

# ESERCIZIO PRATICO S5/L1

## 1. Settaggio del firewall pfsense

```
browser:
      http://192.168.40.1/

Press <ENTER> to continue.
*** Welcome to pfSense 2.0-RC3-cdrom (i386) on pfSense ***

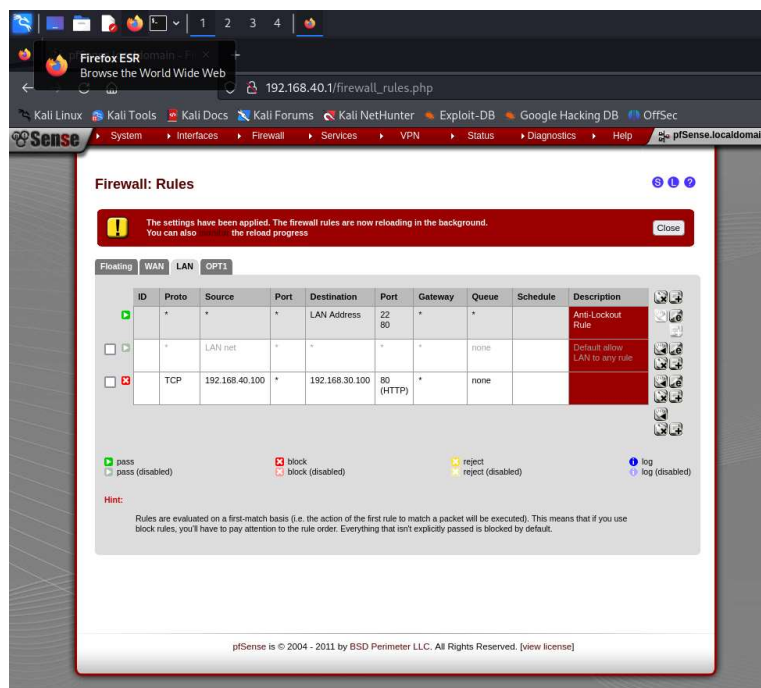
WAN (wan)          -> em0          -> 10.0.2.15 (DHCP)
LAN (lan)           -> em1          -> 192.168.40.1
OPT1 (opt1)         -> em2          -> 192.168.30.1

0) Logout (SSH only)      8) Shell
1) Assign Interfaces      9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults 12) pfSense Developer Shell
5) Reboot system          13) Upgrade from console
6) Halt system            14) Enable Secure Shell (sshd)
7) Ping host
99) Install pfSense to a hard drive, etc.

Enter an option:
Message from syslogd@pfSense at May  7 16:39:14 ...
pfSense php: /index.php: Successful webConfigurator login for user 'admin' from
192.168.40.100
```

