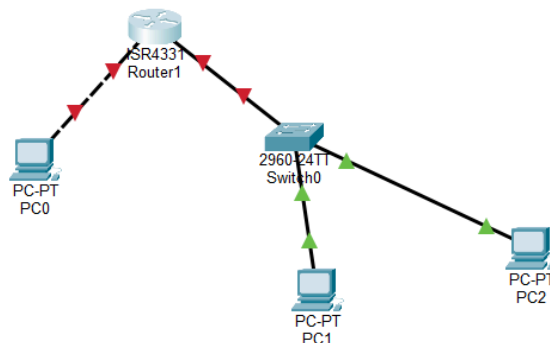


# CREAZIONE POLICY PFSENSE

## OBIETTIVO DELLA RETE

L'obiettivo è creare una policy di blocco con un firewall nella rete sottostante composta da un apparecchio Linux e un computer Metasploitable collegati in 2 reti interne differenti alla macchina Pfense quest'ultima sarà collegata sia alle reti interne differenti sia al router di internet.



In questo caso Pfense funge anche da switch che collega collegando così tutte le reti tra loro, infatti contiene 3 schede dei 3 collegamenti, la WAN con il router il che gli fornisce un indirizzo ip tramite il protocollo DHCP del router, che prevede l'assegnazione dell'IP automatica, mentre per le reti interne si definiscono manualmente e sono LAN con l'ip della macchina Kali e OPT1 con l'ip della Metasploitable.

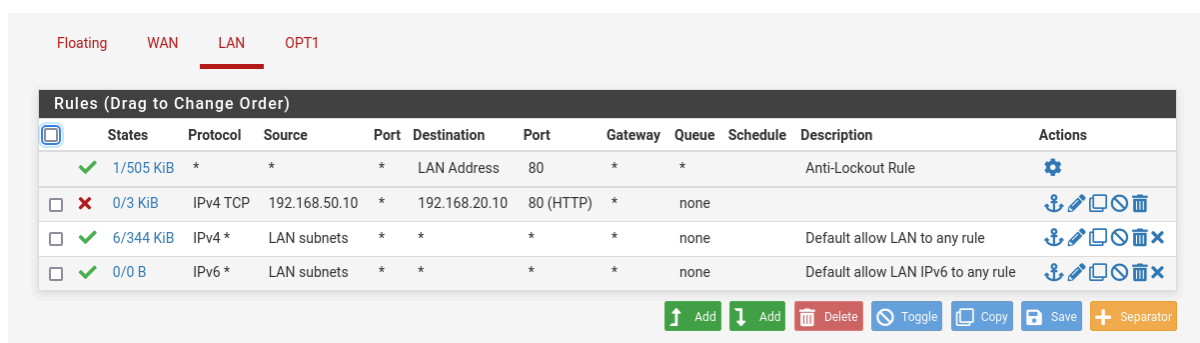
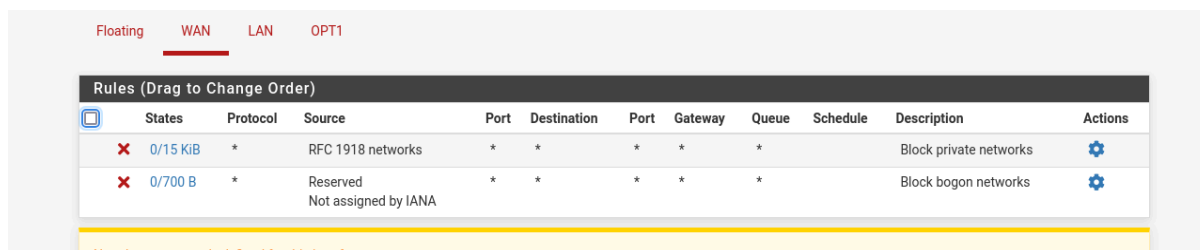
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

