

# **M3 - Settimana 9 - Giorno 5 - RELAZIONE - 05/09/2025 - Giuseppe Gigliotti - PFSENSE**

---

**Questa esercitazione è divisa in due fasi preliminari 1 e 2 e una terza che sarà l'esercizio da svolgere autonomamente 3.**

---

Esercizio che prevede la creazione di un'ulteriore rete e l'applicazione di una policy firewall tra le due reti;

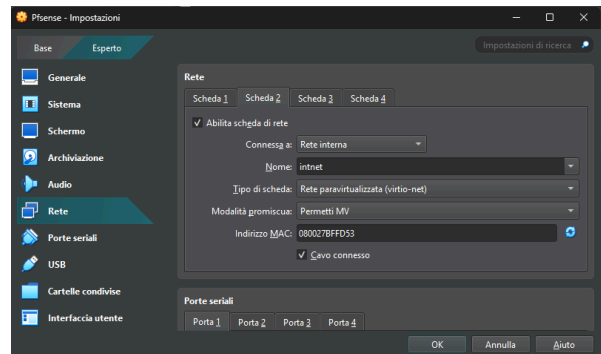
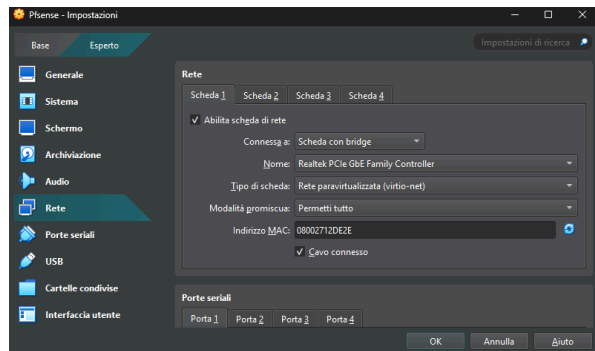
Facoltativo: approfondimenti sulla gestione dei log e del troubleshooting di rete

## **1. Installazione di Pfsense e configurazione architettura di partenza (aka architettura target)**

Per quando riguarda l'installazione e la configurazione della nuova macchina Pfsense, lasciamo solo immagini della macchina a risultato finito, in quanto essa è stata configurata durante l'esercitazione.

- Nella prima immagine vediamo la configurazione della scheda 1 in modalità "bridge" per poter utilizzare internet sulle nostre macchine.
- Nella seconda immagine vediamo la configurazione della scheda 2 in modalità "rete interna" per avere le nostre due macchine (kali e metasploitable ) nella

stessa sottorete



Il risultato finale sarà come nell'immagine sottostante!

```
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: c80962b353cdf9de8b32
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

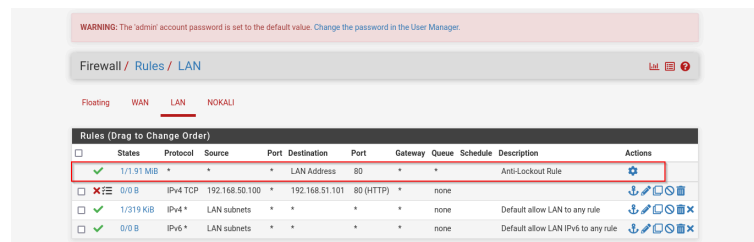
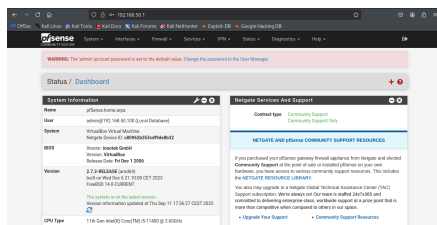
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.90/24
                                   v6/DHCP6: 2001:b07:646f:cfc1:a00:27ff:fe12:de2
e/64
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
NOKALI (opt1)  -> vtnet2      -> v4: 192.168.51.1/24

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: █
```

