR (ad esempio /32 per definire un singolo indirizzo o /24 per definire una subnet mask 255.255.255.0)



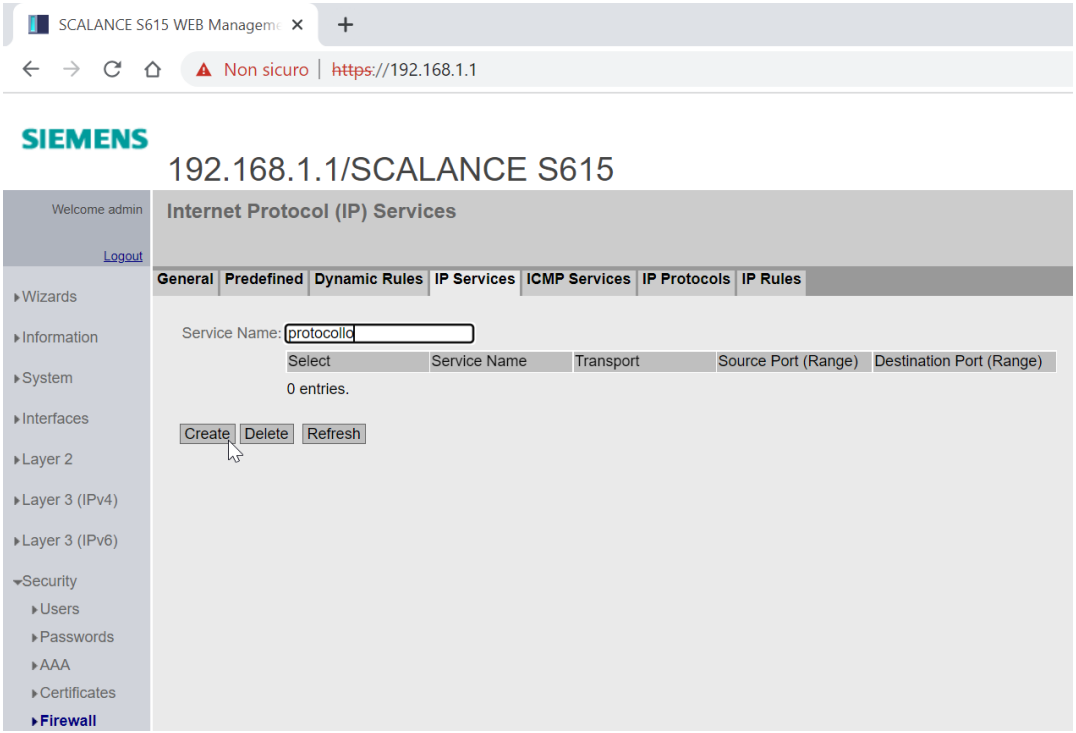
Infine, è possibile anche selezionare il protocollo o servizio abilitato per la specifica regola.
Al termine della creazione della regola cliccare su "Set Values".