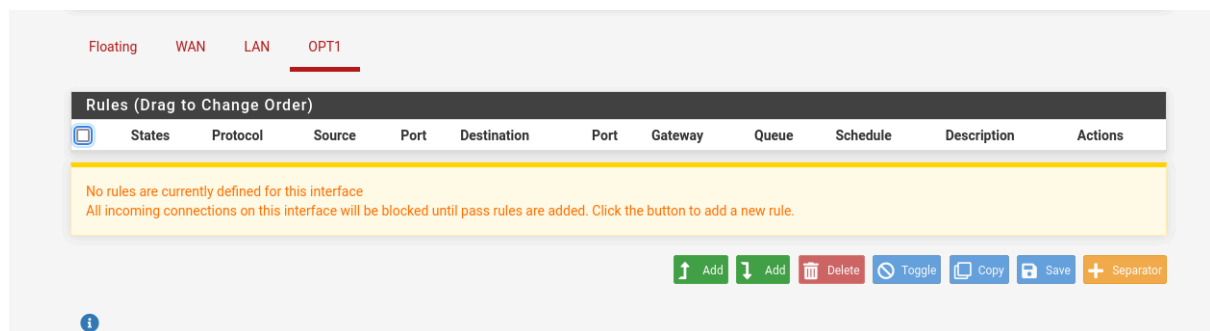
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.12/24
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0        -> v4: 192.168.20.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
```

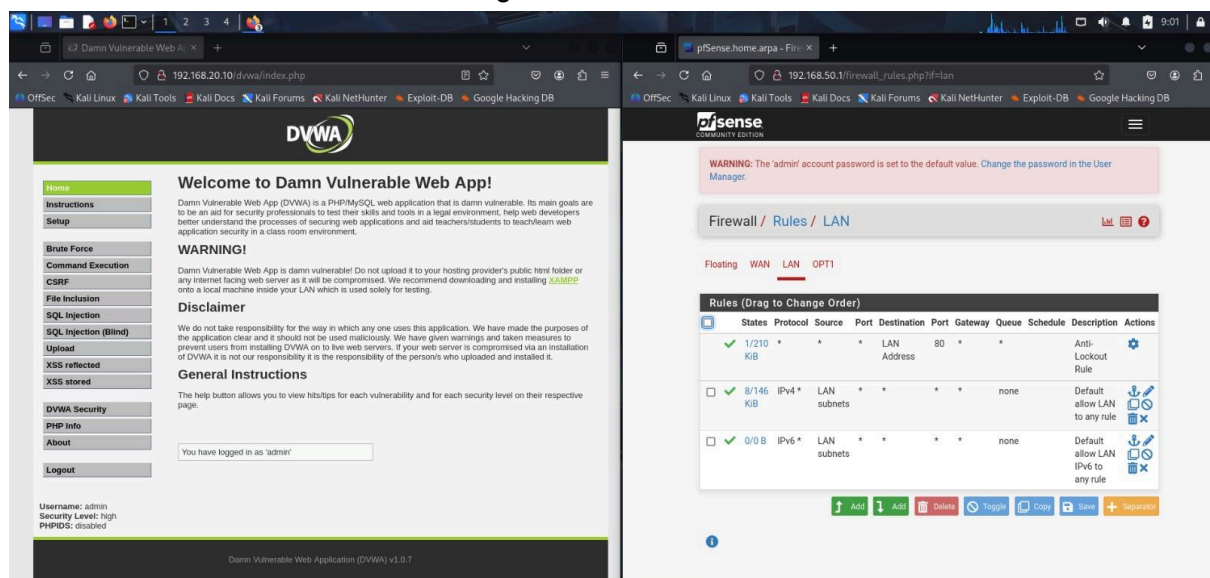
## COLLEGAMENTO

Tramite il browser della Kali possiamo accedere al pannello della Pfense, possiamo controllare da quest'ultima le configurazioni della rete e di tutti i suoi computer collegati ad essa.

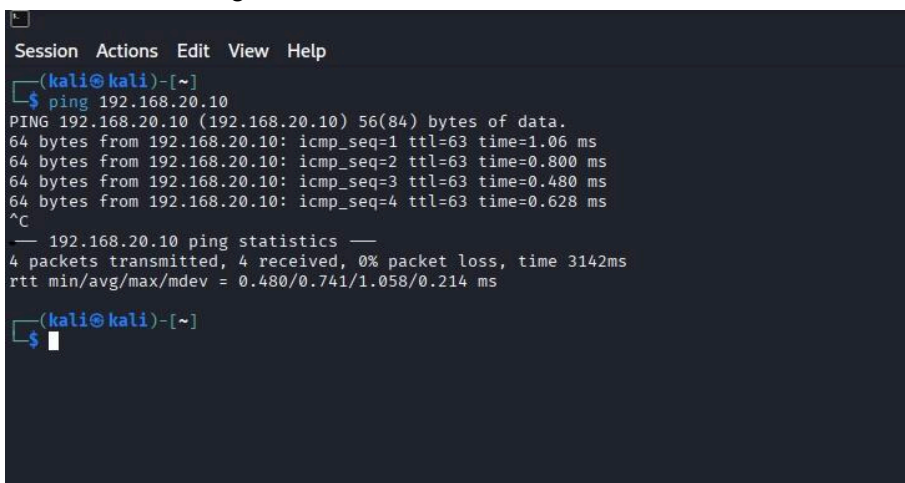




Infatti sempre tramite per testare il collegamento proviamo ad accedere, sempre tramite browser di Kali, sia alla pagina servita della Metasploitable, che a quella della Pfsense prova del fatto che nella rete siano tutti collegati tra loro,



dopo aver testato il collegamento di livello 7 della IO, ovvero tramite applicativo, testiamo il collegamento a livello base tramite ping della macchina in questo caso il ping partirà dal terminale della Kali, collegata solo a Pfsense e dovrà raggiungere Metasploitable, che anch'essa è collegata solo alla Pfsense.

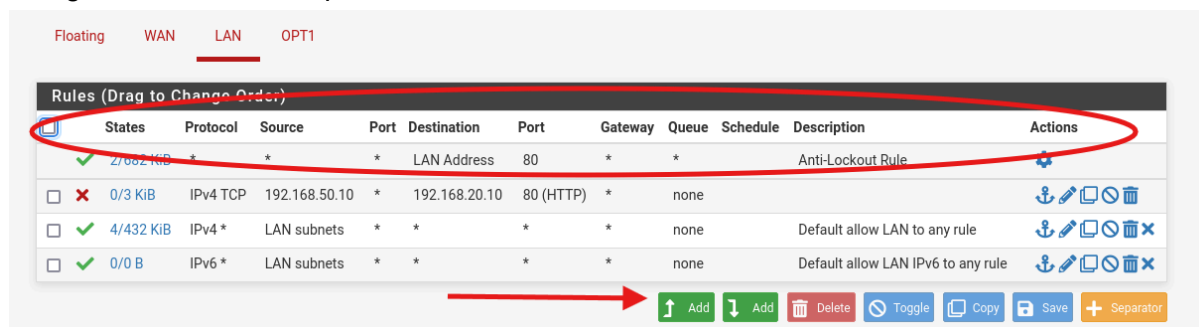


Questa dimostrazione prova che tutta la rete sia collegata come da progetto.

# POLICY DI BLOCCO PFSENSE

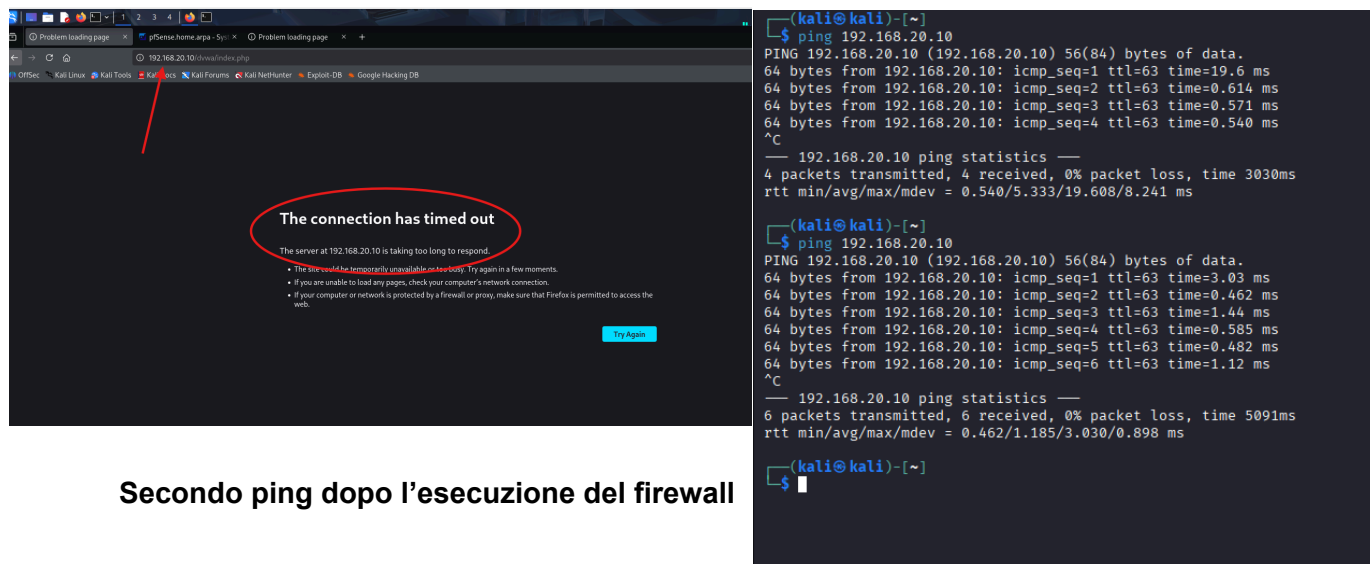
