Creazione Policy PfSense

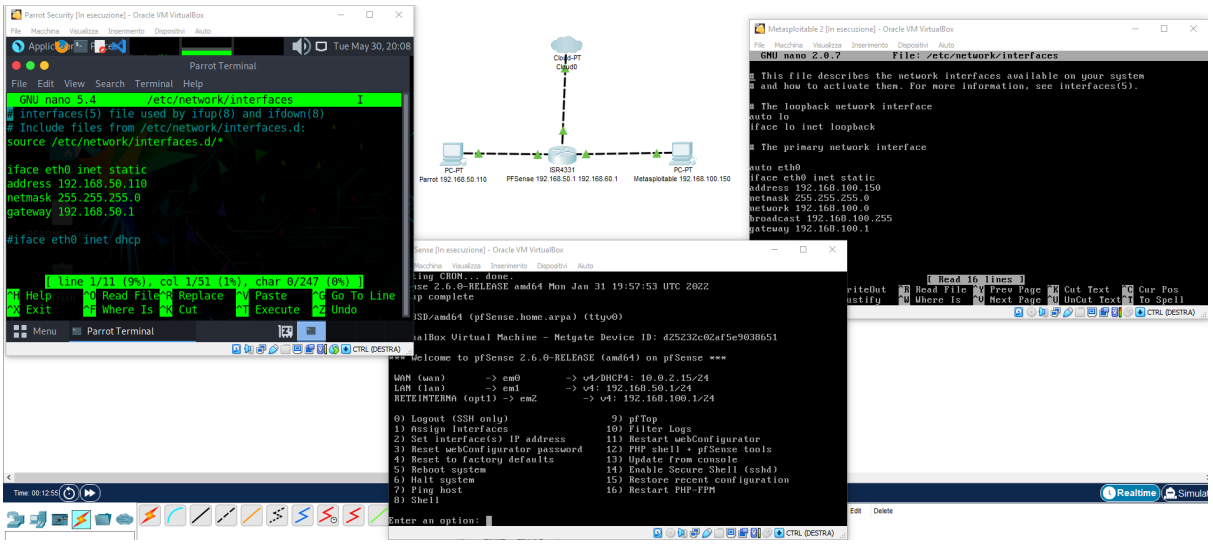
Obiettivo: Creazione pratica di una regola Firewall che blocchi l'accesso a DVWA
Software utilizzati:

- **Parrot OS**
- **PfSense** utilizzato in questo caso come Router e Firewall
- **Metasploitable 2** (dove si trova la DVWA)

1) Configurazione Indirizzi IP

Per iniziare l'esercizio ho dovuto settare per prima cosa gli indirizzi IP con annessi Gateway delle due macchine:

- ***Parrot***: 192.168.50.110/24 - ***Gateway***: 192.168.50.1
- ***Metasploitable***: 192.168.100.150/24 - ***Gateway***: 192.168.100.1