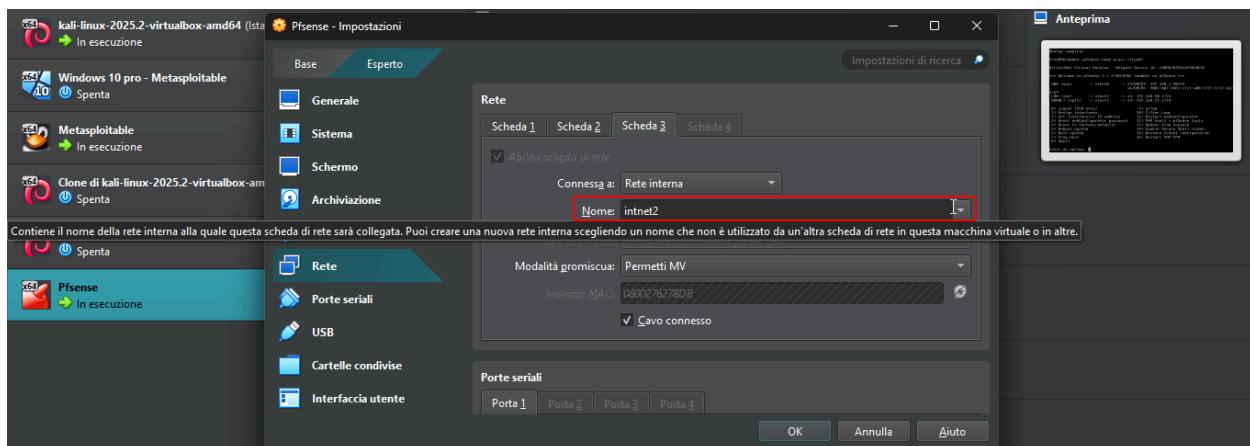
## 2. Creazione guidata di una policy firewall generica

- Configurata la pfsense ed aver assegnato l'indirizzo IP 192.168.50.1 (ci farà da default gateway), passiamo sulla kali e da browser nella barra degli indirizzi inseriamo lo stesso IP per raggiungere la pfsense.
- Inserite le credenziali di default (username :admin , password : pfsense), arriviamo sulla dashboard di pfsense.
- Configuriamo anche dal browser, andiamo su Firewall nel menù a tendina e selezioniamo su Rules
- Arrivati su Rules, andiamo su LAN, e possiamo vedere che esiste già una policy firewall generica che permette di usare qualsiasi protocollo, qualsiasi sorgente, su porta 80 che va sulla lan e non viene bloccata mai

