REPORT S3/L5

Traccia

Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete

Soluzione

Facciamo un primo test sulle due macchine, rispettivamente ***kali*** e ***metasploitable***, controllandoo che esse si trovino sulla stessa rete mediante comando ***ipconfig*** e possano comunicare tra loro mediante comando ***ping.***

Figura1: Ip di metasploitable

La macchina metasploitable avrà ***ipaddress***: *192.168.56.101* con ***subnetmask***: *255.255.255.0*.

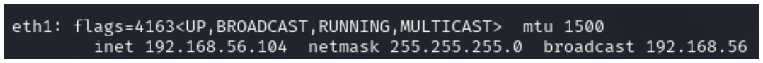


Figura2: Ip di kali

La macchina Kali avrà ***ipaddress***: *192.168.50.10* con ***subnetmask***: *255.255.255.0*.

E verifichiamo mendiante ***ping*** che le 2 macchine siano in grado di comunicare tra loro.

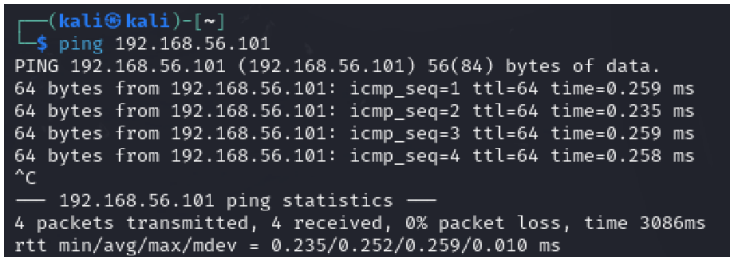


Figura3: Ping di verifica tra le 2 macchine

Controlleremo anche che sia possibile effettuare l' acceso da kali sulla DVWA su METASPLOITABLE. Andando ad inserire come url l' indirizzo ip della nostra macchina metasploitable.

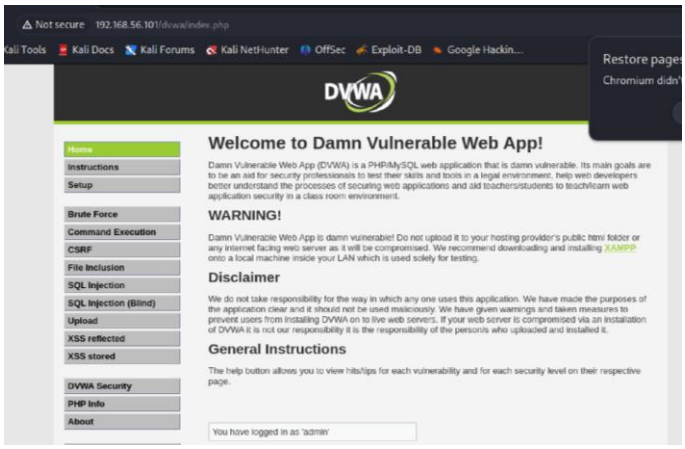


Figura 4: Verifichiamo l'accesso alla DVWA da kali su meta, nella medesima rete

Ai fini dell' esercizio è necessario che i due host siano su reti diverse, per farlo vado manulamente a modificare l' ip statico della macchina kali assegnando un nuovo ip: 192.168.1.10, lasciando invariato quello della macchina metasploitable, ora le macchine non comunicheranno piu tra loro e saranno appartenti a due network differenti. ***Figura 4***

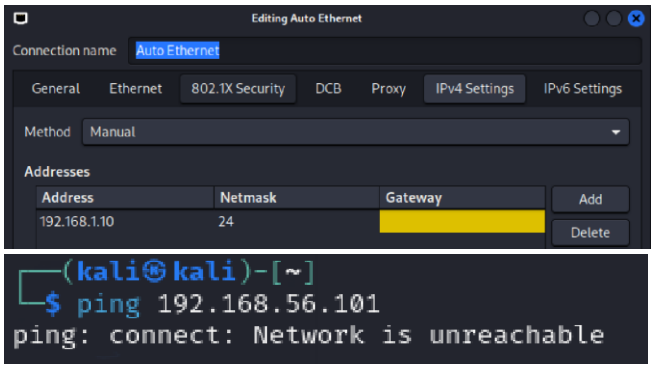


Figura 5: Modifica manuale dell' IP di kali, e test di ping con metasploitable.

