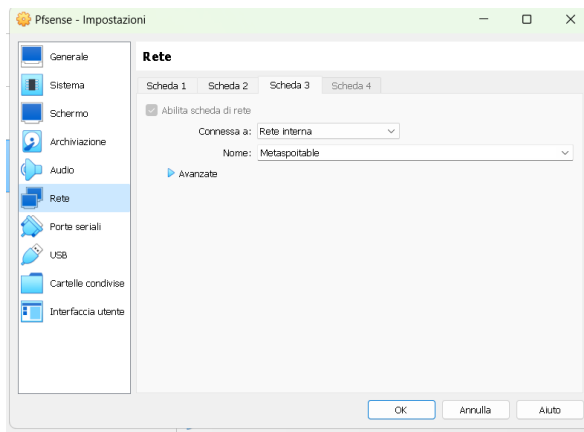
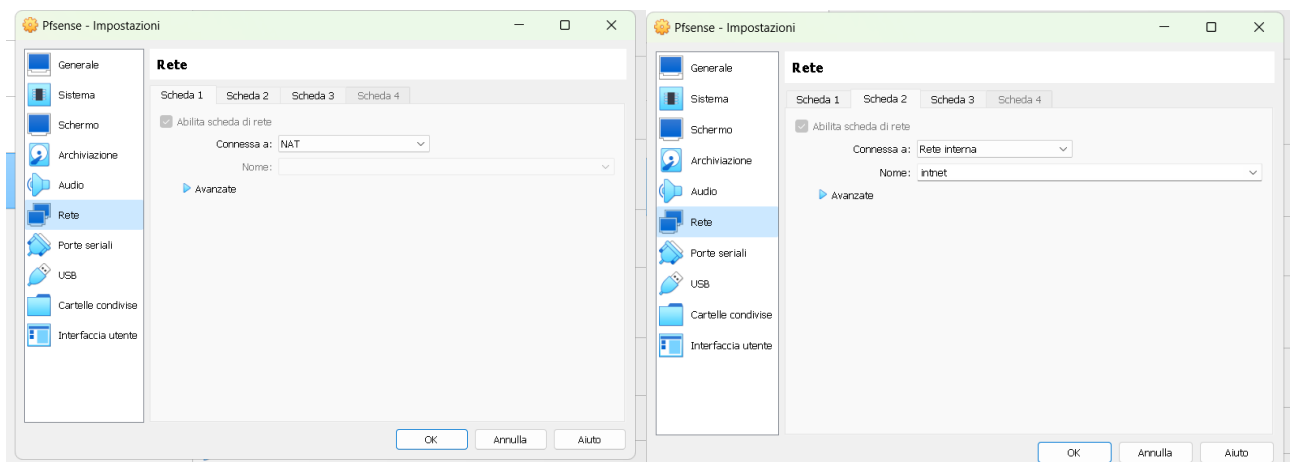


Configurazione delle reti virtuali , routing e firewall su Pfsense

Per procedere alla risoluzione dell'esercizio per creare la regola firewall su pfsense, dobbiamo prima configurare le schede di rete di quest'ultima.

- Abilitiamo la scheda di rete 1 in NAT per la connettività ad internet.
- Abilitiamo la scheda di rete 2 nella rete INTERNA intnet a cui conatteremo la macchina kali linux
- Abilitiamo la scheda di rete 3 nella rete INTERNA metasploitable a cui conatteremo appunto la macchina metasploitable2.



- Dopo queste procedure avviamo pfsense e notiamo che abbiamo attive 3 schede di rete.

```

Press ENTER to continue.

Message from syslogd@pfSense at Apr 22 20:02:45 ...
php-fpm[398]: /index.php: Successful login for user 'admin' from: 192.168.1.110
(Local Database)
^CVirtualBox Virtual Machine - Netgate Device ID: 13b55fdf296ff02e3724

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.2.1/24

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:

```

- Come abbiamo visto su pfsense ci sono attive 3 schede di rete, la rete interna INTNET sarà quella a cui collegheremo la macchina kali linux
- Sulla nostra macchina Metasoitable2 invece collegheremo la scheda di rete interna di pfsense ,chiamata appunto metaspitable.

```

GNU nano 2.0.7 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.2.120
netmask 255.255.255.0
network 192.168.2.0
broadcast 192.168.2.255
gateway 192.168.2.1