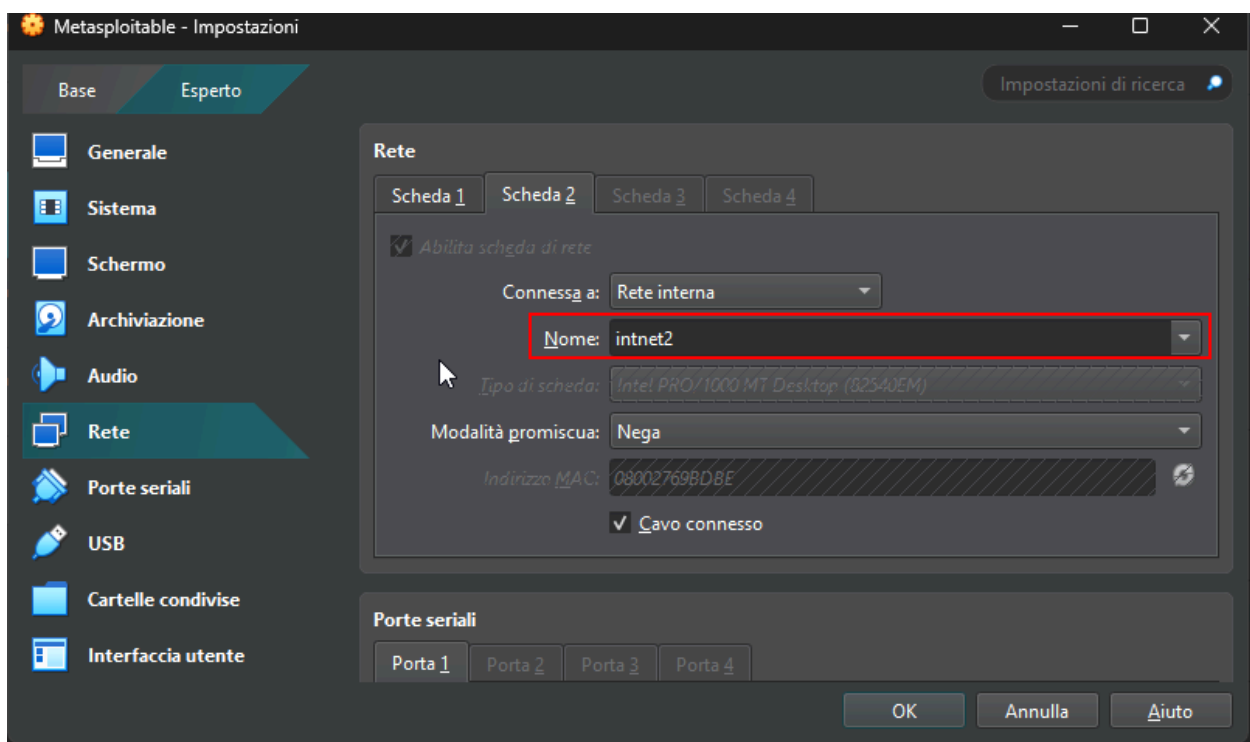


### 3. Esercizio che prevede la creazione di un'ulteriore rete e applicazione di una policy firewall tra le due reti.

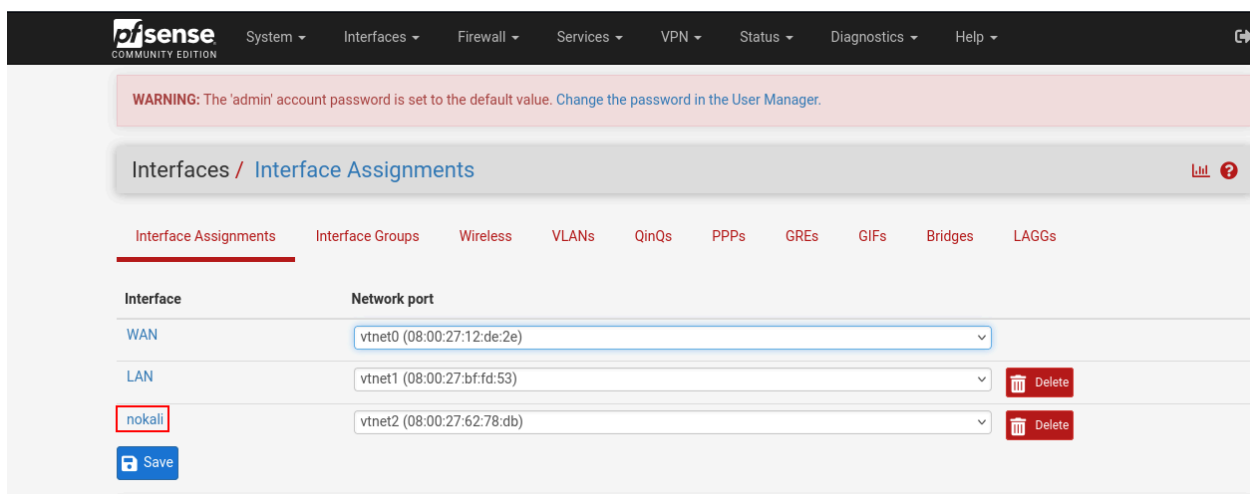
- Per fare questo andiamo sulla pfsense e la spegniamo
- Andiamo nelle impostazioni della macchina virtuale pfsense ed aggiungiamo un'altra interfaccia di rete.
- Abilitiamo la scheda 3, su rete interna, e visto che l'esercizio chiede un'ulteriore rete cambiamo il nome in intnet2



- Stessa cosa facciamo sulla metasploitable, andiamo in impostazioni di rete e abilitiamo la scheda 2 e cambiamo la rete in inet2