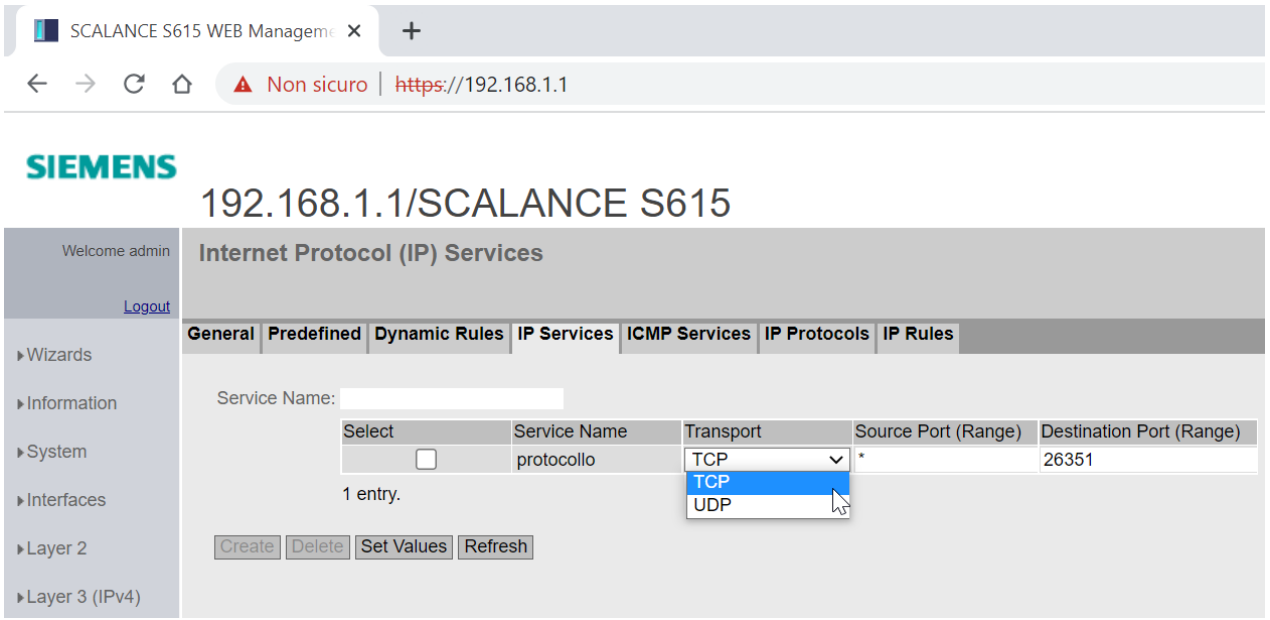
N.B.: i servizi vanno prima definiti nella tab IP Services (vedere capitolo successivo) per essere selezionati dal menu a tendina.

Creazione di servizi basati su porte TCP/UDP

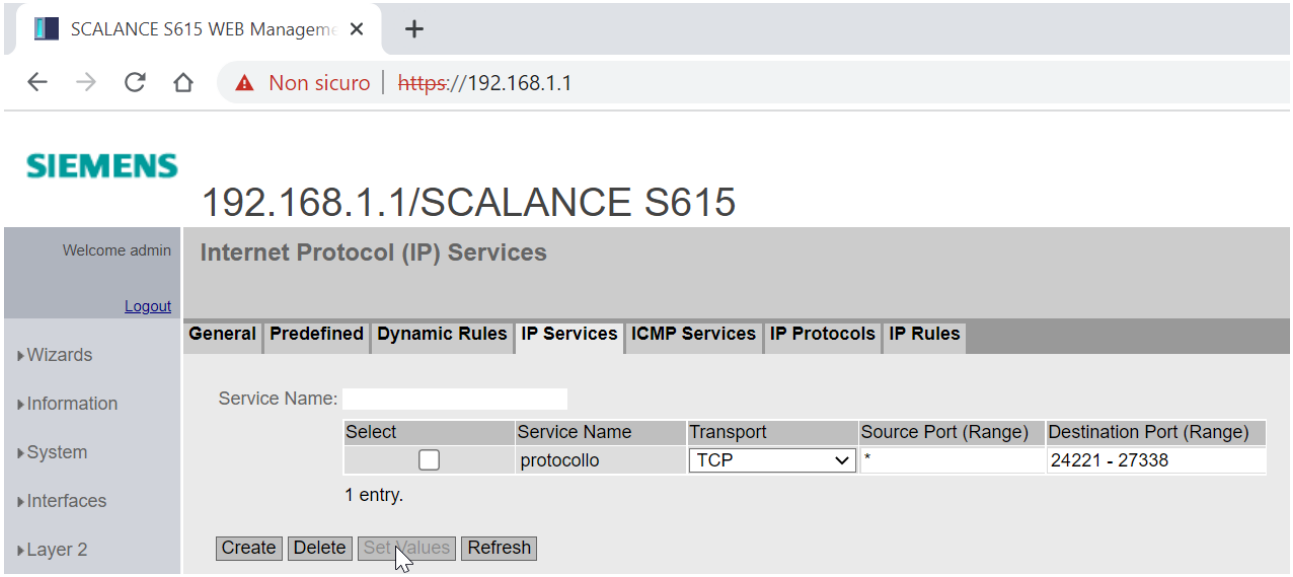
Per sfruttare le funzionalità Layer 4 del firewall, legate al filtraggio sulla base del protocollo di comunicazione, è necessario creare dei servizi nel tab "IP Services".
Inserire un nome a piacere per denominare il servizio in corrispondenza di **"Service Name"** e cliccare su **"Create".**



