

Configurazione di **pfSense** con tre interfacce.

```
Enter an option:

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: cc71555b1997f71386dd

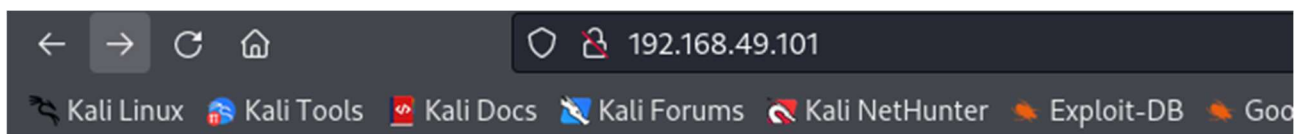
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.49.1/24

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: █
```

Inizialmente, senza alcuna regola di **blocco firewall** specifica, riesco ad accedere alla DVWA (porta 80 HTTP) di Metasploitable (IP: 192.168.49.101) da Kali Linux (IP: 192.168.50.100).



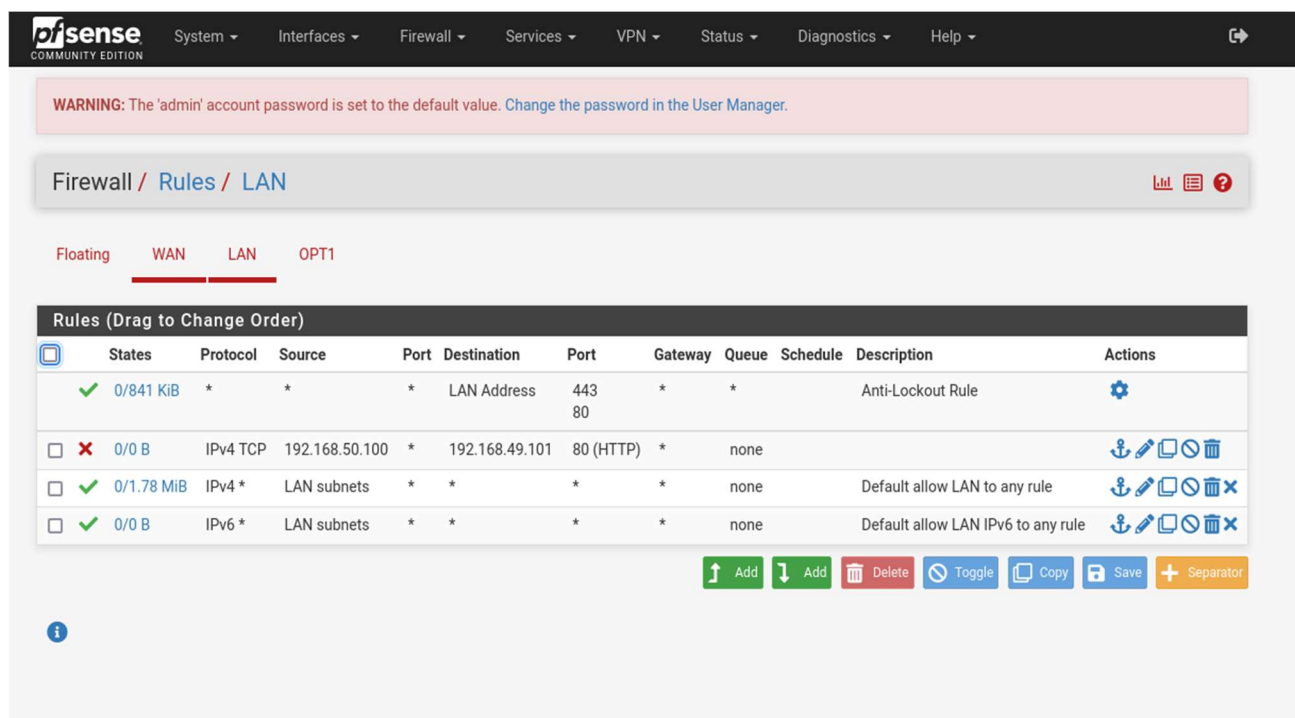
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Imposto una regola di blocco firewall, con **sorgente** Kali Linux e **destinazione** porta 80 di Metasploitable.



WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / LAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