- Torniamo su kali sulla pagina browser di pfsense e dopo esserci riloggati (visto che per configurare la nuova scheda di rete abbiamo spento la macchina) andiamo in Interfaces e poi dal menù a tendina Assignments
- Aggiungiamo la nuova interfaccia (avrà il nome nokali). Nella configurazione mettiamo indirizzo IP statico e poi lo aggiungiamo dopo, che sarà 192.168.51.1. Alla fine possiamo salvare e tornare sulla metasploitable



- Sulla metasploitable utilizzando il comando, aggiungiamo la nuova sottorete

```
sudo vim /etc/network/interfaces # apriamo con vim il file di configurazione
# delle interfacce di metasploitable
```

```
# 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 192.168.50.101
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
gateway 192.168.50.1

auto eth1
iface eth1 inet static
address 192.168.51.101
netmask 255.255.255.0
network 192.168.51.0
broadcast 192.168.51.255
gateway 192.168.51.1

~
~
~
~
~
~
~
~
~
"/etc/network/interfaces" 24L, 529C
```

E con il comando

```
sudo /etc/init.d/restart networking # ricarichiamo il file di
# configurazione della rete
```

- Aggiungiamo una nuova regola generica sull'interfaccia nokali (per semplificarci il lavoro copiamo una regola dall'interfaccia LAN già presente su

pfsense). Ricordiamo che nella regola la source deve essere su "nokali subnet" per non avere problemi di comunicazione.

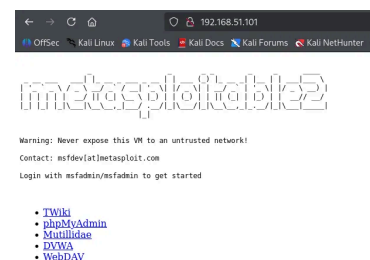
- Possiamo passare all'esercizio.

## Esercizio:

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 (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più). 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.

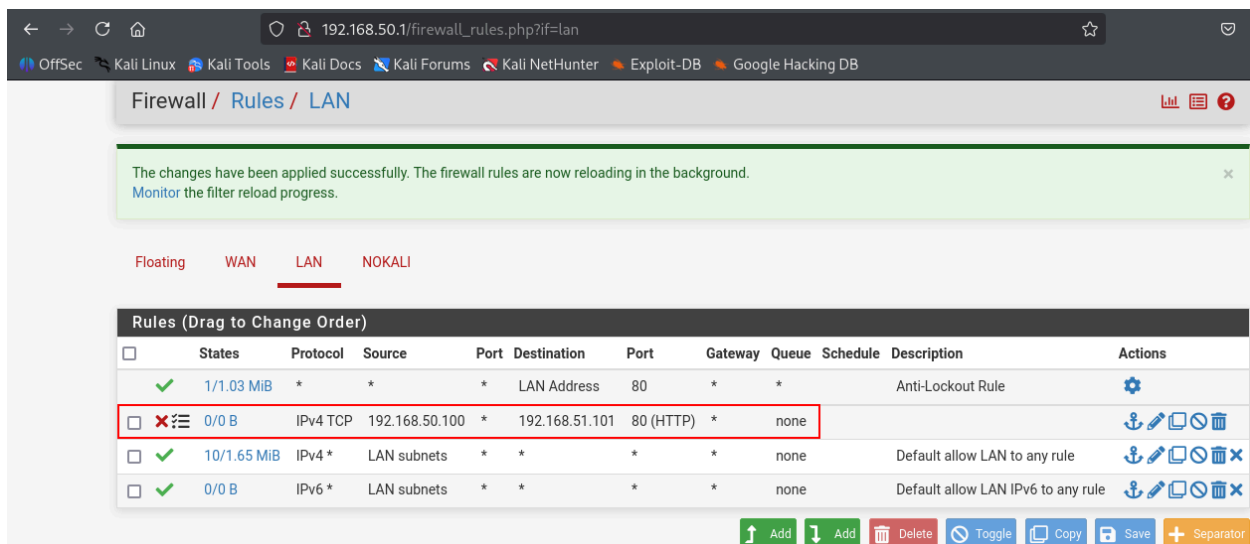
- Avendo già configurato una nuova interfaccia passiamo sulla creazione della regola
- Controlliamo che l'accesso alla DVWA da kali sia possibile

```
kali@kali: ~  
$ ping 192.168.51.101  
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data:  
64 bytes from 192.168.51.101: icmp_seq=1 ttl=64 time=1.56 ms  
64 bytes from 192.168.51.101: icmp_seq=2 ttl=64 time=0.977 ms  
64 bytes from 192.168.51.101: icmp_seq=3 ttl=64 time=1.16 ms  
64 bytes from 192.168.51.101: icmp_seq=4 ttl=64 time=0.933 ms  
^C  
--- 192.168.51.101 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3033ms  
rtt min/avg/max/mdev = 0.933/1.157/1.558/0.246 ms
```



