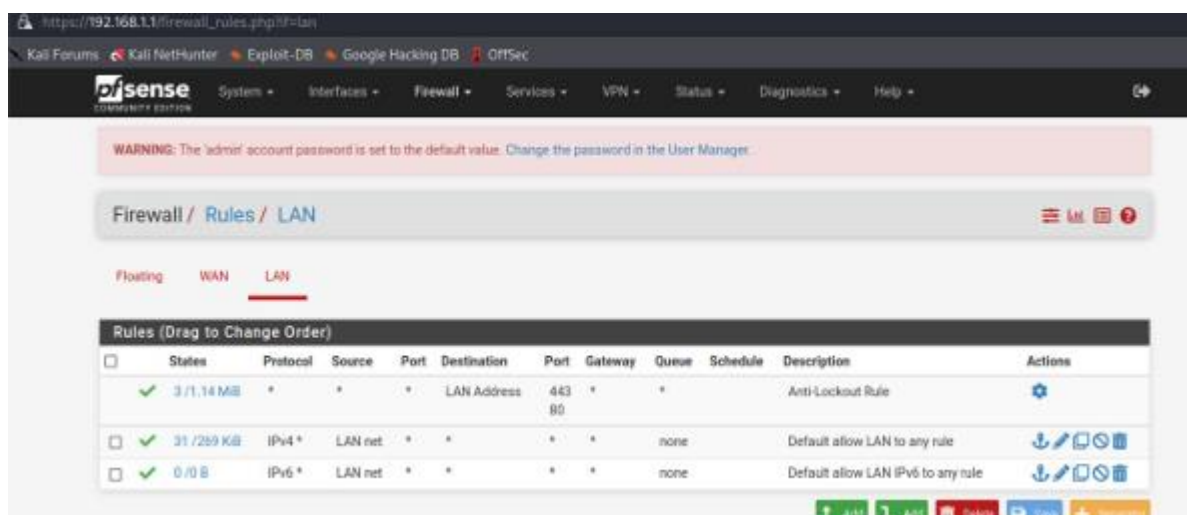


## Progetto S3/L5

### Creazione policy Pfsense

Data la traccia:







“Creazione pratica di una regola Firewall. Esercizio Pfsense Per la creazione di una regola firewall, andare su Firewall > Rules. In questa sezione si può scegliere su quale interfaccia creare la regola: scegliamo LAN e clicchiamo su ADD (come vedete ci sono 2 add, il primo crea la regola in cima al policy set, la seconda in basso):”




Sulla base di quanto visto, creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.

## Sviluppo della traccia: configurazione


Negli screen seguenti riporto la configurazione delle schede di rete delle macchine virtuali utilizzate:

Metasploitable2		Generale	
	Spenta	Nome:	Metasploitable2
		Sistema operativo:	Linux 2.6 / 3.x / 4.x / 5.x (32-bit)
Windows 10		Sistema	
	Spenta	Memoria di base:	512 MB
		Ordine di avvio:	Floppy, Ottico, Disco fisso
		Accelerazione:	PAE/NX, Paravirtualizzazione KVM
Windows 7		Schermo	
	Spenta	Memoria video:	16 MB
		Scheda grafica:	VMSVGA
		Server di desktop remoto:	Disabilitato
		Registrazione:	Disabilitata
Windows 10 ita		Archiviazione	
	Spenta	Controller: IDE	
		Dispositivo IDE secondario 0:	[Lettore ottico] Vuoto
		Controller: SATA	
		Porta SATA 0:	Metasploitable.vmdk (Normale, 8,00 GB)
pfsense		Audio	
	Spenta	Driver host:	Predefinita
		Controller:	ICH AC97
kali-linux-2024.3-virtualbox-amd64		Rete	
	Spenta	Scheda 1:	Intel PRO/1000 MT Desktop (Rete interna, 'intnet')




Metasploitable2

Spenta




Windows 10

Spenta




Windows 7

Spenta




Windows 10 ita

Spenta



pfsense

Spenta



kali-linux-2024.3-virtualbox-amd64

Spenta

Generale

Nome:

kali-linux-2024.3-virtualbox-amd64

Sistema operativo:

Debian (64-bit)

Sistema

Memoria di base:

2048 MB

Processori:

2

Ordine di avvio:

Disco fisso, Ottico

Accelerazione:

Paginazione nidificata, PAE/NX, Paravirtualizzazione KVM

Schermo

Memoria video:

128 MB

Scheda grafica:

VMSVGA

Server di desktop remoto:

Disabilitato

Registrazione:

Disabilitata

Archiviazione

Controller: IDE

Dispositivo IDE secondario 0: [Lettore ottico] Vuoto

Controller: SATA

Porta SATA 0: kali-linux-2024.3-virtualbox-amd64.vdi (Normale, 80,09 GB)

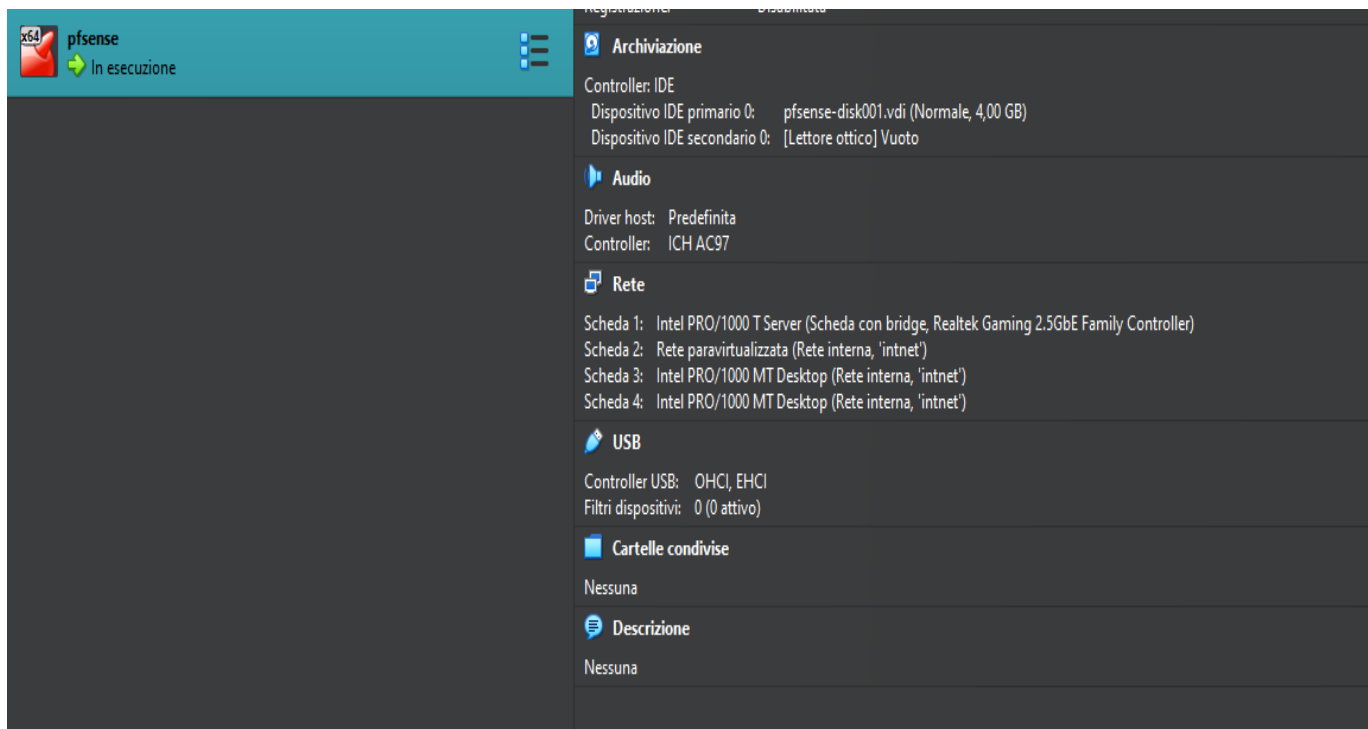
Audio

Driver host: Windows DirectSound

Controller: ICH AC97

Rete

Scheda 1: Intel PRO/1000 MT Desktop (Rete interna, 'intnet')



Come possiamo vedere abbiamo impostato Pfsense con la 1° scheda di rete come “Bridge” e le restanti come “Rete interna”, mentre le nostre macchine virtuali di Metasploitable e Kali Linux sono su rete interna.

