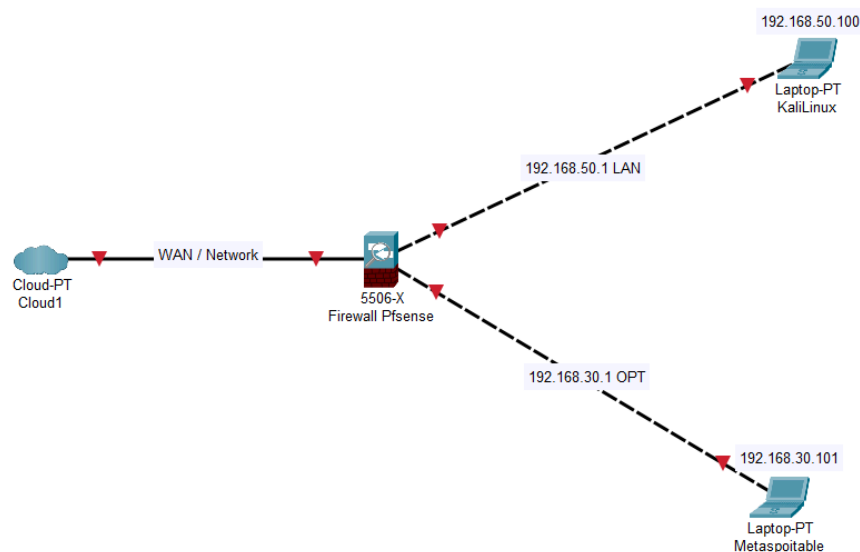


## S5.L1 Firewall

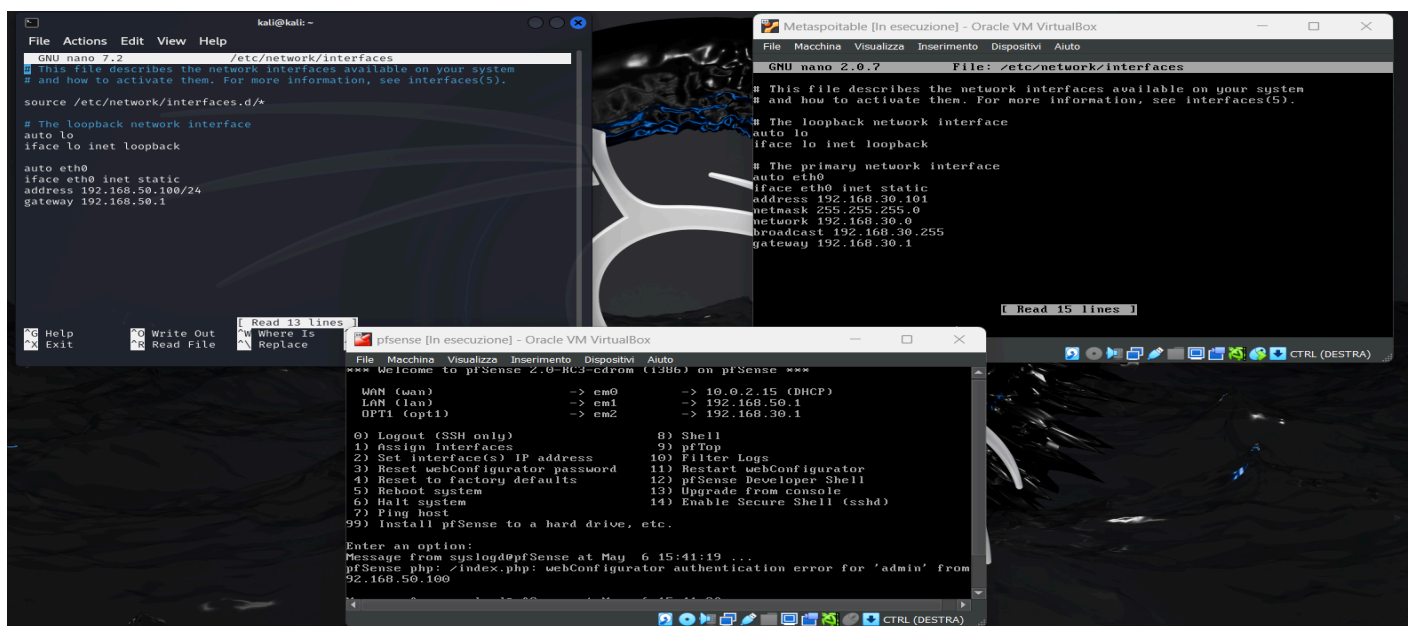
1 - È necessario configurare una regola del firewall che prevenga l'accesso a DVWA (su Metasploitable) dalla macchina Kali Linux e ne blocchi quindi la possibilità di effettuare scansioni. Una condizione essenziale per l'esercizio è che le macchine Kali e Metasploitable debbano trovarsi su reti separate; pertanto, è possibile aggiungere una nuova interfaccia di rete a Pfsense per amministrare una rete aggiuntiva.

### Simulazione di rete e utilizzo del firewall pfSense



Questa è una simulazione di rete con i relativi percorsi di rete ed un ipotetico utilizzo del firewall pfsense .