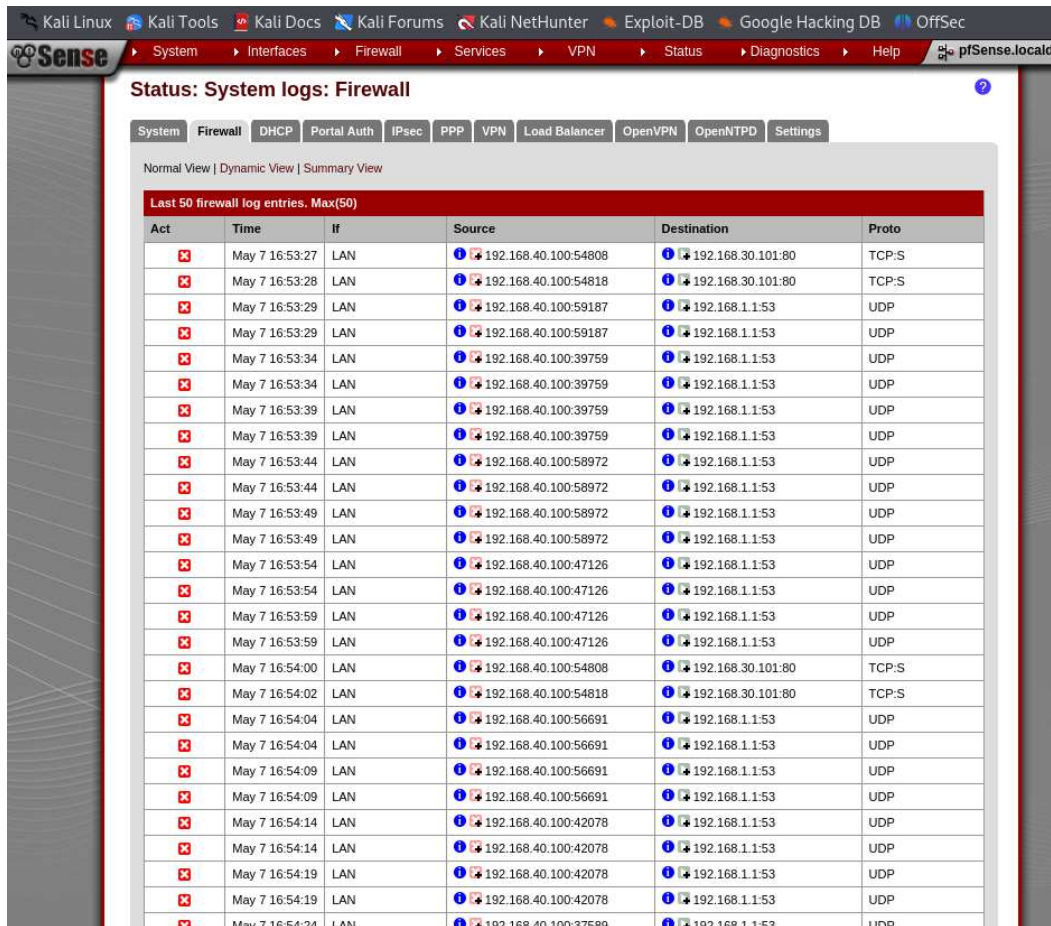
Dopo aver installato 'pfsense' su una VM abbiamo proceduto con il settaggio del firewall, impostando inizialmente **3 schede di rete** ( una 'NAT' e due 'Rete interna') e successivamente abbiamo proceduto impostando una **WAN** e due **LAN** con quest'ultime alle quali abbiamo impostato gli indirizzi **IP di gateway** relativamente di **KALI** e **METASPLOITABLE**.

## 2. Impostazioni regole pfsense



Successivamente abbiamo proceduto ad impostare le **regole** sul **firewall**, in particolare abbiamo bloccato la trasmissione dei dati che partivano dall'**indirizzo IP di Metasploitable** verso l'**indirizzo IP di Kali**.