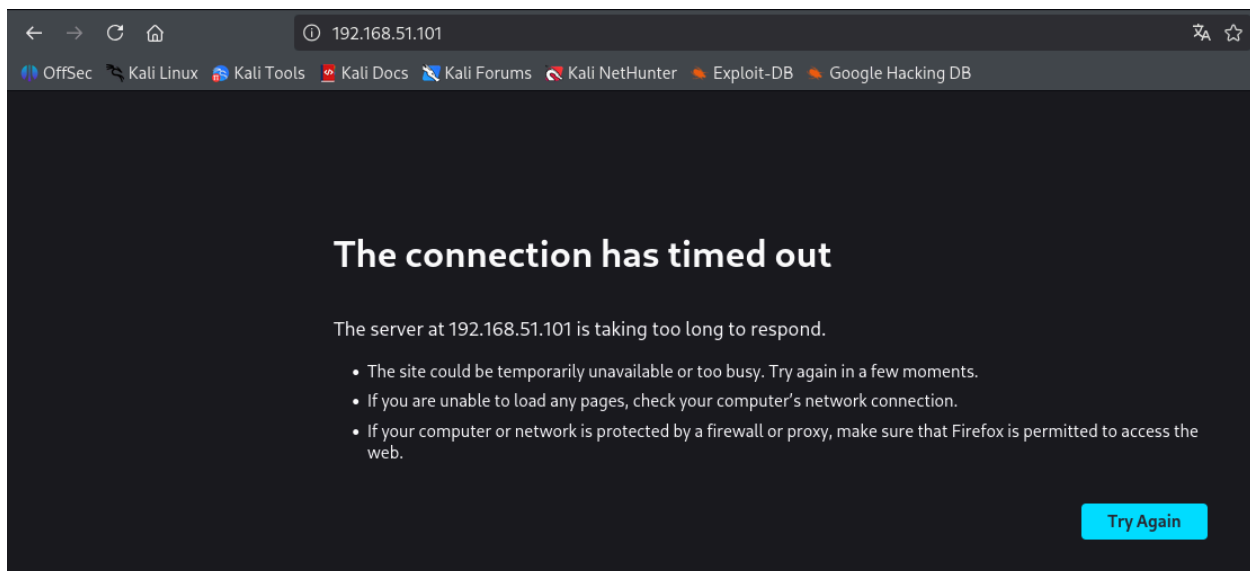
- Visto questo, andiamo su kali sulla pagina browser di pfsense e andiamo in Firewall e dal menù a tendina andiamo in Rules
- Aggiungiamo la regola, mettiamo come azione della regola Block (visto che dobbiamo bloccare l'accesso) , come source , seleziono adress o alias e inserisco l'ip della kali (192.68.50.100), mentre per destination o alias inserisco l'ip della nuova rete data alla metasploitable (192.168.51.101), inoltre essendo che la richiesta dell'esercizio è bloccare l'accesso sulla DVWA, andiamo su destination port e selezioniamo la porta 80 HTTP.
- Salviamo la configurazione e riproviamo a conneterci.

N.B. durante la configurazione della regola aggiungiamo la spunta sull'extra option Log, per poter svolgere l'esercizio facoltativo



- Appena in funzione vediamo che la nostra regola blocca la comunicazione con la metasploitable, ma solo sulla porta 80.