Dopo aver configurato le nostre macchine virtuali, andiamo a configurare gli IP. Vanno configurati in modo che non ci siano blocchi tra di loro e che, come richiesto dalla traccia, Metasploitable e Kali siano di 2 reti diverse (quindi andremo a cambiare il 3° ottetto), mentre Pfsense e Kali faranno parte della stessa rete.

Riporto screen di seguito che mostreranno gli IP delle 3 componenti:

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:dd:16:1e
          inet addr:192.168.50.152  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedd:161e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4434 (4.3 KB)  TX bytes:7272 (7.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25525 (24.9 KB)  TX bytes:25525 (24.9 KB)

```

Sull'immagine che troviamo sopra possiamo vedere l'IP di Metasploitable, che abbiamo cambiato grazie al comando

**“sudo ifconfig eth0 192.168.50.152 netmask 255.255.255.0”**

```

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.151/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
        valid_lft 6314sec preferred_lft 6314sec
    inet6 fe80::d39:5f44:2506:319c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali@kali)-[~]

```

Qua invece possiamo vedere sottolineato in rosso l'IP che abbiamo scelto per Kali, lo possiamo vedere grazie al comando “ip a”

Enable ☒ Enable interface

Description   
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU   
If this field is blank, the adapter's default MTU will be used. This is typically 1500.

MSS   
If a value is entered in this field, then MSS clamping for TCP connection minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex   
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed)

