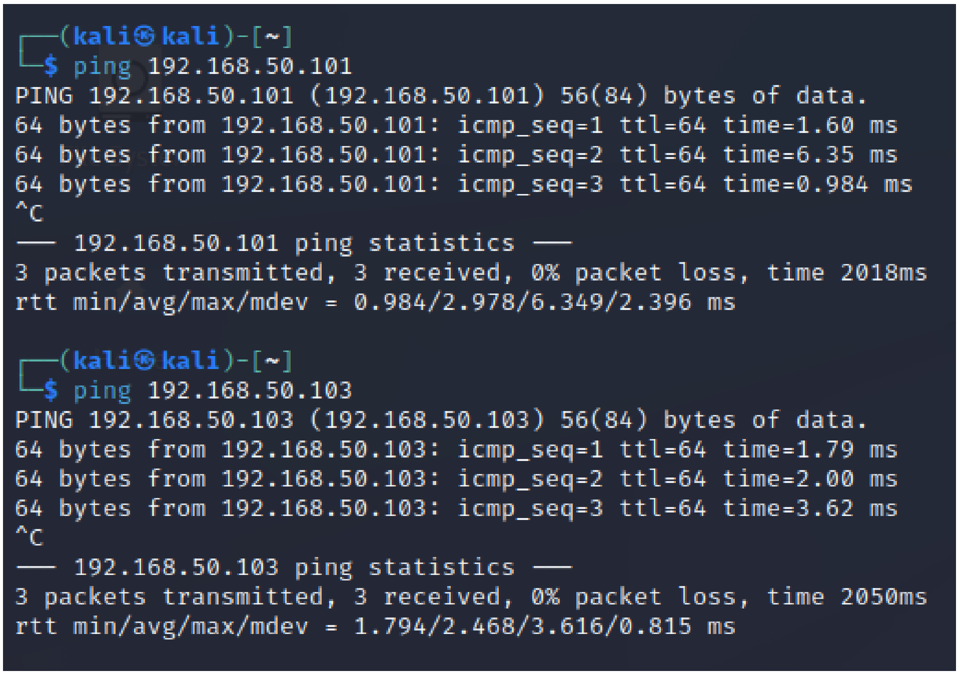
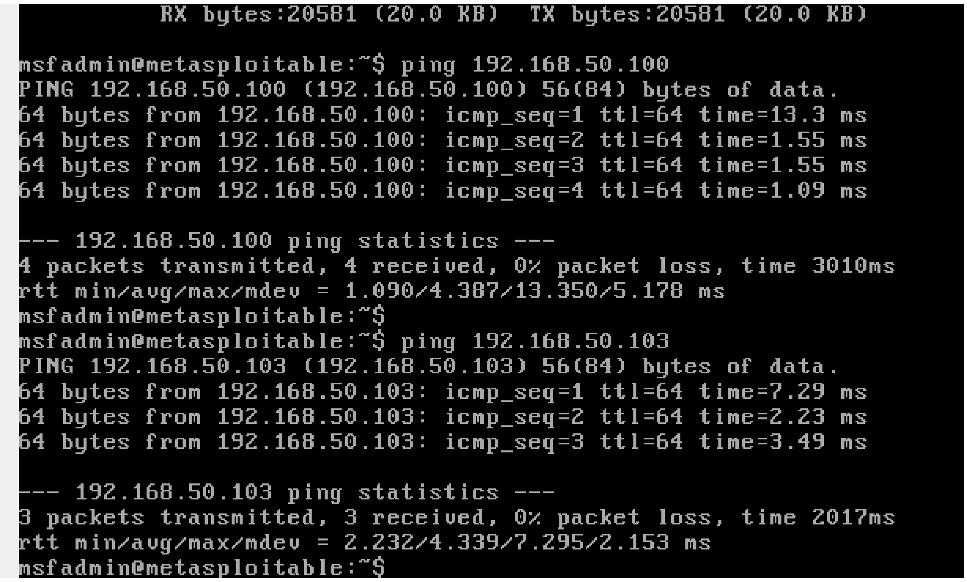
Creazione policy Pfsense

Innanzitutto mostro il ping tra le 3 macchine (Kali, Meta e Pfsense).