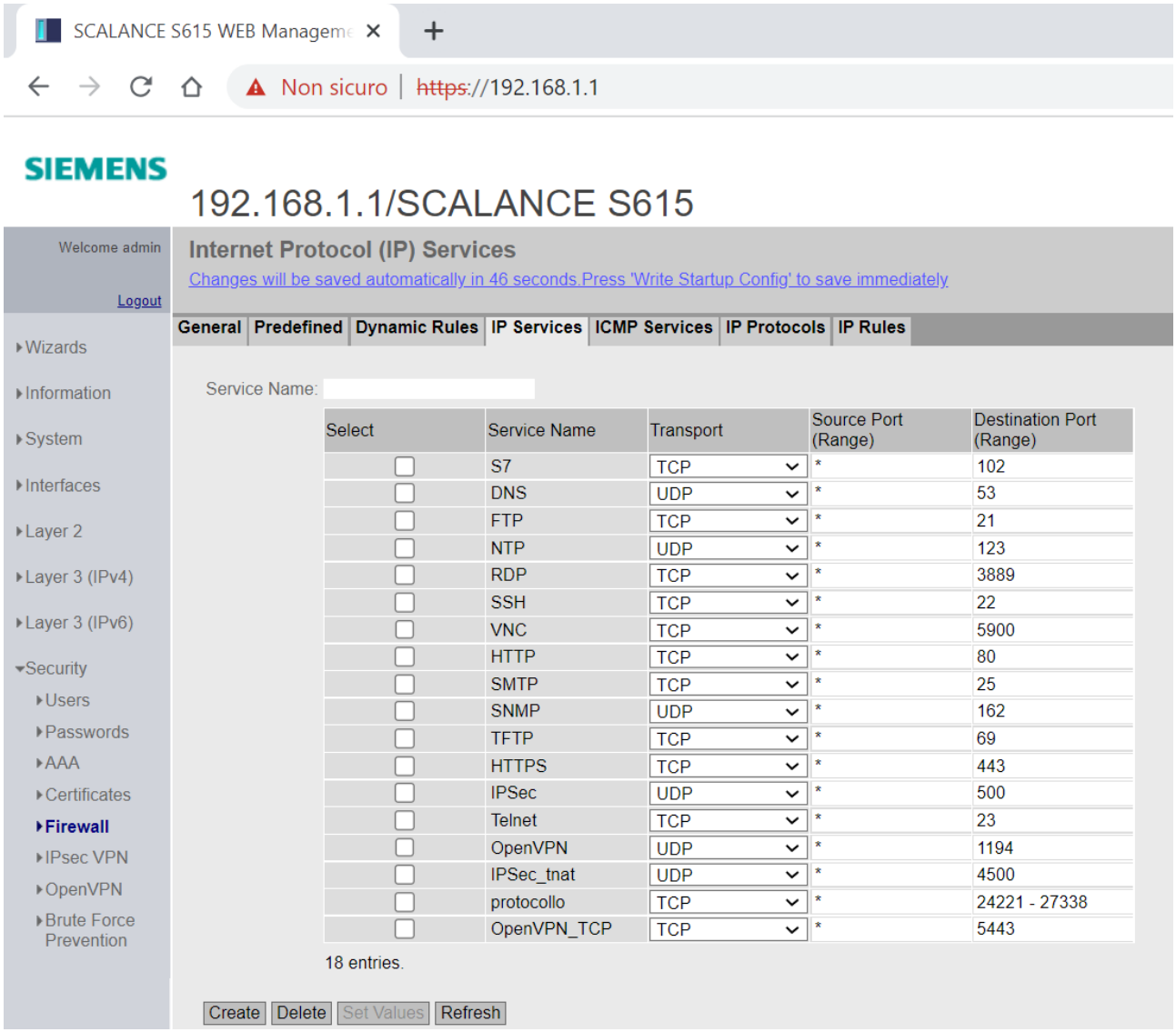
Una volta creato, è possibile definire il protocollo in base alla tipologia TCP/UDP e la porta di destinazione o sorgente (il carattere * indica qualsiasi porta). Al termine della modifica, cliccare su **"Set Values".**



N.B.: Se il servizio in questione è definito da un intervallo di porte è possibile usare il carattere "-" fra la porta iniziale e quella finale per definire l'intervallo