```

- Verifichiamo la raggiungibilità delle nostre 2 macchine da pfsense tramite il ping

```

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: 7

Enter a host name or IP address: 192.168.1.110

PING 192.168.1.110 (192.168.1.110): 56 data bytes
64 bytes from 192.168.1.110: icmp_seq=0 ttl=64 time=1.924 ms
64 bytes from 192.168.1.110: icmp_seq=1 ttl=64 time=1.854 ms
64 bytes from 192.168.1.110: icmp_seq=2 ttl=64 time=1.101 ms

--- 192.168.1.110 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.054/1.368/1.924/0.399 ms

Press ENTER to continue.

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: 7

Enter a host name or IP address: 192.168.2.120

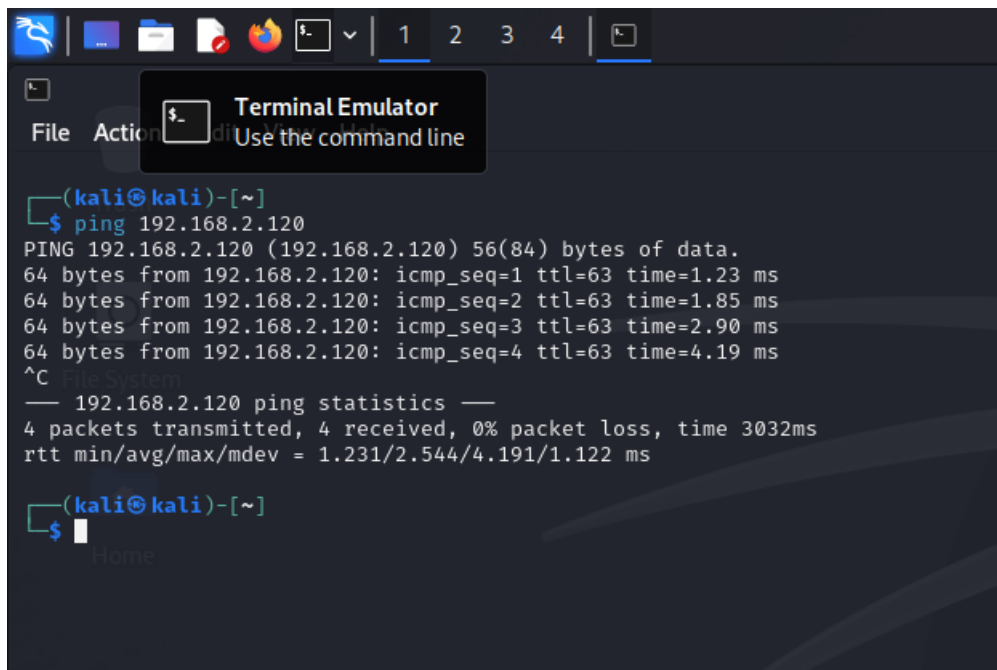
PING 192.168.2.120 (192.168.2.120): 56 data bytes
64 bytes from 192.168.2.120: icmp_seq=0 ttl=64 time=2.220 ms
64 bytes from 192.168.2.120: icmp_seq=1 ttl=64 time=0.846 ms
64 bytes from 192.168.2.120: icmp_seq=2 ttl=64 time=1.114 ms

--- 192.168.2.120 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.846/1.394/2.220/0.595 ms

Press ENTER to continue.

```

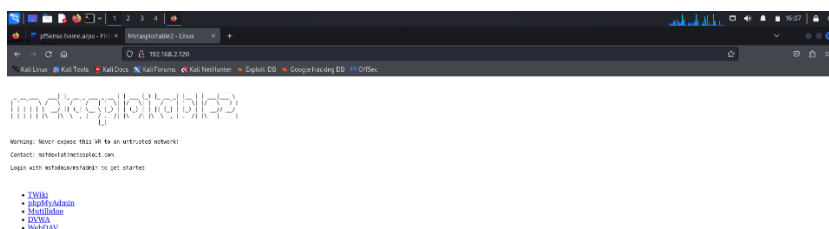
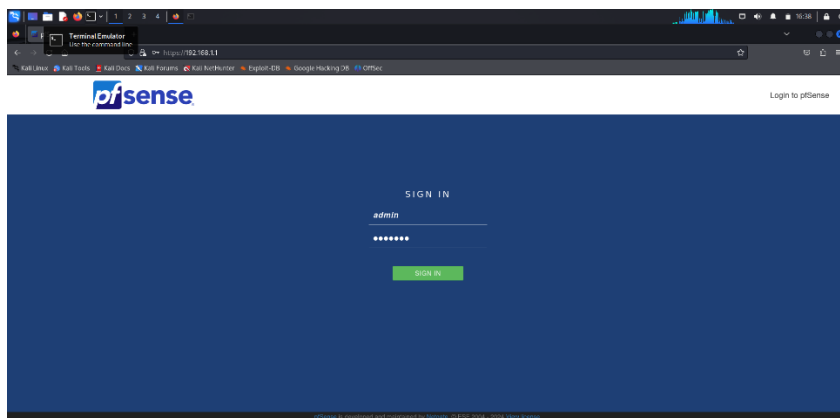
- Verifichiamo se da kali linux riusciamo a pingare la macchina metasoitable che è su un'altra rete.