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.60 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=6.35 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.984 ms
^C
--- 192.168.50.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.984/2.978/6.349/2.396 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.103
PING 192.168.50.103 (192.168.50.103) 56(84) bytes of data.
64 bytes from 192.168.50.103: icmp_seq=1 ttl=64 time=1.79 ms
64 bytes from 192.168.50.103: icmp_seq=2 ttl=64 time=2.00 ms
64 bytes from 192.168.50.103: icmp_seq=3 ttl=64 time=3.62 ms
^C
--- 192.168.50.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2050ms
rtt min/avg/max/mdev = 1.794/2.468/3.616/0.815 ms
```

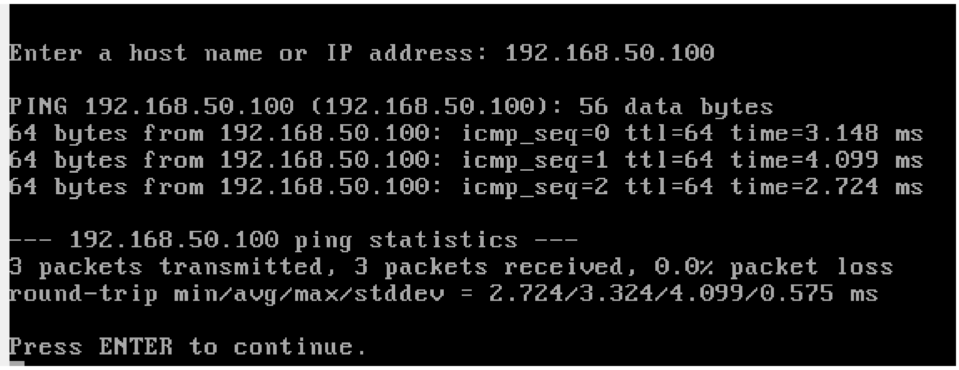


```
          RX bytes:20581 (20.0 KB)  TX bytes:20581 (20.0 KB)

msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=13.3 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.55 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=1.55 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.09 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 1.090/4.387/13.350/5.178 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ping 192.168.50.103
PING 192.168.50.103 (192.168.50.103) 56(84) bytes of data.
64 bytes from 192.168.50.103: icmp_seq=1 ttl=64 time=7.29 ms
64 bytes from 192.168.50.103: icmp_seq=2 ttl=64 time=2.23 ms
64 bytes from 192.168.50.103: icmp_seq=3 ttl=64 time=3.49 ms

--- 192.168.50.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2017ms
rtt min/avg/max/mdev = 2.232/4.339/7.295/2.153 ms
msfadmin@metasploitable:~$
```



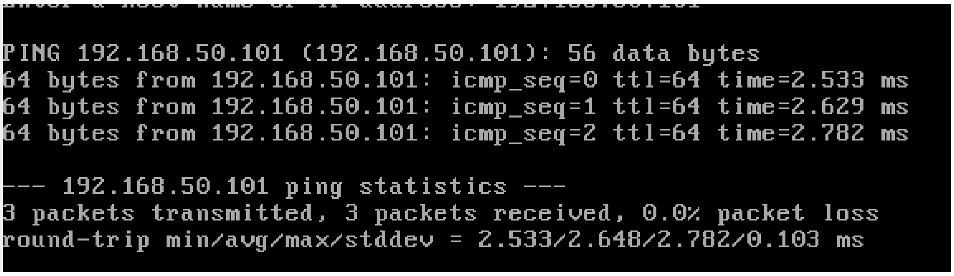
```
Enter a host name or IP address: 192.168.50.100

PING 192.168.50.100 (192.168.50.100): 56 data bytes
64 bytes from 192.168.50.100: icmp_seq=0 ttl=64 time=3.148 ms
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=4.099 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=2.724 ms

--- 192.168.50.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.724/3.324/4.099/0.575 ms