Andiamo adesso ad avviare il firewall pfsense con ***ip lan***: 192.168.1.1/24 e da kali accediamo al ***web-configurator*** inserendo nella barra degli url questo indirizzo. Sarà necessario adesso aggiungere la nuova interfaccia per la gestione delle due reti di appartenze dei due differenti host.

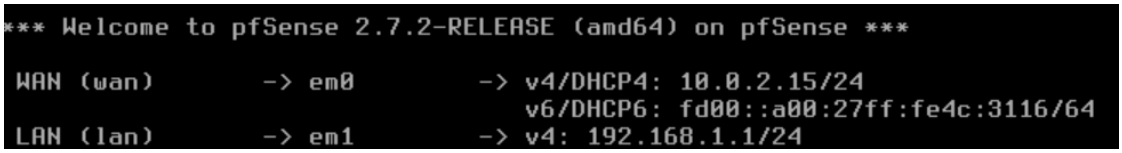
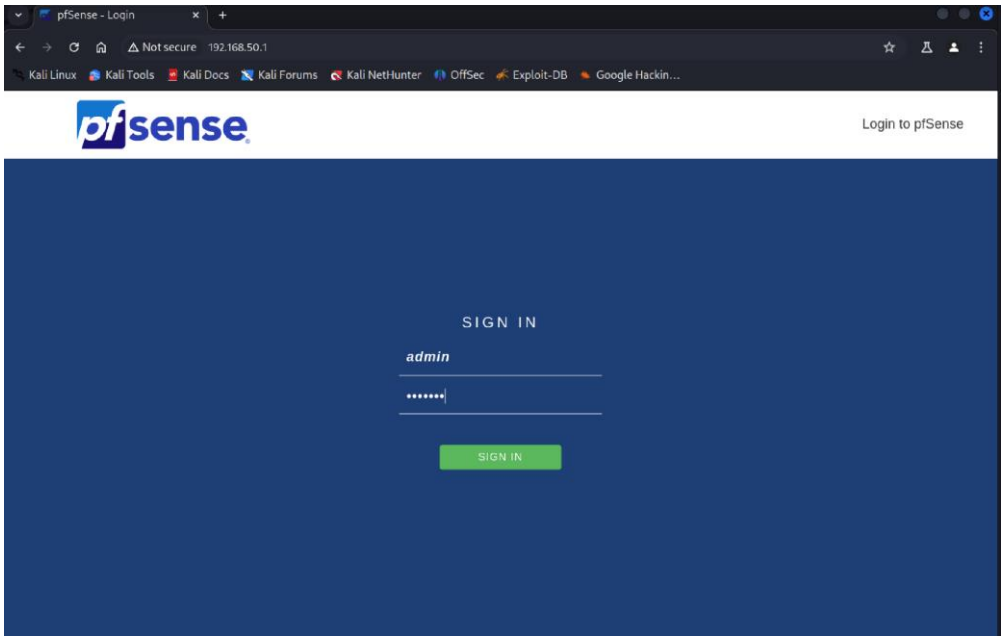


Figura5: Avvio del firewall, 192.168.1.1



Procedo quindi con l' aggiunta della nuova interfaccia alla quale assegnerò ip statico del gateway della macchina ***metasploitable***, in questo caso ***ip: 192.168.56.1***. ***Figura 6***

