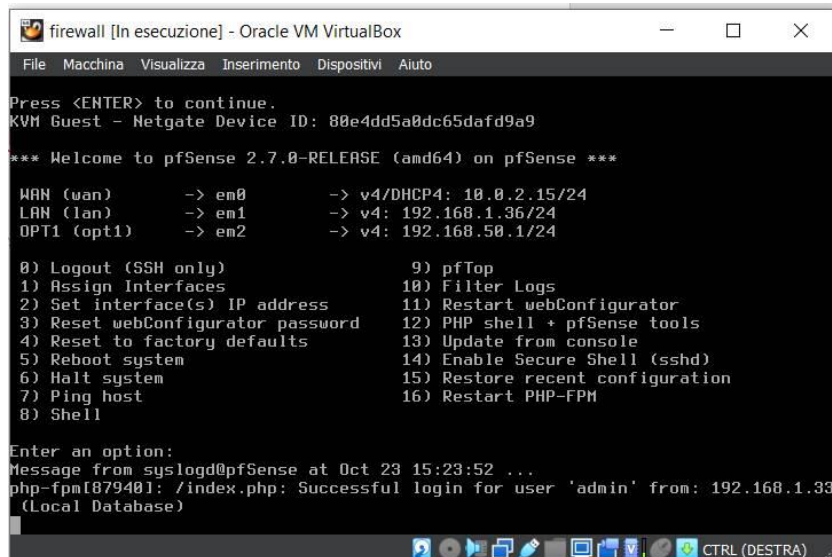


Settimana 5 Esercizio 1

Policy PfSense

- Configuriamo il firewall PfSense con 3reti diverse a cui corrispondono 3 schede di rete (NAT, Bridge e Interna);



```
firewall [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

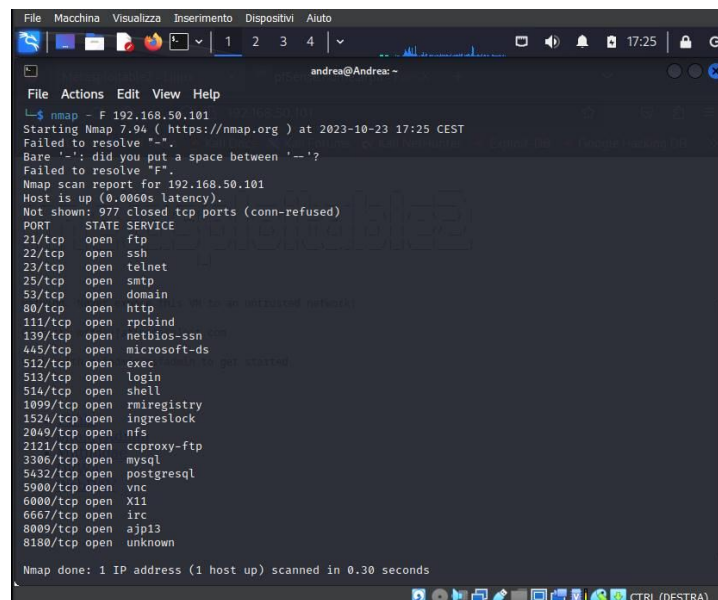
Press <ENTER> to continue.
KVM Guest - Netgate Device ID: 80e4dd5a0dc65dafd9a9

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.36/24
OPT1 (opt1)    -> em2      -> v4: 192.168.50.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Oct 23 15:23:52 ...
php-fpm[879401]: /index.php: Successful login for user 'admin' from: 192.168.1.33
(Local Database)
```

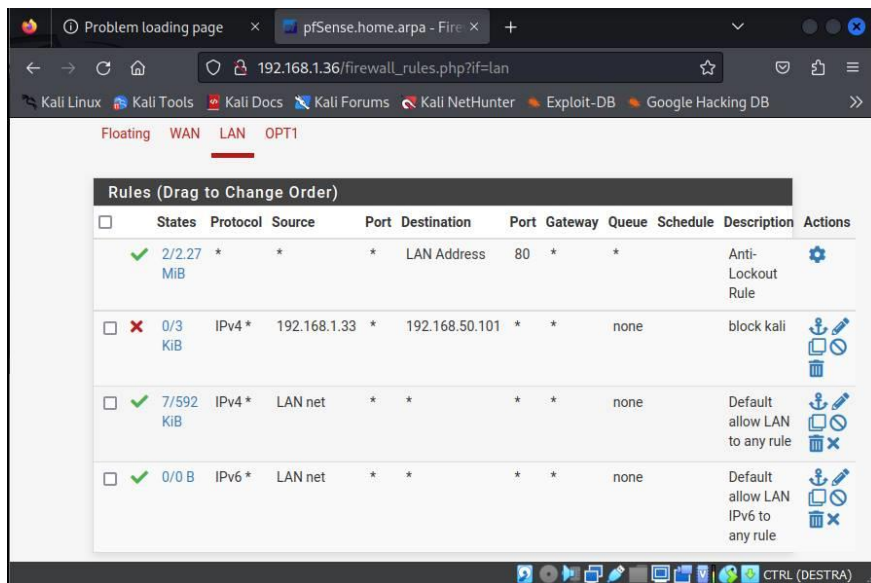


```
andrea@Andrea: ~
File  Actions  Edit  View  Help

nmap -F 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-23 17:25 CEST
Failed to resolve '-'.
Base '-': did you put a space between '--'?
Failed to resolve 'F'.
Nmap scan report for 192.168.50.101
Host is up (0.0060s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

- A questo punto le macchine comunicheranno (Kali e Meta) e andiamo a settare le regole per creare eccezioni. Possiamo creare restrizioni per molti protocolli, a noi interessa ICMP per il ping e TCP per l'http;



- A questo punto non ci sarà più connessione tra le due macchine, sia se andiamo a provare il ping sia se cerchiamo la pagina DVWA;