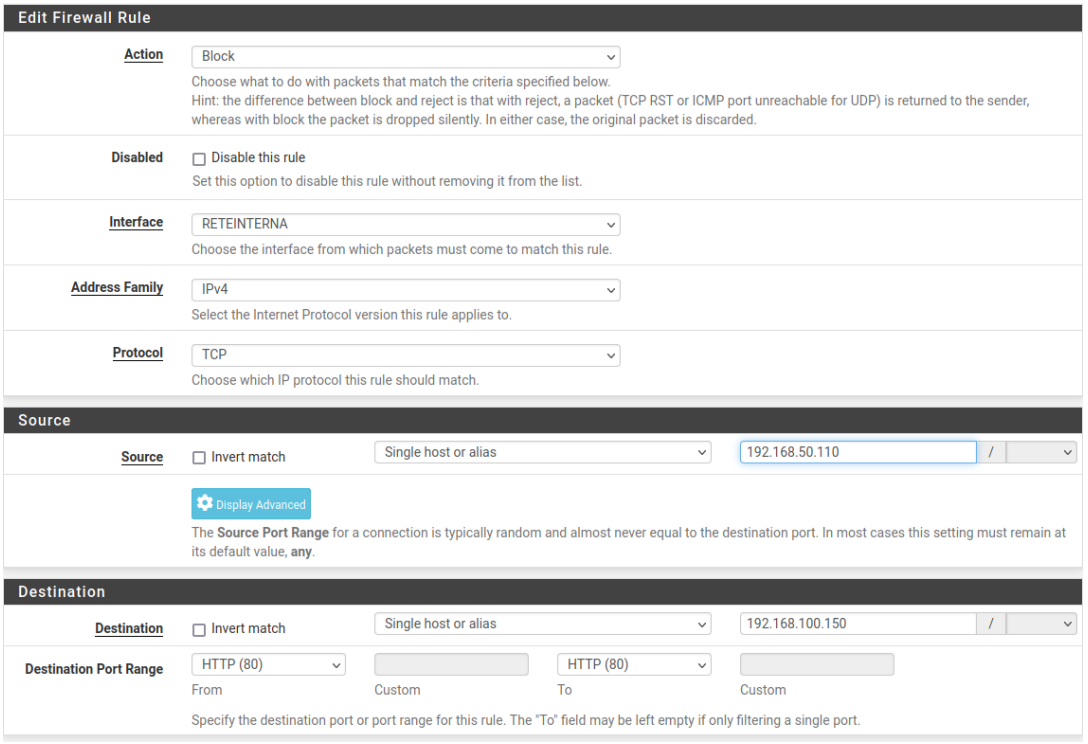


Ho configurato inoltre due reti interne su PfSense:

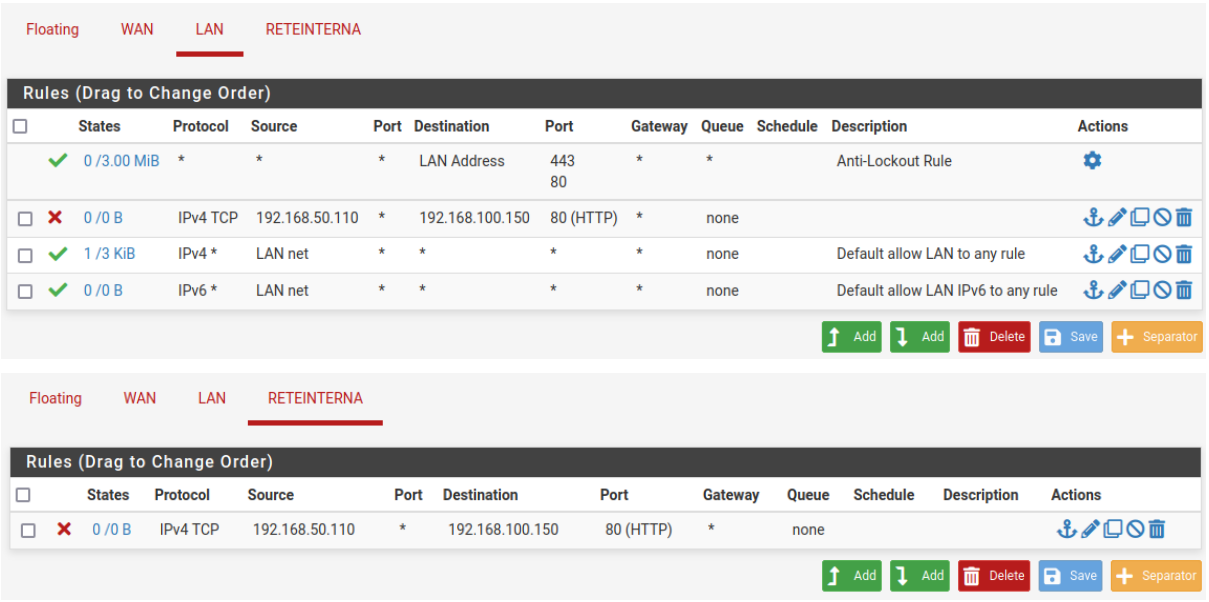
- **LAN** settata secondo il gateway della macchina **Parrot**
- **RETEINTERNA** collegata a **Metasploitable** simulando una rete estranea alla **LAN** (per esempio uno studio in casa)

2) Creazione Policy del Firewall

Per la creazione della regola del Firewall sono entrato da browser dentro **PfSense** utilizzando l'indirizzo *192.168.50.1* e cliccando su *Firewall/Rules* ho aggiunto sulla **RETEINTERNA** la regola che bloccava lo scambio di protocolli TCP provenienti da Parrot (source) con destinazione Metasploitable (porta 80). Ho dovuto settare la stessa regola posizionandola sopra tutte le altre sulla rete LAN perchè quest'ultime facevano comunicare lo stesso i due indirizzi IP.



Questa è la regola usata per entrambe le reti interne.