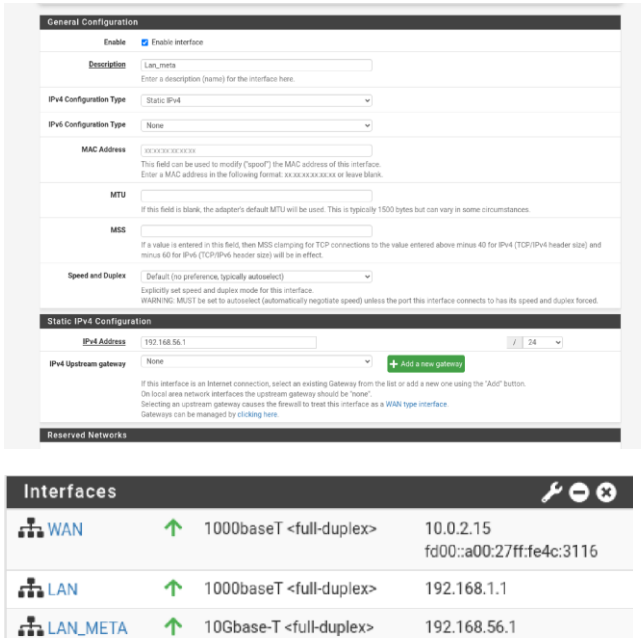


Figura 6: Aggiungo manualmente la nuova interfaccia dal web configurator di pfsense.

Dobbiamo adesso a gestire le regole per il traffico tra i due host, in particolare dobbiamo consentire il traffico sulla nuova interfaccia creata con delle regole di "pass" su tutte le subnet della nuova interfaccia, come source inserireme le subnet della rete e come destinazione "any". Figura 7

Per farlo procederemo accedendo alle sezione firewall in alto e successivametne rules.