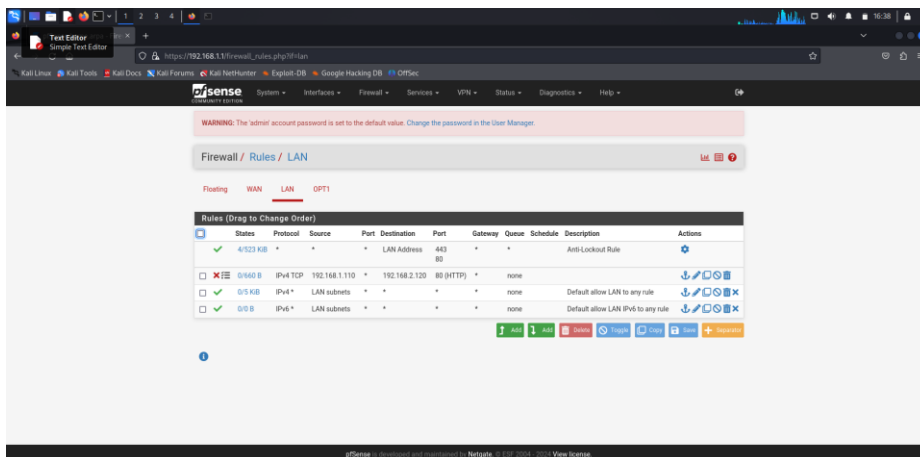
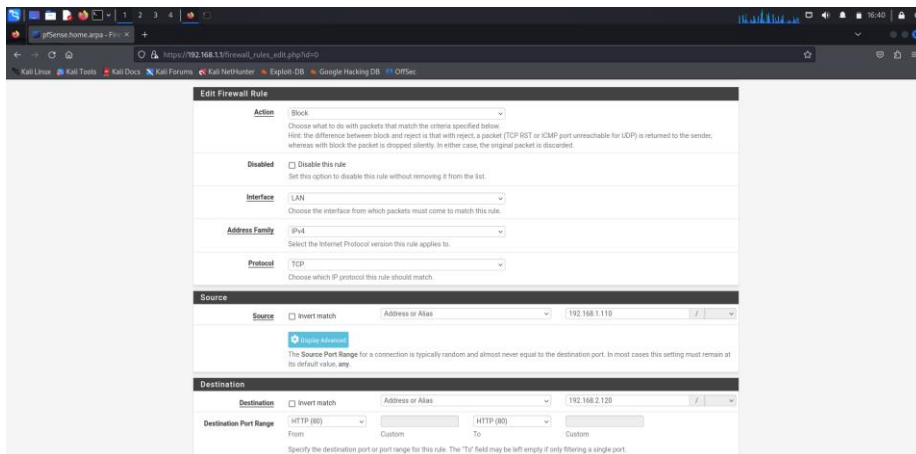
Terminal Emulator
Use the command line

```
(kali㉿kali)-[~]  
$ ping 192.168.2.120  
PING 192.168.2.120 (192.168.2.120) 56(84) bytes of data.  
64 bytes from 192.168.2.120: icmp_seq=1 ttl=63 time=1.23 ms  
64 bytes from 192.168.2.120: icmp_seq=2 ttl=63 time=1.85 ms  
64 bytes from 192.168.2.120: icmp_seq=3 ttl=63 time=2.90 ms  
64 bytes from 192.168.2.120: icmp_seq=4 ttl=63 time=4.19 ms  
^C  
— 192.168.2.120 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3032ms  
rtt min/avg/max/mdev = 1.231/2.544/4.191/1.122 ms  
  
(kali㉿kali)-[~]  
$
```

- Verifichiamo la raggiungibilità della pagina web di pfsense e della macchina metasploitable tramite kali linux.



- Impostiamo una nuova regola firewall da kali linux per bloccare il traffico dati sulla porta 80 di metasploitable tramite pfSense



- Verifichiamo se la regola che abbiamo appena applicato funziona