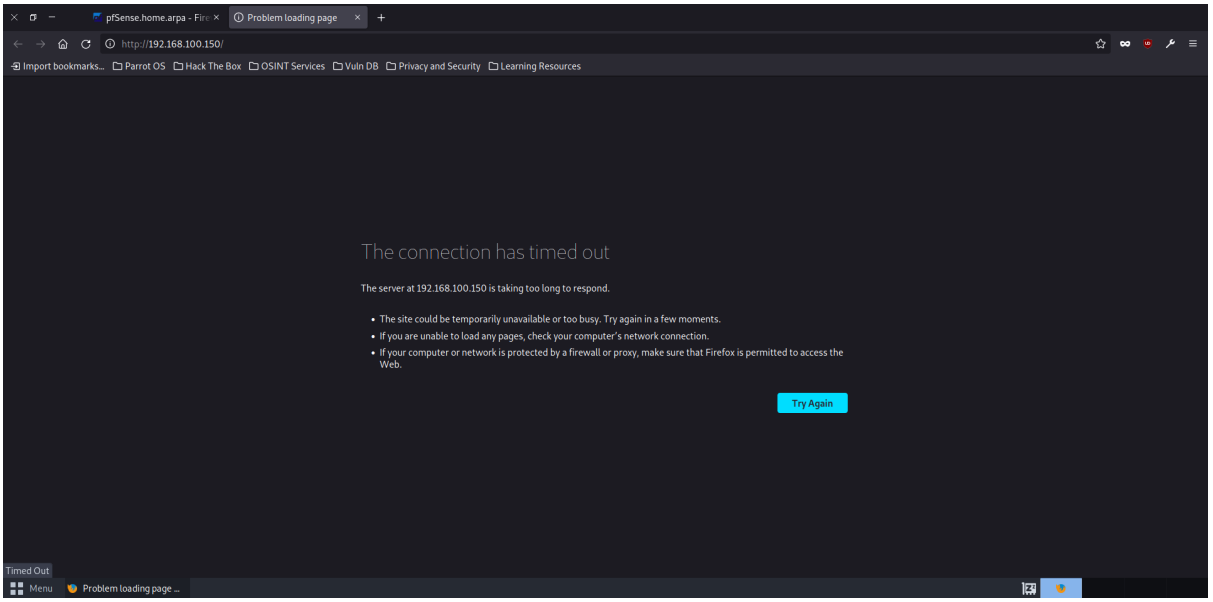


Queste due immagini mostrano invece le regole settate per entrambe le reti. Nel caso della **LAN** non è necessario disattivarle, ma l'importante è mettere la regola di blocco prima di qualsiasi regola "permissiva" perchè l'ordine con il quale vengono eseguite va dall'alto verso il basso.

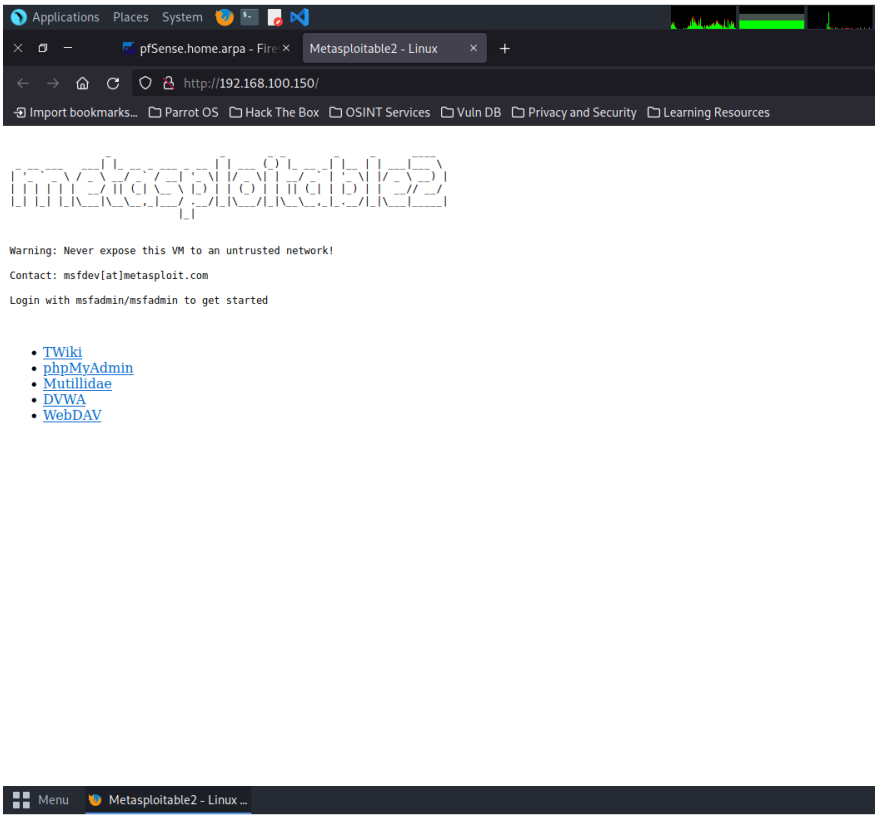
3) Prova da Browser

Ho effettuato due prove:

- *Prima prova*: con **policy firewall** attivate; il risultato è stato un lungo periodo di caricamento che ha portato il browser a lasciare un messaggio dove diceva che il tempo di risposta era troppo lungo, quindi la **Metasploitable** era irraggiungibile



- *Seconda prova*: con **policy firewall** disattivate; in questo caso il browser si è immediatamente connesso alla **Metasploitable** ed è stato possibile entrare nella **DVWA**.



Username

Password

Login