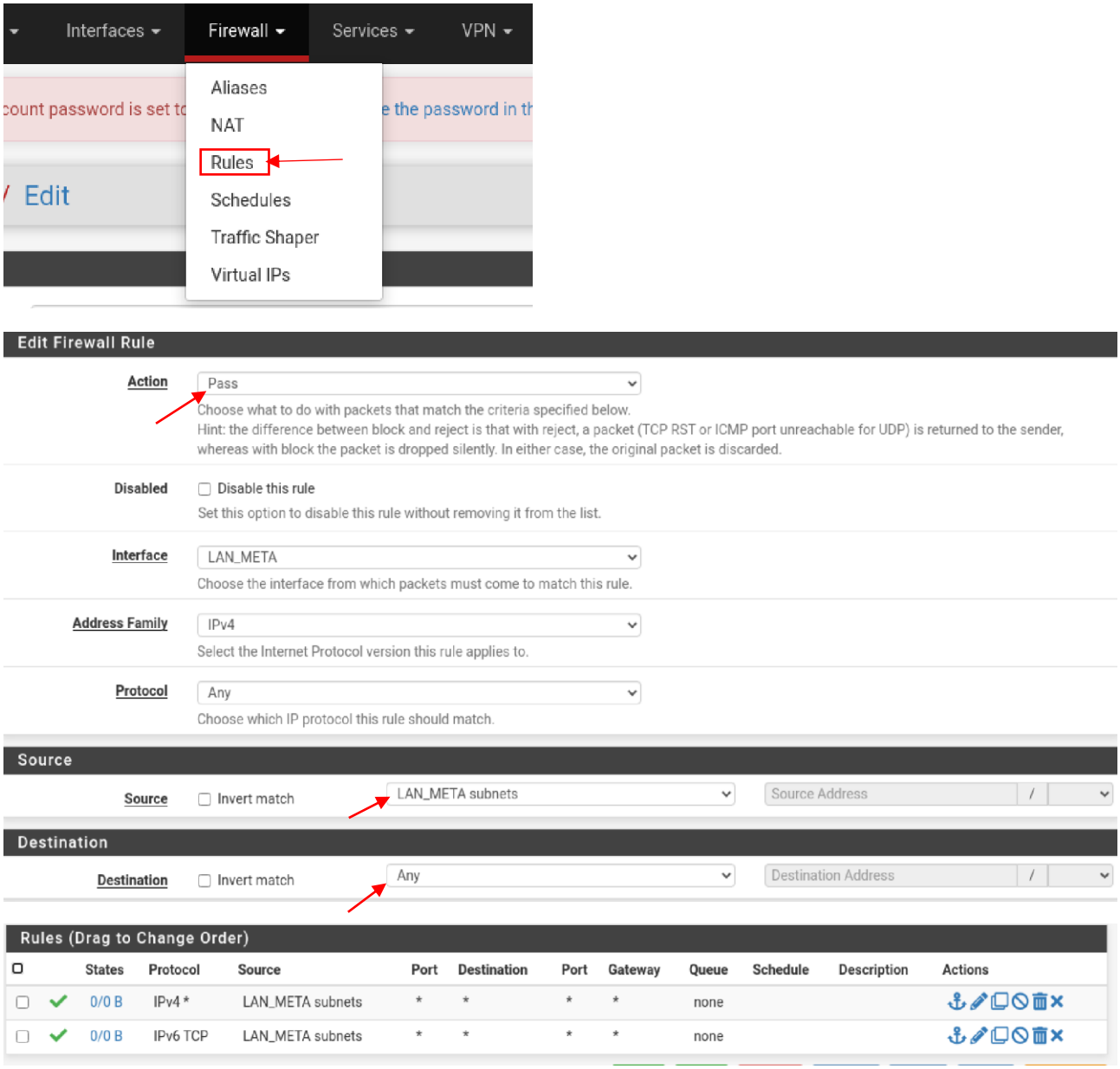


Figura 7: Aggiungo la regola per consentire il traffico.

infine abiliteremo il routing sulla nuova interfaccia da ***system→routing→static routes*** e aggiungendo la rete riferita alla nuova interfaccia.

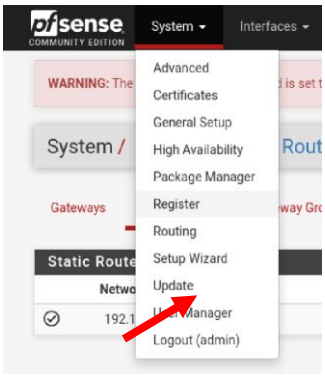


Figura 8: Viene abilitato il routing sulla nuova interfaccia per consentire la comunicazione.

Possiamo ora testare, con il comando ***ping,*** che le due macchine siano in grado di comunicare pur appartendendo a due reti diverse, proviamo dalla macchina kali pingando la macchina metasploitable.

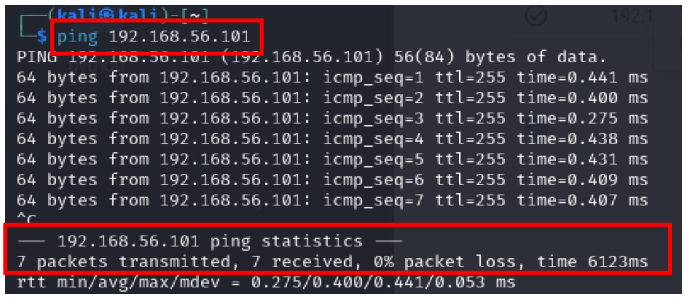


Figura 9: Ping di test.

Il ping è riuscito quindi le due macchine comunicano tra loro. Vogliamo ora creare una regola che blocchi il traffico verso la ***DVWA*** su ***metasploitable*** da kali. Per farlo aggiungeremo una regola che avrà come sorgente la macchina ***kali*** come destinazione ***meta*** e la porta 80 o l' indirizzo specifico da bloccare, ***Figura 10***. Andremo successivamente a fare un test per verificare che efftivamente inserendo su un browser di kali l' url della macchina meta/dvwa non si possa fare piu effettuare l' accesso a questa poichè il traffico sarà bloccato. ***Figura 11***