L'obiettivo è quello di mettere un blocco di firewall del protocollo HTTP dalla macchina Kali alla Metasploitable e quindi bloccare solamente la rete web tramite quest'ultimo protocollo.

Tramite browser Kali andiamo nell'area dedicata ai firewall alla scheda della Kali quindi al collegamento LAN dove possiamo creare un blocco.



Più il firewall si colloca in alto e più ha priorità di esecuzione, nel settaggio del andiamo a specificare che non si tratta di una respinta dell'accesso, che verrebbe notificato, ma di un blocco che semplicemente non fa accede, senza che ci venga inviata alcuna prova di accesso, specificando sia l'IP della Kali, ovvero l'ip di partenza, che l'IP della Metasploitable, quindi l'ip di arrivo, e settiamo unicamente il protocollo http con la porta 80, ricordando di posizionare il blocco nella rete interna.

Questa operazione farà sì che il browser della macchina Kali non sia più in grado di collegarsi con l'HTTP alla macchina Metasploitable, quindi quest'ultima non potrà più raggiungere l'indirizzo web.



Secondo ping dopo l'esecuzione del firewall

Ma comunque il collegamento della rete interna tra le due macchine continua, il blocco è unicamente per il protocollo HTTP quindi tramite ping possiamo provare che le macchine restano collegate tra loro e che la rete non ha avuto ripercussioni come da obiettivo del nostro firewall eseguito in modo corretto.