### 2 -Configurazione di Metasploitable e Kali Linux per l'utilizzo del firewall



### 3 - impostazioni firewall per impedire l'accesso in dvwa con l'utilizzo di pf sense

#### Accesso consentito:

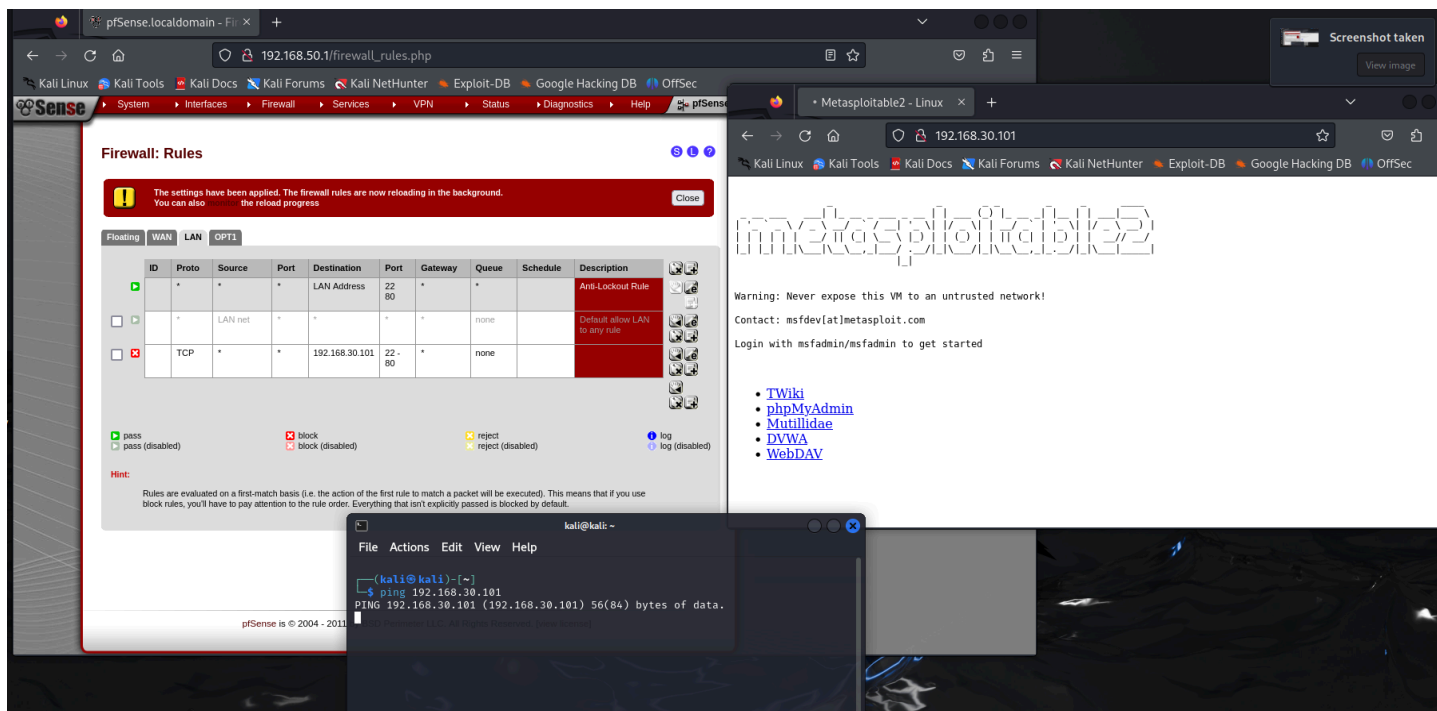
The screenshot displays the pfSense Firewall Rules configuration interface. A red notification bar at the top states: "The settings have been applied. The firewall rules are now reloading in the background. You can also monitor the reload progress." Below this, the "LAN" tab is selected, showing a table of rules. The first rule, "Anti-Logout Rule", is active and allows traffic from LAN to port 22. The second rule, "Default allow LAN to any rule", is also active and allows traffic from LAN to any destination. The third rule, "TCP", is active and allows traffic from LAN to port 22-80. The "pass" action is selected for all rules. A hint at the bottom states: "Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default."

Below the pfSense interface, a terminal window shows the output of a ping command to 192.168.30.101:

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali] ~  
$ ping 192.168.30.101  
PING 192.168.30.101 (192.168.30.101) 56(84) bytes of data:  
64 bytes from 192.168.30.101: icmp_seq=1 ttl=63 time=1.96 ms  
64 bytes from 192.168.30.101: icmp_seq=2 ttl=63 time=1.67 ms  
64 bytes from 192.168.30.101: icmp_seq=3 ttl=63 time=1.51 ms
```

- Le impostazioni di pfSense sono configurate per consentire il traffico HTTP/HTTPS verso l'indirizzo IP 192.168.30.101 (Metasploitable) dove è ospitato DVWA.
- Nell'esempio, le regole del firewall mostrano che l'accesso a tale indirizzo non viene bloccato, permettendo a utenti su Kali Linux e altri dispositivi nella rete di raggiungere DVWA.
- Il monitoraggio del traffico tramite logs di pfSense conferma che le richieste verso DVWA sono consentite e trattate correttamente.

## Accesso Negato:



- **Modifica delle regole del firewall in pfSense per bloccare esplicitamente il traffico verso l'indirizzo 192.168.30.101.**
- **L'interfaccia di configurazione mostra le regole aggiornate che negano il traffico. Questo impedisce l'accesso a DVWA da parte degli utenti, come verificato tramite tentativi di ping da Kali Linux verso Metasploitable, risultando in un fallimento del comando ping a causa delle restrizioni impostate.**

## Conclusioni

L'implementazione di pfSense come soluzione di firewall nella rete simulata offre un controllo flessibile e robusto del traffico, essenziale per la formazione sulla sicurezza e il testing. La capacità di configurare dettagliatamente l'accesso a risorse specifiche come DVWA dimostra l'efficacia di pfSense nel gestire scenari di sicurezza complessi in un ambiente controllato.