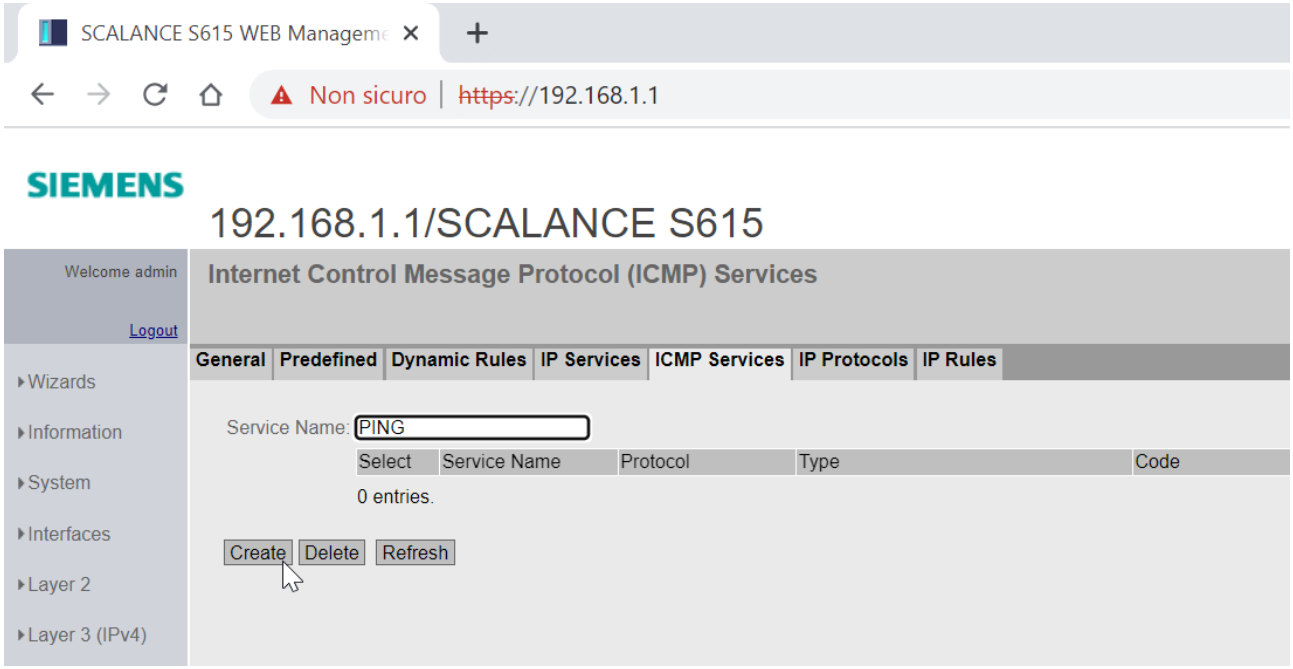


E' possibile inserire diversi tipi di servizi, sia noti che personalizzati. Riportiamo qui alcuni esempi.