**Static IPv4 Configuration**

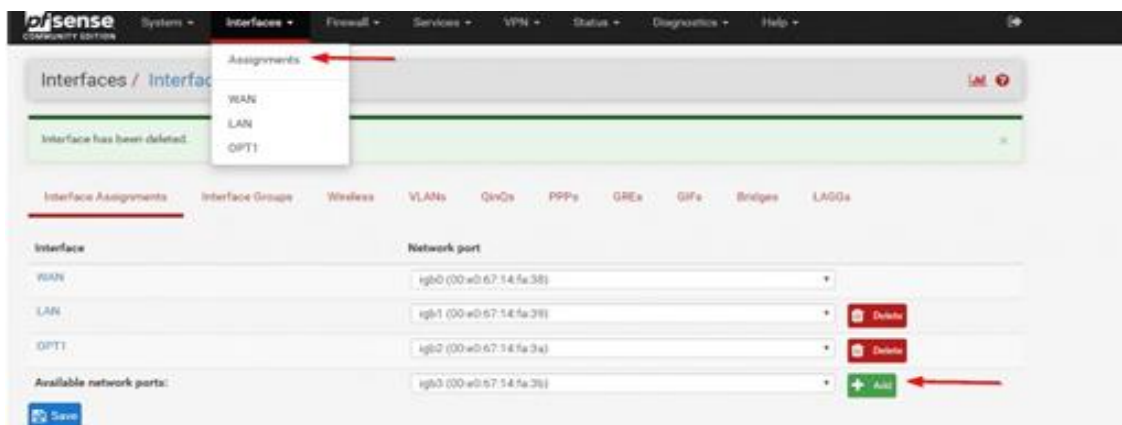
IPv4 Address

E qui vediamo che l'IP di Pfsense ha i tre ottetti uguali a quello di Kali, quindi fanno parte della stessa rete ("192.168.50")

In questo caso l'IP possiamo vederlo anche dall'URL in alto, ossia "192.168.50.1"

## Interface: aggiungere un OTP

Una volta che abbiamo completato la parte di settaggio e di configurazione delle VM e dei vari IP, ora possiamo aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete:



Cliccando su “Add”, di fianco alla freccia, possiamo aggiungere la rete di Metasploitable che abbiamo configurato.

Completato questo passaggio, andiamo a selezionare “OPT2” dopo aver aggiunto la rete, e configuriamo l’IP statico che abbiamo cambiato prima su Metasploitable:

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="OPT2"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> This field can be used to modify (“spoof”) the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

### Static IPv4 Configuration

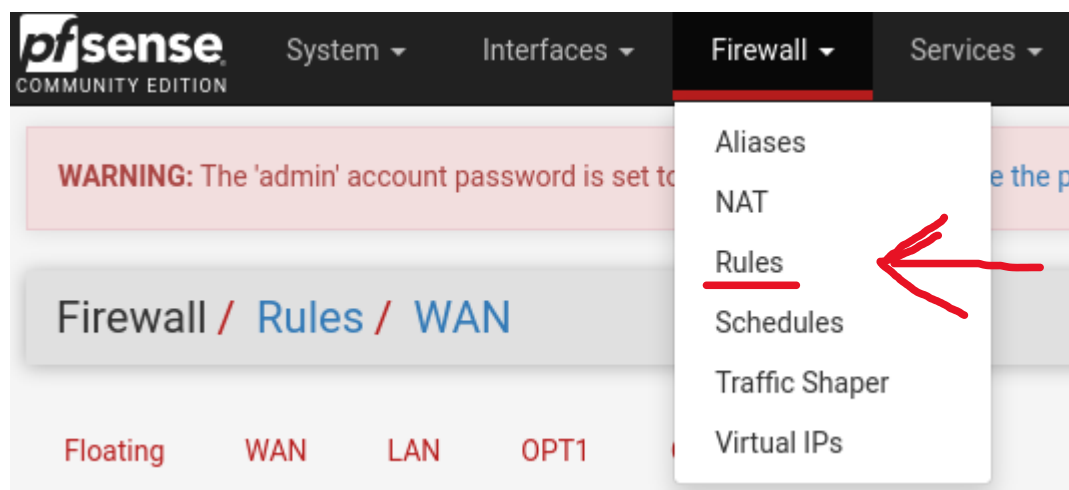
IPv4 Address	<input type="text" value="192.168.60.150"/>	/ 24
--------------	---	------

L’IP ovviamente combacerà con quello inserito prima a terminale, e dobbiamo andare a modificare anche il valore CIDR, mettendo /24 come spiegato precedentemente.

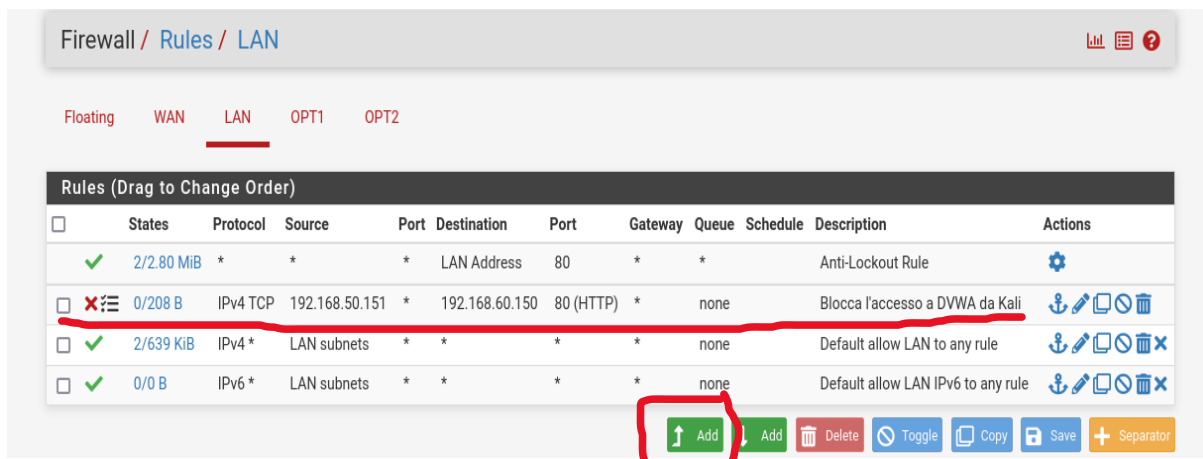
## Creazione della Regola del Firewall

A questo punto andiamo a creare la nostra policy Pfsense.

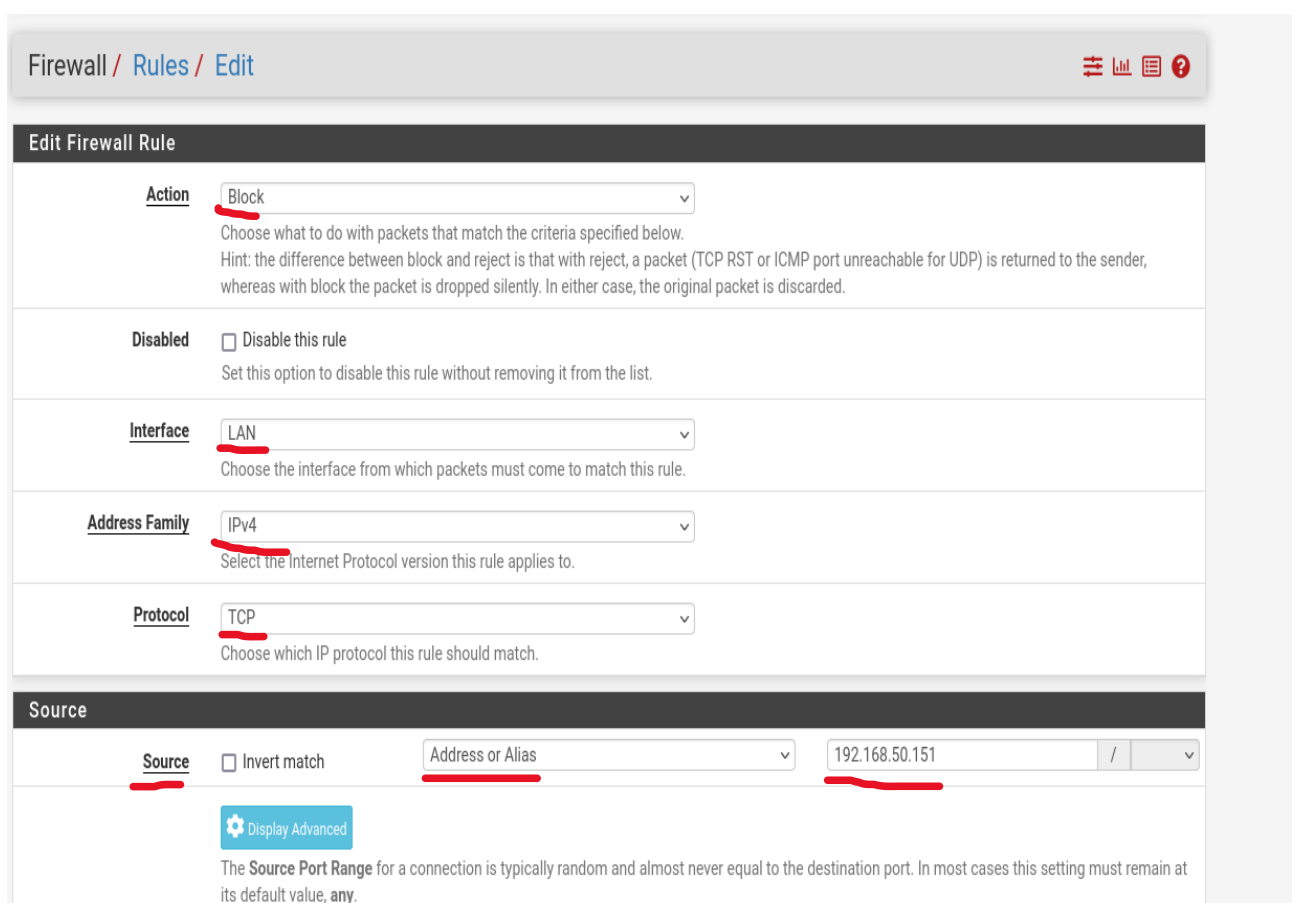
Per farlo, dobbiamo seguire un iter di azioni che spiegherò di seguito: in alto a sinistra clicchiamo su Firewall, si aprirà un menù a tendina dove dobbiamo andare a scegliere l'opzione "Rules", come in figura sotto:



Procediamo ora con la creazione, in questo caso “aggiungere” una regola al nostro firewall. Clicchiamo su “Add”, quello con la freccia rivolta verso l’alto (è importante dal momento che le regole nei Firewall hanno una maggiore importanza, una maggiore priorità, andando dall’alto verso il basso), come nella figura che troviamo più in basso:



Mostrerò invece nell'immagine di seguito la configurazione della regola:





**Destination**

Destination ☐ Invert match Address or Alias 192.168.60.150 /

**Destination Port Range** HTTP (80) From Custom 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** Blocca l'accesso a DVWA da Kali  
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	1734097342
Created	12/13/24 13:42:22 by admin@192.168.50.151 (Local Database)
Updated	12/13/24 14:21:28 by admin@192.168.50.151 (Local Database)

[Save](#)

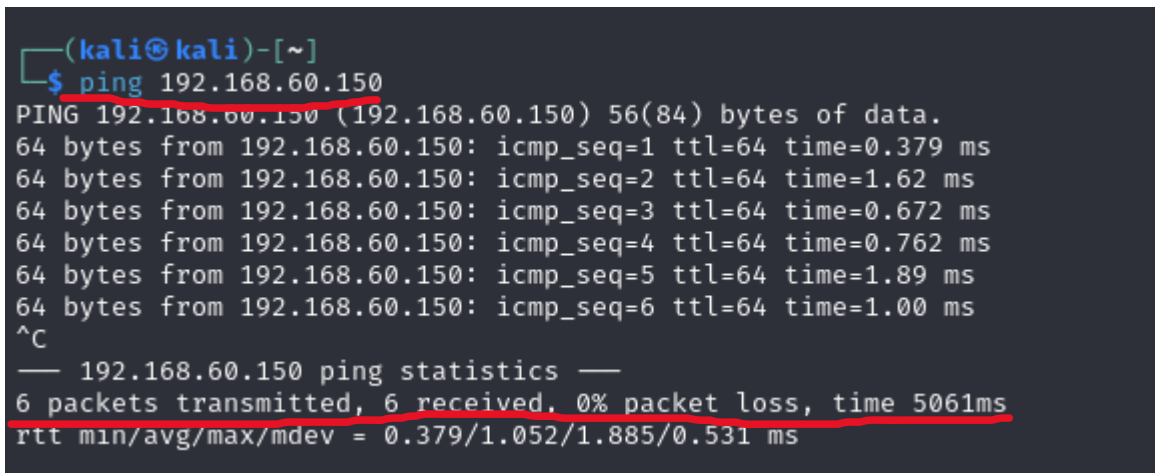
Come si può notare dalla configurazione in “Action” è una Regola di “Blocco”, andiamo a selezionare l’IP di destinazione (ovvero quello della nostra macchina Metasploitable, dato che andremo a bloccare la visualizzazione della DVWA di Metasploitable) e in Source il nostro tester, in questo caso Kali, quindi inseriamo l’IP di Kali.

## Verifica della regola aggiunta

Dal momento che abbiamo completato tutti questi step possiamo ora andare a fare le dovute verifiche per dimostrare che abbiamo eseguito tutto correttamente:

1) Proviamo come prima cosa a vedere se Kali e Metasploitable riescono a comunicare tra di loro grazie a PFsense.

Immettiamo un comando di ping da Kali verso Metasploitable, in questo modo: “ping” 192.168.60.150 (IP di Metasploitable). Vedi dimostrazione nella figura che segue:



```
(kali㉿kali)-[~]  
$ ping 192.168.60.150  
PING 192.168.60.150 (192.168.60.150) 56(84) bytes of data.  
64 bytes from 192.168.60.150: icmp_seq=1 ttl=64 time=0.379 ms  
64 bytes from 192.168.60.150: icmp_seq=2 ttl=64 time=1.62 ms  
64 bytes from 192.168.60.150: icmp_seq=3 ttl=64 time=0.672 ms  
64 bytes from 192.168.60.150: icmp_seq=4 ttl=64 time=0.762 ms  
64 bytes from 192.168.60.150: icmp_seq=5 ttl=64 time=1.89 ms  
64 bytes from 192.168.60.150: icmp_seq=6 ttl=64 time=1.00 ms  
^C  
— 192.168.60.150 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5061ms  
rtt min/avg/max/mdev = 0.379/1.052/1.885/0.531 ms
```

2) Se facciamo una prova disabilitando momentaneamente la regola, dovremmo visualizzare correttamente la porta in quanto non viene bloccata.

Come vediamo nel tentativo di comando “nmap” sotto invece, riabilitandola, la scansione verrà bloccata.

```
(kali㉿kali)-[~]
$ nmap -p 80 192.168.60.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 08:44 EST
Nmap scan report for 192.168.60.150
Host is up (0.0018s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