### 3. Verifica del funzionamento del firewall tramite i log di pfsense

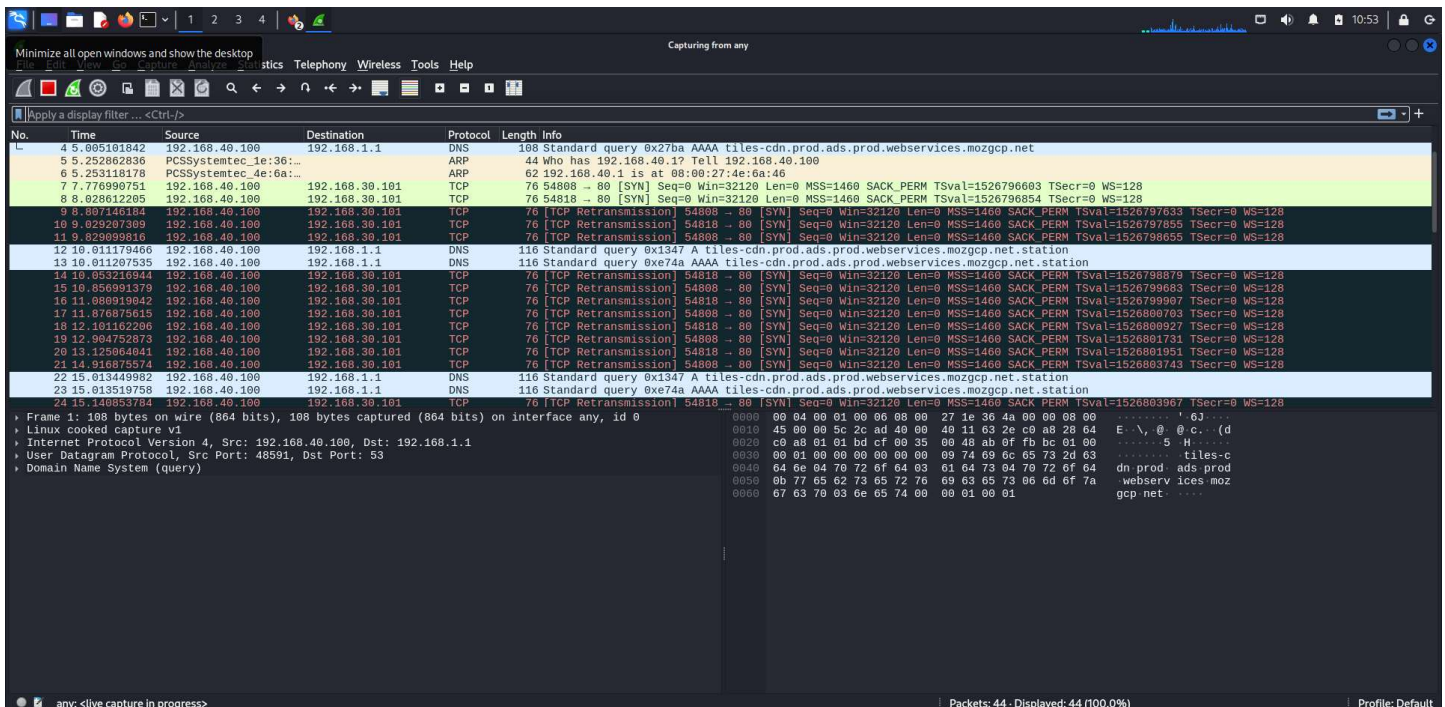


The screenshot shows the pfSense web interface with the 'Status: System logs: Firewall' page. The 'System' tab is selected, and the 'Firewall' sub-tab is active. The log shows a series of blocked connections from 192.168.40.100 to 192.168.1.153. The connections are blocked for both TCP and UDP protocols. The log entries are as follows:

Act	Time	If	Source	Destination	Proto
[X]	May 7 16:53:27	LAN	192.168.40.100:54808	192.168.30.101:80	TCP:S
[X]	May 7 16:53:28	LAN	192.168.40.100:54818	192.168.30.101:80	TCP:S
[X]	May 7 16:53:29	LAN	192.168.40.100:59187	192.168.1.1:53	UDP
[X]	May 7 16:53:29	LAN	192.168.40.100:59187	192.168.1.1:53	UDP
[X]	May 7 16:53:34	LAN	192.168.40.100:39759	192.168.1.1:53	UDP
[X]	May 7 16:53:34	LAN	192.168.40.100:39759	192.168.1.1:53	UDP
[X]	May 7 16:53:39	LAN	192.168.40.100:39759	192.168.1.1:53	UDP
[X]	May 7 16:53:39	LAN	192.168.40.100:39759	192.168.1.1:53	UDP
[X]	May 7 16:53:44	LAN	192.168.40.100:58972	192.168.1.1:53	UDP
[X]	May 7 16:53:44	LAN	192.168.40.100:58972	192.168.1.1:53	UDP
[X]	May 7 16:53:49	LAN	192.168.40.100:58972	192.168.1.1:53	UDP
[X]	May 7 16:53:49	LAN	192.168.40.100:58972	192.168.1.1:53	UDP
[X]	May 7 16:53:54	LAN	192.168.40.100:47126	192.168.1.1:53	UDP
[X]	May 7 16:53:54	LAN	192.168.40.100:47126	192.168.1.1:53	UDP
[X]	May 7 16:53:59	LAN	192.168.40.100:47126	192.168.1.1:53	UDP
[X]	May 7 16:53:59	LAN	192.168.40.100:47126	192.168.1.1:53	UDP
[X]	May 7 16:54:00	LAN	192.168.40.100:54808	192.168.30.101:80	TCP:S
[X]	May 7 16:54:02	LAN	192.168.40.100:54818	192.168.30.101:80	TCP:S
[X]	May 7 16:54:04	LAN	192.168.40.100:56691	192.168.1.1:53	UDP
[X]	May 7 16:54:04	LAN	192.168.40.100:56691	192.168.1.1:53	UDP
[X]	May 7 16:54:09	LAN	192.168.40.100:56691	192.168.1.1:53	UDP
[X]	May 7 16:54:09	LAN	192.168.40.100:56691	192.168.1.1:53	UDP
[X]	May 7 16:54:14	LAN	192.168.40.100:42078	192.168.1.1:53	UDP
[X]	May 7 16:54:14	LAN	192.168.40.100:42078	192.168.1.1:53	UDP
[X]	May 7 16:54:19	LAN	192.168.40.100:42078	192.168.1.1:53	UDP
[X]	May 7 16:54:19	LAN	192.168.40.100:42078	192.168.1.1:53	UDP
[X]	May 7 16:54:24	LAN	192.168.40.100:37589	192.168.1.1:53	UDP