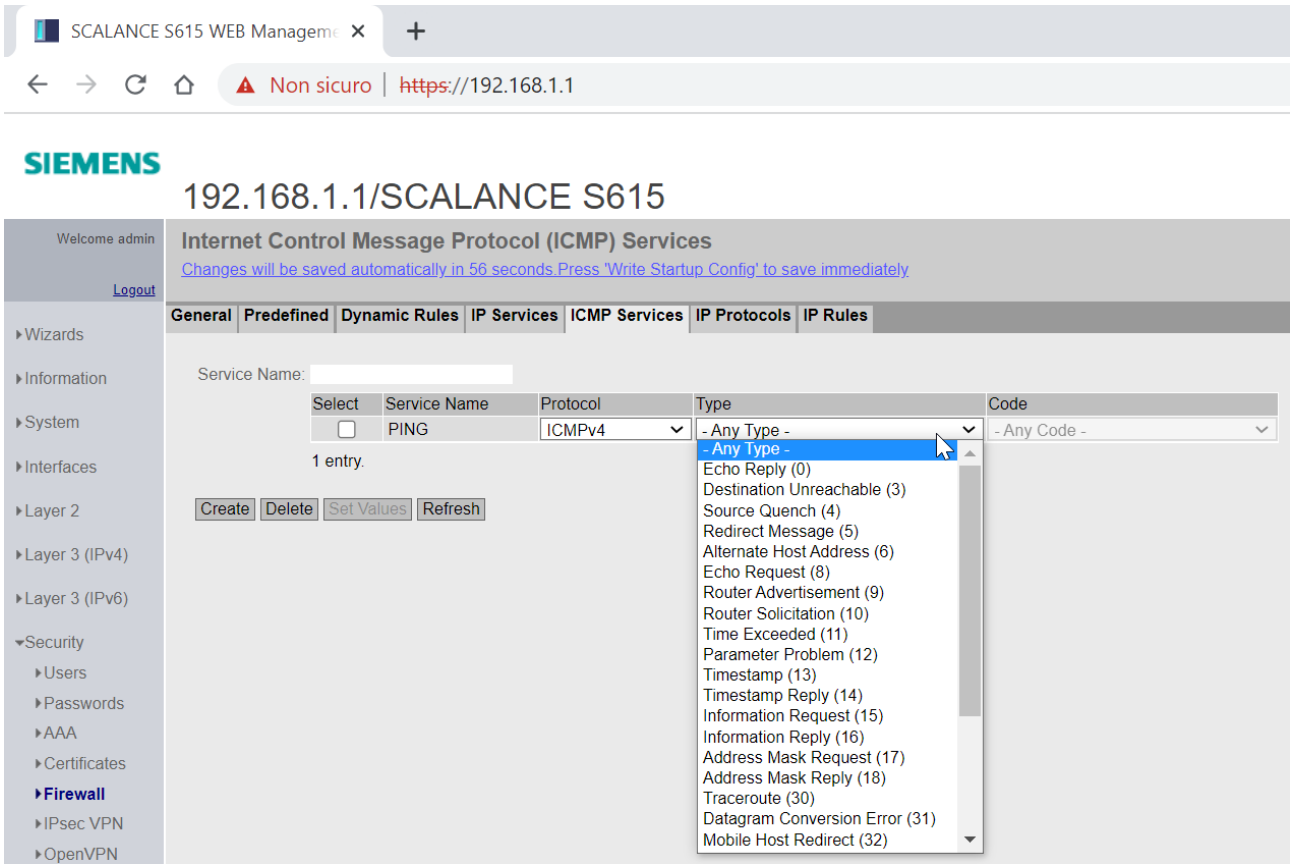


Creazione di servizi basati su ICMP

All'elenco del paragrafo precedente fanno eccezione i servizi ICMP, come il ping che, non essendo un servizio basato su TCP/UPD, va definito a parte nella tab **"ICMP Services"**.
Inserire il nome scelto in corrispondenza di "Service Name" e cliccare su **"Create"**