Press ENTER to continue.
```

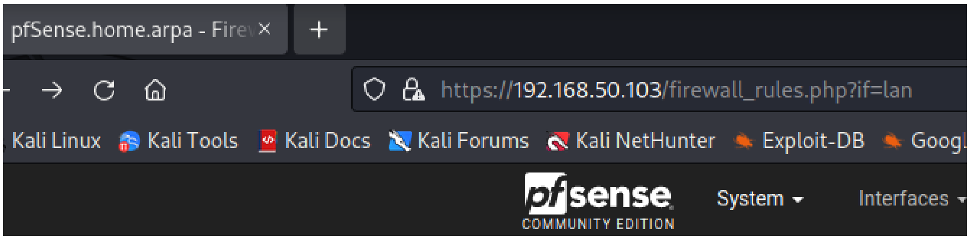
```
Enter a host name or IP address: 192.168.50.101
```



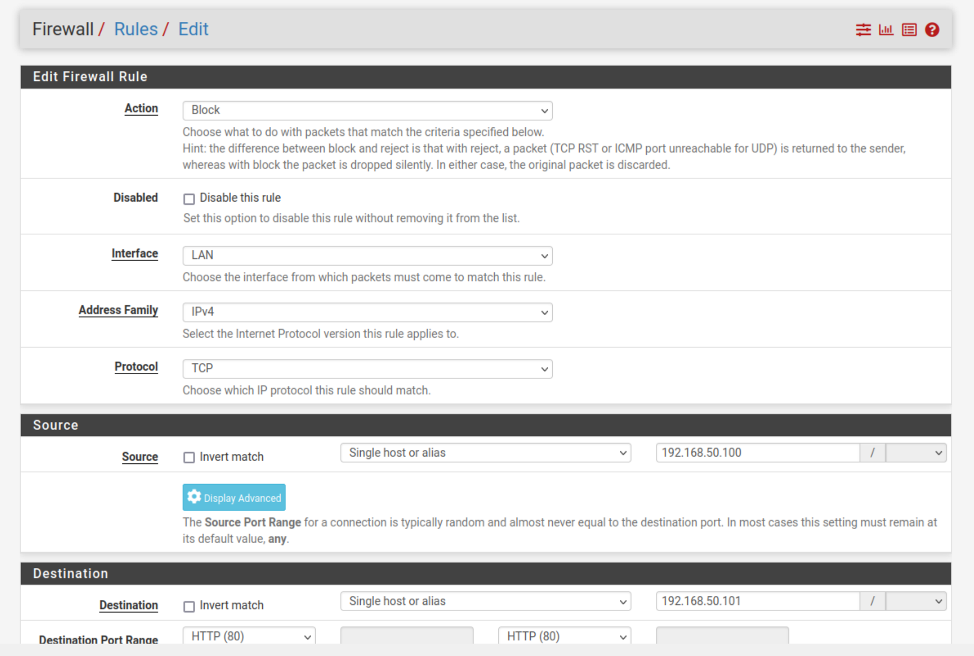
```
PING 192.168.50.101 (192.168.50.101): 56 data bytes
64 bytes from 192.168.50.101: icmp_seq=0 ttl=64 time=2.533 ms
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=2.629 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=2.782 ms