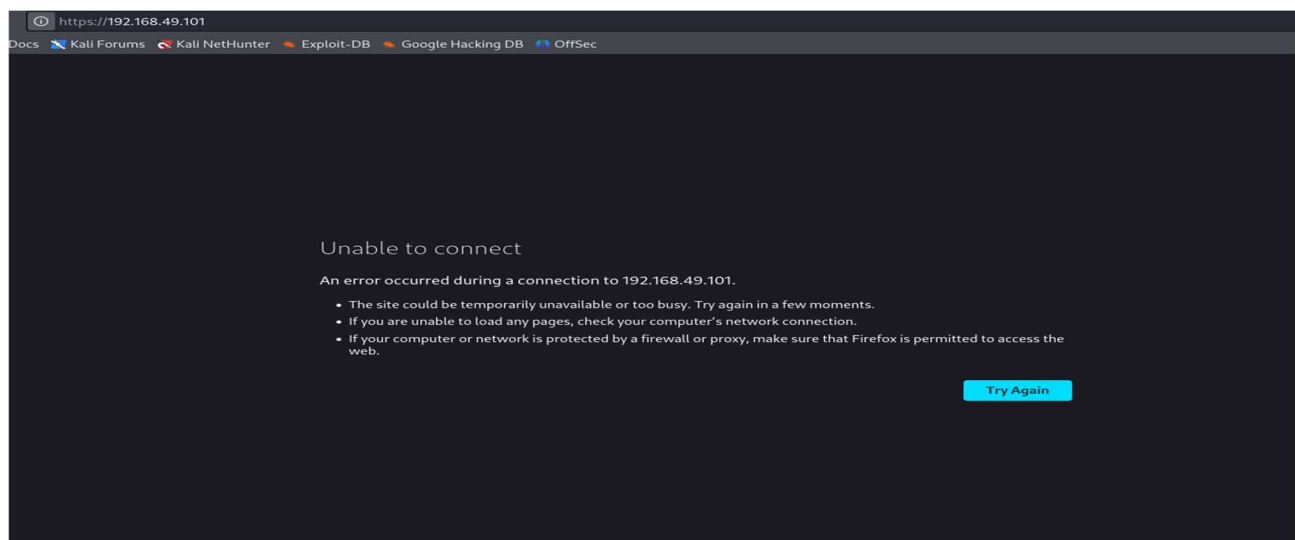
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/841 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✗ 0/0 B	IPv4 TCP	192.168.50.100	*	192.168.49.101	80 (HTTP)	*	none			
✓ 0/1.78 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Con l'opzione **block** viene bloccato il caricamento della pagina web, con tentativi continui di stabilire una connessione (come si può notare analizzando i pacchetti su Wireshark).

No.	Time	Source	Destination	Protocol	Length	Info
3828	3828.7421208...	192.168.50.100	192.168.50.1	TCP	66	43902 → 443 [ACK] Seq=15965 Ack=795403 Win=253696 Len=0 TSval=2994446869 TSecr=2665157458
3829	3828.7422317...	192.168.50.1	192.168.50.100	TCP	2962	443 → 43902 [ACK] Seq=795403 Ack=15965 Win=65792 Len=2896 TSval=2665157458 TSecr=2994446679 [TCP segment of a reassemb
3830	3828.7422427...	192.168.50.100	192.168.50.1	TCP	66	43902 → 443 [ACK] Seq=15965 Ack=798299 Win=251776 Len=0 TSval=2994446869 TSecr=2665157458
3831	3828.7423986...	192.168.50.1	192.168.50.100	TLSv1.3	4319	Application Data
3832	3828.7424081...	192.168.50.100	192.168.50.1	TCP	66	43902 → 443 [ACK] Seq=15965 Ack=802552 Win=253696 Len=0 TSval=2994446869 TSecr=2665157458
3833	3841.4447882...	192.168.50.100	192.168.49.101	TCP	74	42030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978494426 TSecr=0 WS=128
3834	3841.6959699...	192.168.50.100	192.168.49.101	TCP	74	42042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978494677 TSecr=0 WS=128
3835	3842.4536319...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978495435 TSecr=0 WS=128
3836	3842.7080419...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978495690 TSecr=0 WS=128
3837	3843.4767176...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978496458 TSecr=0 WS=128
3838	3843.7328550...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978496714 TSecr=0 WS=128
3839	3844.4969821...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978497478 TSecr=0 WS=128
3840	3844.7526542...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978497734 TSecr=0 WS=128
3841	3845.5247937...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978498566 TSecr=0 WS=128
3842	3845.7762689...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978498758 TSecr=0 WS=128
3843	3846.5470813...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978499529 TSecr=0 WS=128
3844	3846.8046731...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978499786 TSecr=0 WS=128
3845	3848.5642656...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978501546 TSecr=0 WS=128
3846	3848.8202746...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978501802 TSecr=0 WS=128
3847	3852.7561233...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978505738 TSecr=0 WS=128
3848	3853.0081329...	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 42042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2978505990 TSecr=0 WS=128

Con l'opzione **refuse** viene invece rifiutata e interrotta immediatamente la connessione.



https://192.168.49.101

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Unable to connect

An error occurred during a connection to 192.168.49.101.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

L'utilizzo dell'opzione block o refuse dipende dal comportamento desiderato.

Notiamo invece come il ping (**ICMP**) funzioni ancora, poiché abbiamo bloccato solo la porta 80 **TCP**.

```
(kali㉿kali)-[~]  
$ ping 192.168.49.101  
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.  
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=7.04 ms  
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=0.949 ms  
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=0.656 ms  
64 bytes from 192.168.49.101: icmp_seq=4 ttl=63 time=1.11 ms  
64 bytes from 192.168.49.101: icmp_seq=5 ttl=63 time=1.51 ms  
64 bytes from 192.168.49.101: icmp_seq=6 ttl=63 time=1.08 ms  
^C  
— 192.168.49.101 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5066ms  
rtt min/avg/max/mdev = 0.656/2.058/7.042/2.243 ms
```