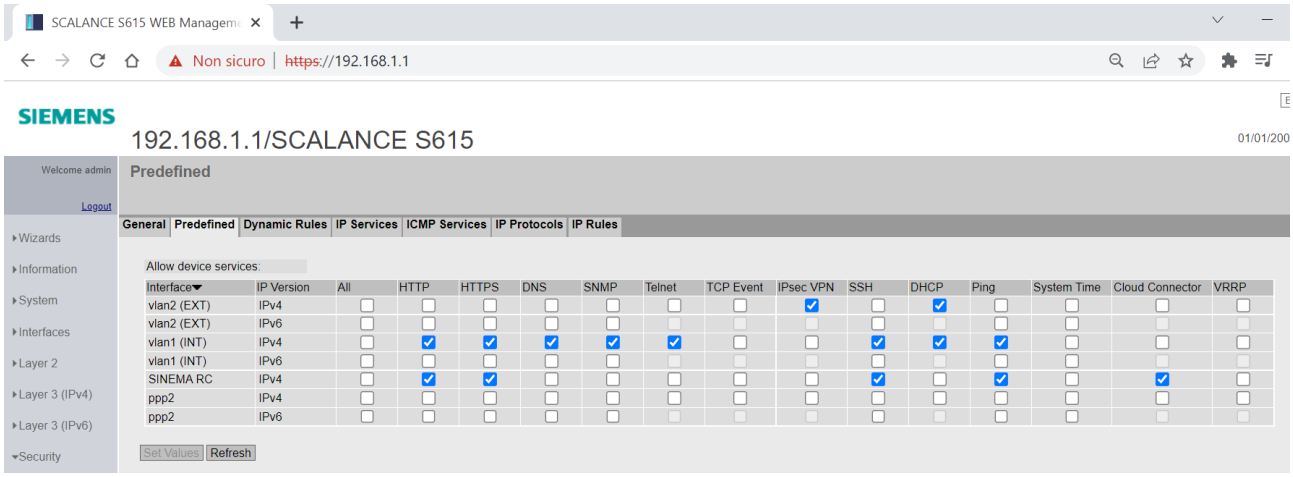


Definire il tipo di ping (in caso di dubbio lasciare "Any Type") e cliccare **"Set Values".**



Servizi predefiniti su Scalance S/M

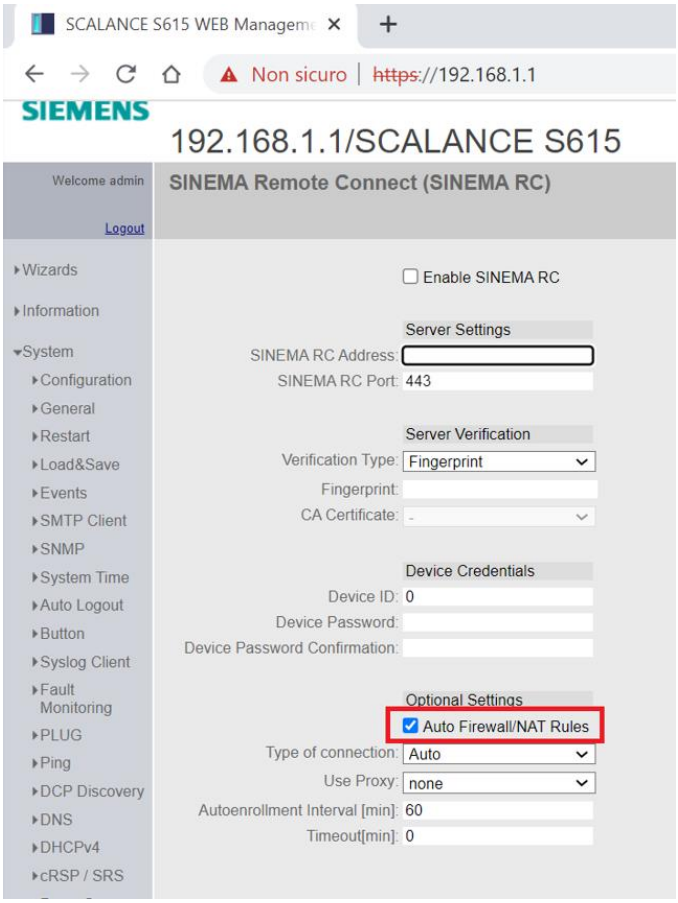
Nel tab “Predefined” del menu Firewall è anche possibile attivare dei servizi IP predefiniti.
Questi servizi riguardano solamente quelli che possono **accedere al device** (cioè lo Scalance).
Non è quindi necessario utilizzare queste impostazioni per impostare regole di comunicazione fra dispositivi esterni che insistono su subnet diverse e devono comunicare attraverso lo Scalance! Per queste si procede con la tab IPServices, come già precedentemente illustrato.



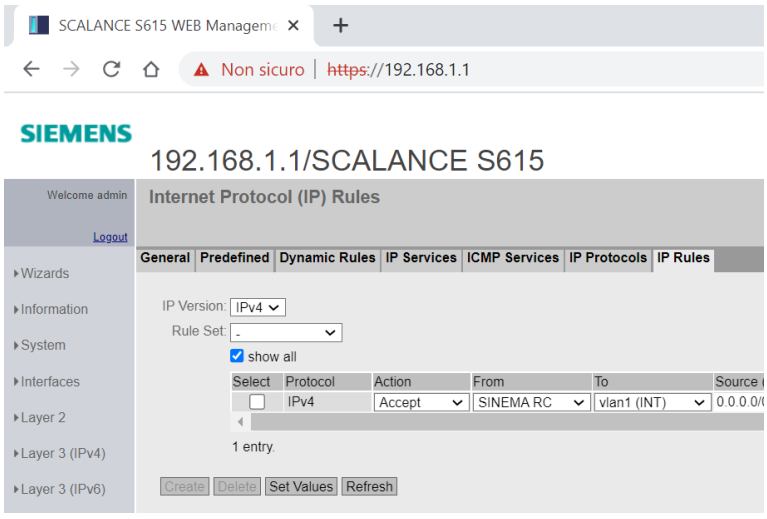
Di default la maggior parte dei servizi può lavorare sulla rete interna (VLAN 1) mentre il device è inaccessibile dall’esterno (VLAN 2 o interfaccia mobile USB0).