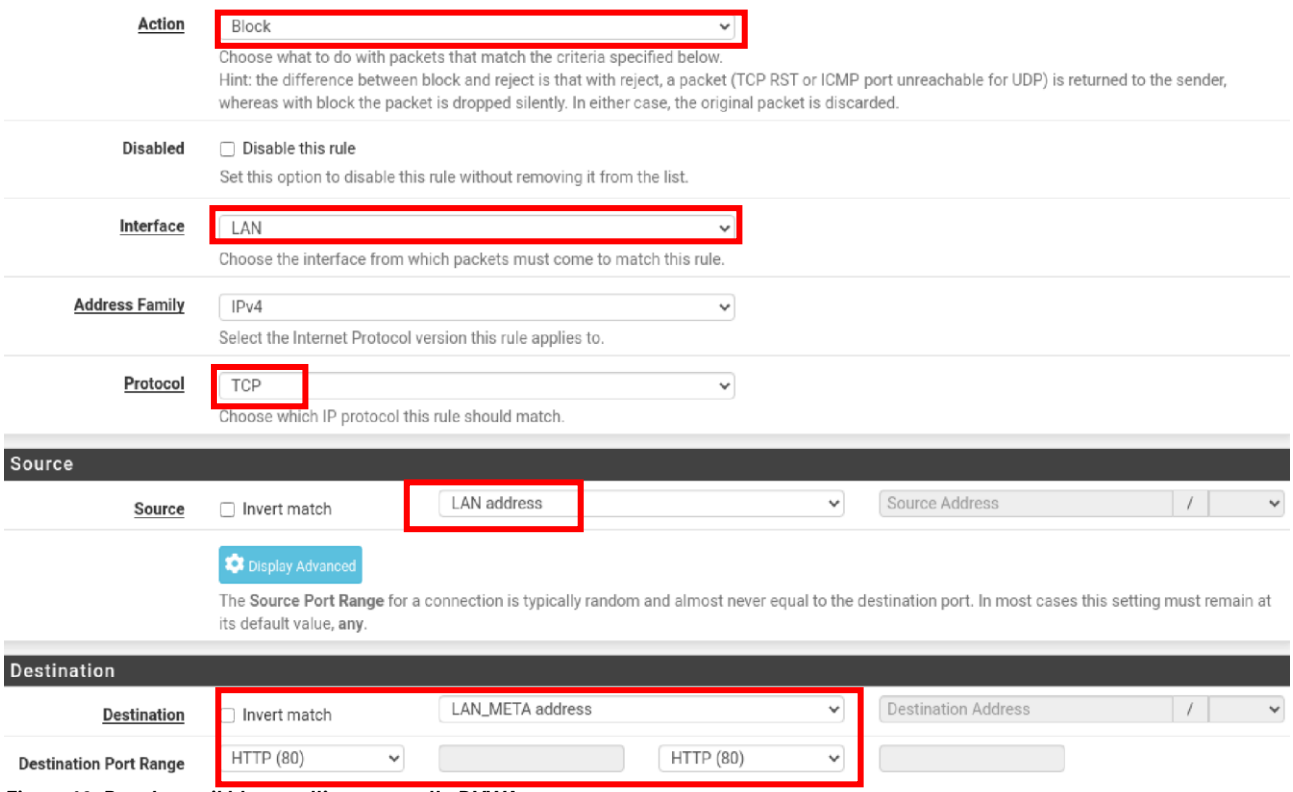


Figura 10: Regola per il blocco all' accesso alla DVWA.