Abbiamo poi proceduto a verificare l'effettivo funzionamento del **firewall** andando a visionare i **log** di pfsense e come previsto la connessione verso l'indirizzo IP di Metasploitable risulta **bloccata** sia per i protocolli **TCP** che per i protocolli **UDP**.

### 4. Verifica del funzionamento del firewall tramite Wireshark



The screenshot shows a Wireshark network traffic capture. The 'Filter' bar is set to 'ip.addr == 192.168.40.100'. The packet list shows several DNS and TCP/UDP packets. The packet details pane shows the 'Standard query' packet (116) and the 'Standard query response' packet (117). The packet bytes pane shows the raw data of the packets. The status bar at the bottom indicates 'Packets: 44 - Displayed: 44 (100.0%)'.

No.	Time	Source	Destination	Protocol	Length	Info
4	5.005181842	192.168.40.100	192.168.1.1	DNS	108	Standard query 0x27ba AAAA tiles-cdn.prod.ads.prod.webservices.mozgcp.net
5	5.252862836	PCSSystemtec.de:6a:...	192.168.40.100	ARP	44	Who has 192.168.40.1? Is at 08:00:27:4e:6a:46
6	5.253118178	PCSSystemtec.de:6a:...	192.168.30.101	TCP	76	54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526796063 TSecr=0 WS=128
7	7.776990751	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526797633 TSecr=0 WS=128
8	8.028612205	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526797633 TSecr=0 WS=128
9	8.097146184	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526797633 TSecr=0 WS=128
10	9.029207309	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526797633 TSecr=0 WS=128
11	9.829099816	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526797633 TSecr=0 WS=128
12	10.011179466	192.168.40.100	192.168.1.1	DNS	116	Standard query 0x1347 A tiles-cdn.prod.ads.prod.webservices.mozgcp.net.station
13	10.011207535	192.168.40.100	192.168.1.1	DNS	116	Standard query 0xe74a AAAA tiles-cdn.prod.ads.prod.webservices.mozgcp.net.station
14	10.053210944	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526798079 TSecr=0 WS=128
15	10.050991379	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526798079 TSecr=0 WS=128
16	11.080919842	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526799907 TSecr=0 WS=128
17	11.076875615	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526800703 TSecr=0 WS=128
18	12.101102296	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526800927 TSecr=0 WS=128
19	12.904752873	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526801731 TSecr=0 WS=128
20	13.125060401	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526801951 TSecr=0 WS=128
21	14.916075574	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526803743 TSecr=0 WS=128
22	15.013449982	192.168.40.100	192.168.1.1	DNS	116	Standard query 0x1347 A tiles-cdn.prod.ads.prod.webservices.mozgcp.net.station
23	15.013519758	192.168.40.100	192.168.1.1	DNS	116	Standard query 0xe74a AAAA tiles-cdn.prod.ads.prod.webservices.mozgcp.net.station
24	15.140837424	192.168.40.100	192.168.30.101	TCP	76	[TCP Retransmission] 54808 -> 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1526803967 TSecr=0 WS=128

Come ulteriore verifica abbiamo proceduto con un'analisi dei pacchetti tramite il software **Wireshark** e anche in questo caso la connessione verso l'indirizzo IP di Metasploitable risulta **bloccata** sia per i protocolli **TCP** che per i protocolli **UDP**.