## FACOLTATIVO:

- Ispezionare i log del Firewall

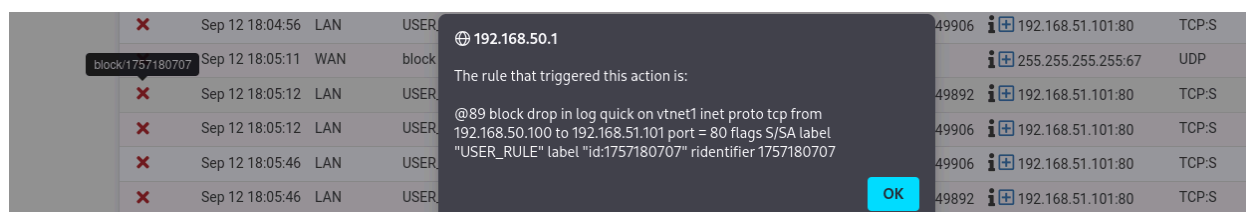
Un ulteriore test può essere controllare il traffico tramite wireshark per vedere cosa succede con l'utilizzo della nostra regola

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.50.1	TCP	66	49102 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3051675628 TSecr=374
2	0.000000594	192.168.50.1	192.168.50.100	TCP	66	[TCP ACKed unseen segment] 80 → 49102 [ACK] Seq=1 Ack=2 Win=514 Len=0
3	1.409793701	192.168.50.100	192.168.51.101	TCP	74	49092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=30275
4	1.604733366	192.168.50.100	192.168.51.101	TCP	74	49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=30275
5	2.303724296	192.168.50.100	192.168.50.1	TCP	66	49088 → 80 [ACK] Seq=1 Ack=1 Win=748 Len=0 TSval=3051677932 TSecr=15
6	2.394575489	192.168.50.1	192.168.50.100	TCP	66	[TCP ACKed unseen segment] 80 → 49088 [ACK] Seq=1 Ack=2 Win=514 Len=0
7	2.435828672	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
8	2.691697523	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
9	3.459489728	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
10	3.715485465	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
11	4.479588616	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
12	4.736248153	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
13	5.507519756	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14	5.763493690	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
15	6.527725560	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
16	6.783837595	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
17	8.544228525	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
18	8.799654816	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
19	10.239947323	192.168.50.100	192.168.50.1	TCP	66	[TCP Dup ACK 1#1] 49102 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=30
20	10.240753546	192.168.50.1	192.168.50.100	TCP	66	[TCP Dup ACK 2#1] 80 → 49102 [ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=37
21	12.543798938	192.168.50.100	192.168.50.1	TCP	66	[TCP Dup ACK 5#1] 49088 → 80 [ACK] Seq=1 Ack=1 Win=748 Len=0 TSval=30
22	12.544677023	192.168.50.1	192.168.50.100	TCP	66	[TCP Dup ACK 6#1] 80 → 49088 [ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=81
23	12.799546037	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
24	13.060195666	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0  
Ethernet II, Src: PCSSystemtec d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec bf:fd:53 (08:00:27:bf:fd:53)  
eth0: <live capture in progress> Packets: 53 Profile: Default

Possiamo avere la prova che la destinazione non ci sta rispondendo, ed il browser continua ad effettuare tentativi di connessione senza ricevere alcuna risposta.

- Infine, andando su kali sulla pagina browser di pfsense, clicchiamo su Status e dal menù a tendina andiamo su System Logs, andiamo su Firewall e dai log del Firewall abbiamo la conferma che la nostra regola, che abbiamo chiamato Block DVWA from Kali, sta effettivamente bloccando il traffico da Kali verso la DVWA (come vediamo nell'immagine)



✗	Sep 12 18:05:12	LAN	USER_RULE (1757180707)	192.168.50.100:49892	192.168.51.101:80	TCP:S
✗	Sep 12 18:05:12	LAN	USER_RULE (1757180707)	192.168.50.100:49906	192.168.51.101:80	TCP:S
✗	Sep 12 18:05:46	LAN	USER_RULE (1757180707)	192.168.50.100:49906	192.168.51.101:80	TCP:S
✗	Sep 12 18:05:46	LAN	USER_RULE (1757180707)	192.168.50.100:49892	192.168.51.101:80	TCP:S