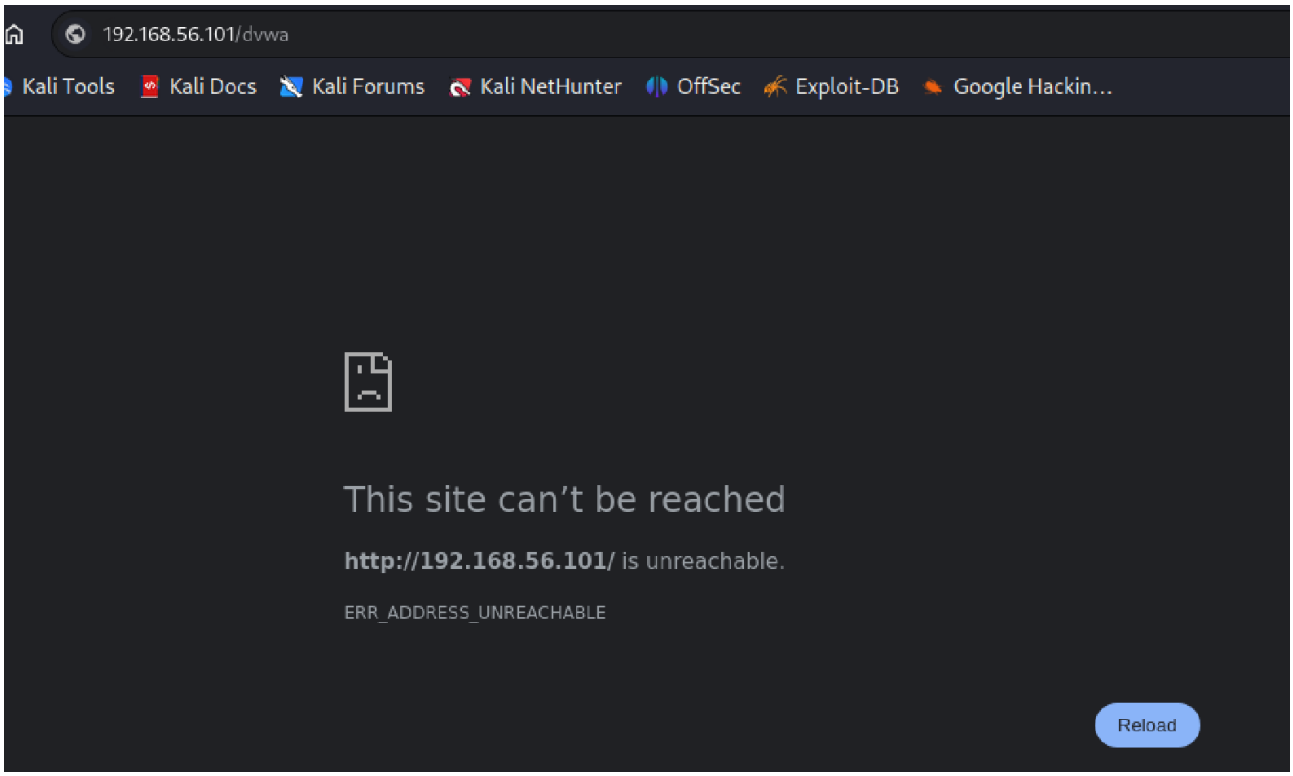


Figura 11: Test di accesso alla DVWA

ESERCIZIO BONUS

Impostare una regola che blocchi il telnet da kali a metasploitable

SOLUZIONE

Ricordiamo che il telnet utilizza la porta 23, analogamente a quanto visto prima andremo ad aggiungere sul pfsense una nuova regola di blocco specifica su questa porta. In interface andremo a impostare la lan di kali, su source la lan di kali e su destination quella di metasploitable specificando la porta ***Telnet(23)*** e protocollo ***Tcp***.

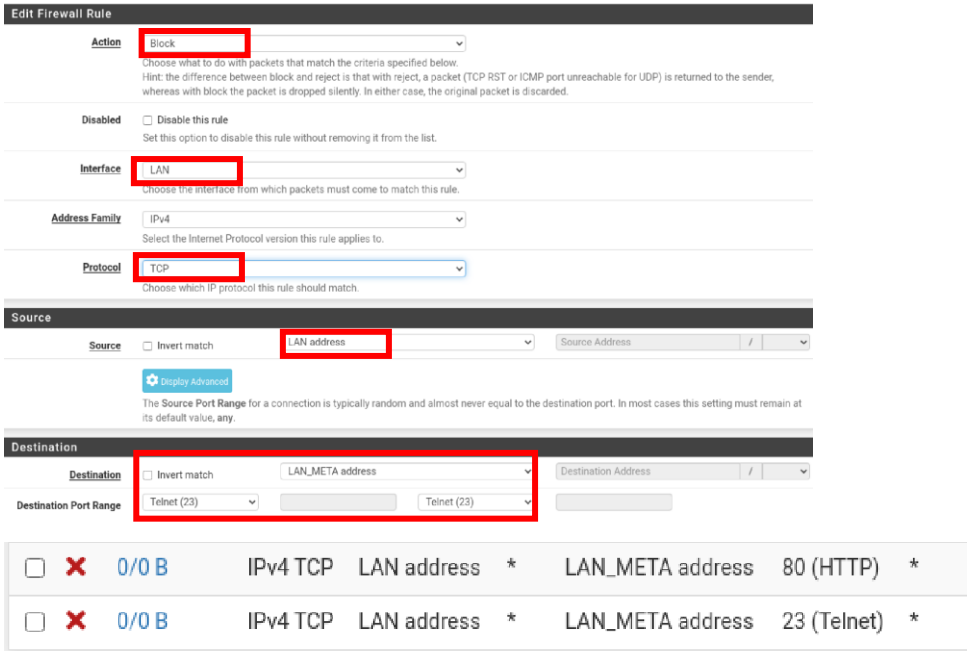


Figura 12: Regola di blocco telnet.