--- 192.168.50.101 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.533/2.648/2.782/0.103 ms
```

Aprire sul browser il firewall sulla sezione Rules



pfSense.home.arpa - Firev
https://192.168.50.103/firewall_rules.php?if=lan
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Googl
pfsense COMMUNITY EDITION
System
Interfaces



Firewall / Rules / Edit

Edit Firewall Rule

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: LAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP
Choose which IP protocol this rule should match.

Source

Source: ☐ Invert match | Single host or alias | 192.168.50.100 /

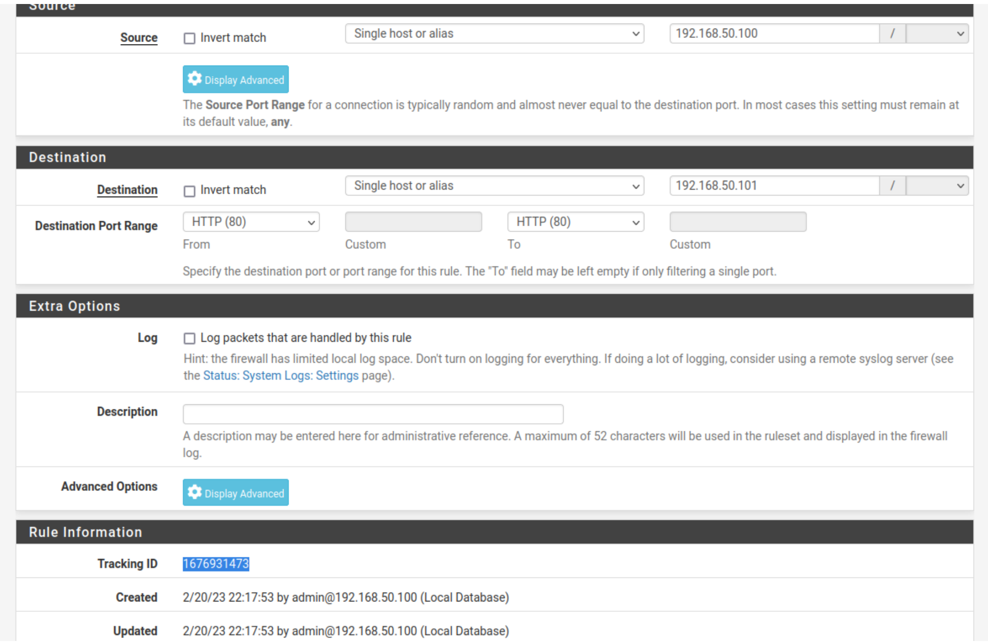
Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: ☐ Invert match | Single host or alias | 192.168.50.101 /

Destination Port Range: HTTP (80) | | HTTP (80) |



Source

Source: ☐ Invert match | Single host or alias | 192.168.50.100 /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: ☐ Invert match | Single host or alias | 192.168.50.101 /

Destination Port Range: HTTP (80) From | Custom | HTTP (80) To | Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log: ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description:
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

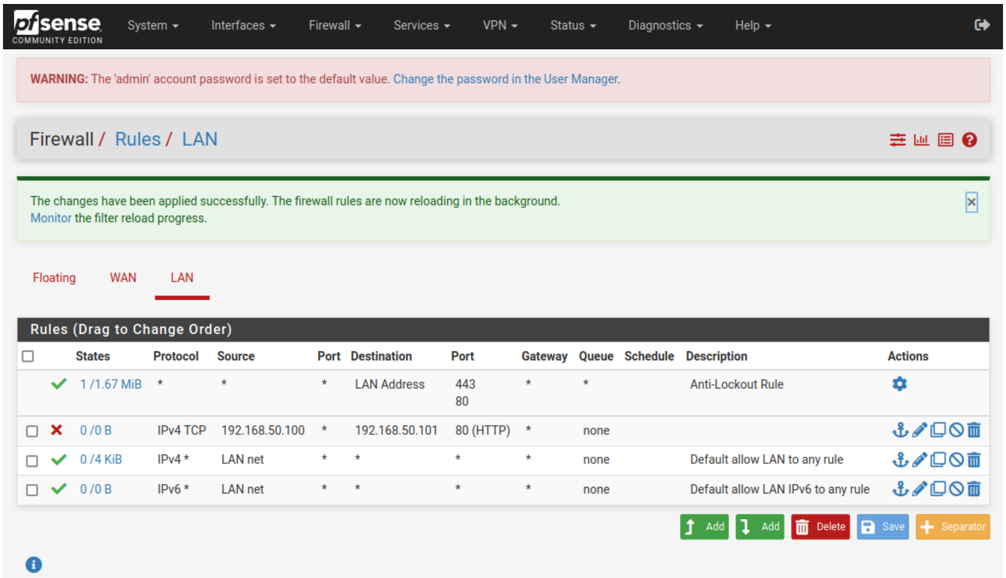
Advanced Options: Display Advanced

Rule Information

Tracking ID: 1676931473

Created: 2/20/23 22:17:53 by admin@192.168.50.100 (Local Database)

Updated: 2/20/23 22:17:53 by admin@192.168.50.100 (Local Database)



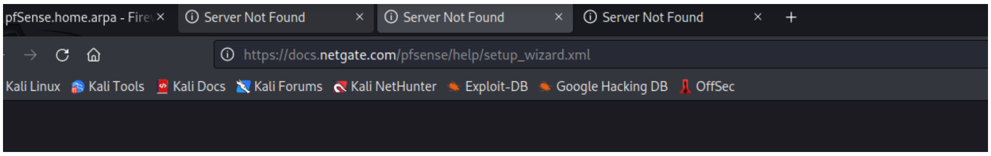
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / LAN

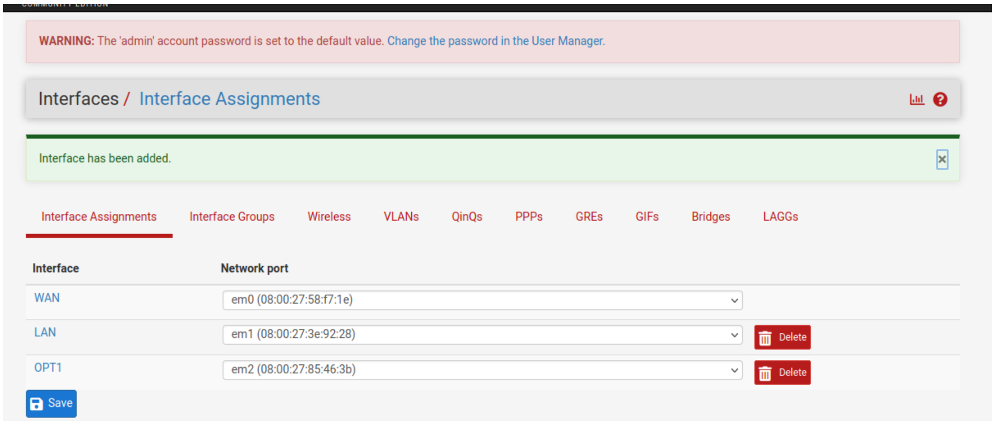
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /1.67 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
□	✗	0 /0 B	IPv4 TCP	192.168.50.100	*	192.168.50.101	80 (HTTP)	*	none			
□	✓	0 /4 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	



https://docs.netgate.com/pfsense/help/setup_wizard.xml



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces / Interface Assignments

Interface has been added.

Interface	Network port	
WAN	em0 (08:00:27:58:f7:1e)	
LAN	em1 (08:00:27:3e:92:28)	Delete
OPT1	em2 (08:00:27:85:46:3b)	Delete