(kali㉿kali)-[~]
$ nmap -p 80 192.168.60.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 08:53 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds

(kali㉿kali)-[~]
$ nmap -p 80 192.168.60.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 08:58 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds
```

2b) Se utilizziamo il comando “nmap” con i privilegi da amministratore, ovvero con il comando “sudo” avremo lo stesso risultato ma con la precisazione che la porta è filtrata tramite firewall in quel momento:

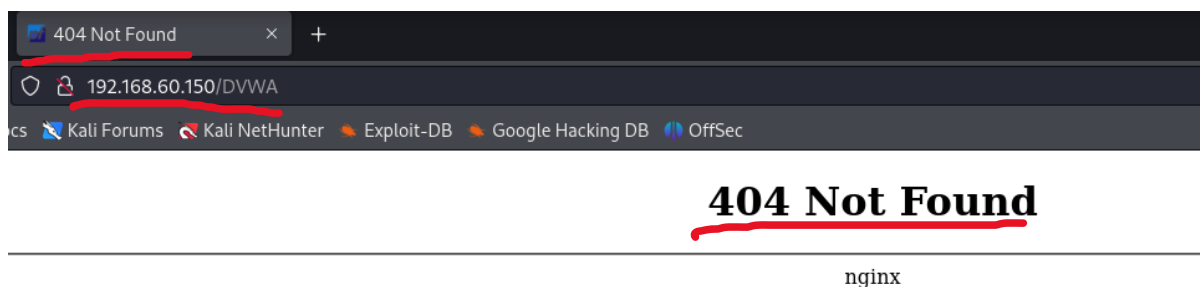
```
(kali㉿kali)-[~]
$ sudo nmap -p 80 192.168.60.150
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 09:56 EST
Nmap scan report for 192.168.60.150
Host is up (0.00070s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

3) Proviamo ora ad andare a visualizzare il DVWA di Metasploitable, mettendo nell’indirizzo URL l’IP di Metasploitable e DVWA, in questo modo: 192.168.60.150/DVWA

Riporto screen della prova di seguito:



Essendo che abbiamo bloccato il passaggio dei pacchetti nella porta 80, con il protocollo TCP, e come destinazione l'IP di Metasploitable, non riusciamo a visualizzare la pagina come ci aspettavamo.

### **Conclusione: Log**

Infine, come ultima dimostrazione, andiamo a vedere i Log che il Firewall ha registrato per andare a verificare che la nostra regola abbia effettivamente bloccato la scansione.

Ci aspettiamo un Log che sarà composto da un tentativo di invio di pacchetti da Kali (indirizzo IP: 192.168.50.151) all'IP di Metasploitable sulla porta 80 (Indirizzo IP: 192.168.60.150:80).

Oltre a ciò, dovremmo vedere il tipo protocollo che viene bloccato, ossia TCP, con annessa data, ora, e rete nella colonna iniziale.

Inserisco immagine di seguito che spiegherà meglio quanto appena citato:

X	Dec 13 13:53:45	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45058	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:45	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45068	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:46	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45068	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:46	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45058	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:47	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45058	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:47	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45068	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:48	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45058	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:48	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45068	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:49	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45058	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:49	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45068	+ 192.168.60.150:80	TCP:S
X	<u>Dec 13 13:53:50</u>	LAN	<u>Blocca l'accesso a DVWA da Kali (1734097342)</u>	<u>i 192.168.50.151:54880</u>	<u>+ 192.168.60.150:80</u>	<u>TCP:S</u>
X	Dec 13 13:53:50	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45058	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:51	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:54880	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:52	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:54880	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:52	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45058	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:53	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:54880	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:54	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:54880	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:55	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:54880	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:56	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:54884	+ 192.168.60.150:80	TCP:S
X	Dec 13 13:53:56	LAN	Blocca l'accesso a DVWA da Kali (1734097342)	i 192.168.50.151:45058	+ 192.168.60.150:80	TCP:S