Configurazione automatica del firewall da Sinema RC

In caso dell'utilizzo del Sinema Remote Connect, non è necessario effettuare alcuna configurazione del firewall. Al default è attivato l'auto-firewall.

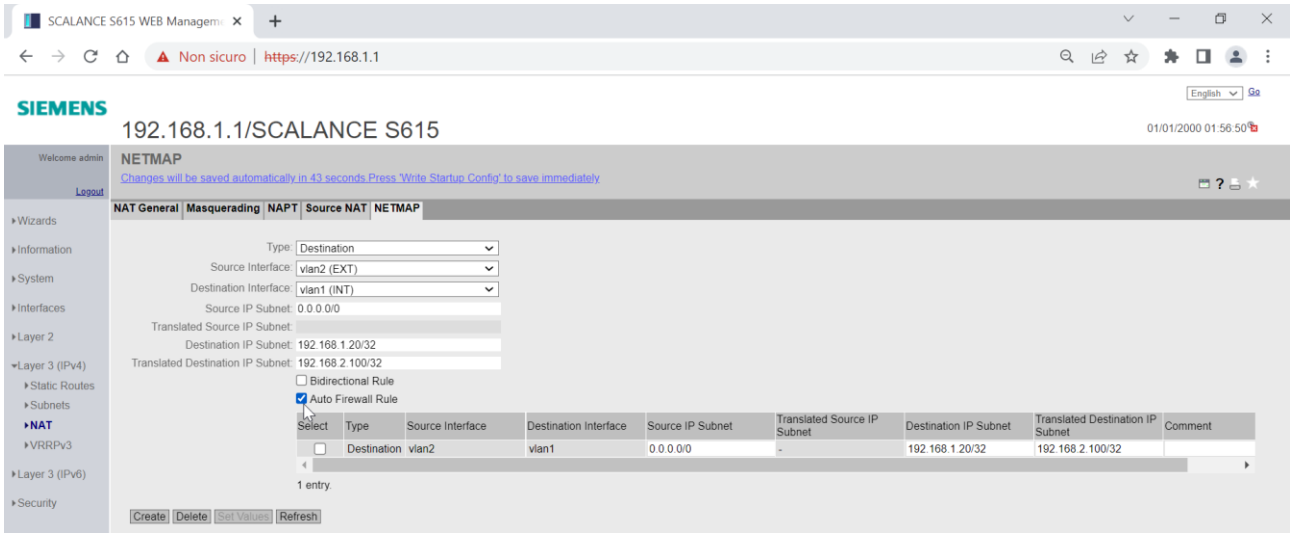


Questo significa che **le regole di firewall, che permettono il passaggio di dati dalla VPN Sinema Remote Connect alle reti configurate sul Sinema Remote Connect Server, sono automaticamente inserite** (così come le regole di NAT).
N.B.: se si vuole filtrare i dati che dalla VPN passano verso le macchine, è necessario disabilitare questa spunta e inserire le regole a mano come riportato nella restante parte della guida.



Configurazione automatica del firewall per regole di NAT

Anche configurando regole di NAT, dalla versione firmware 6.1, è possibile configurare automaticamente le corrispondenti regole di firewall in caso di uso della modalità Netmap (non in NAPT o Source NAT):
Basta infatti inserire le regole di NAT e selezionare la **spunta "Auto Firewall Rule"**



Andando sulla pagina del firewall è infatti possibile osservare che è stata inserita la regola coerente

Tale regola è solo parzialmente modificabile (è possibile restringere gli IP sorgenti e cambiare i servizi) e non cancellabile in quanto legata alla regola di NAT. Di conseguenza per cancellare la regola di firewall occorre cancellare la corrispondente regola di NAT.