

```

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

WAN (wan)      -> em0      -> v4: 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:
Message from syslogd@pfSense at Feb 14 19:00:55 ...
php-fpm[398]: /index.php: Successful login for user 'admin' from: 192.168.50.100
(Local Database)

```

pfSense.home.arpa - Fire x Problem loading page x +

https://192.168.50.1/firewall\_rules.php?if=lan

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

Firewall / Rules / LAN

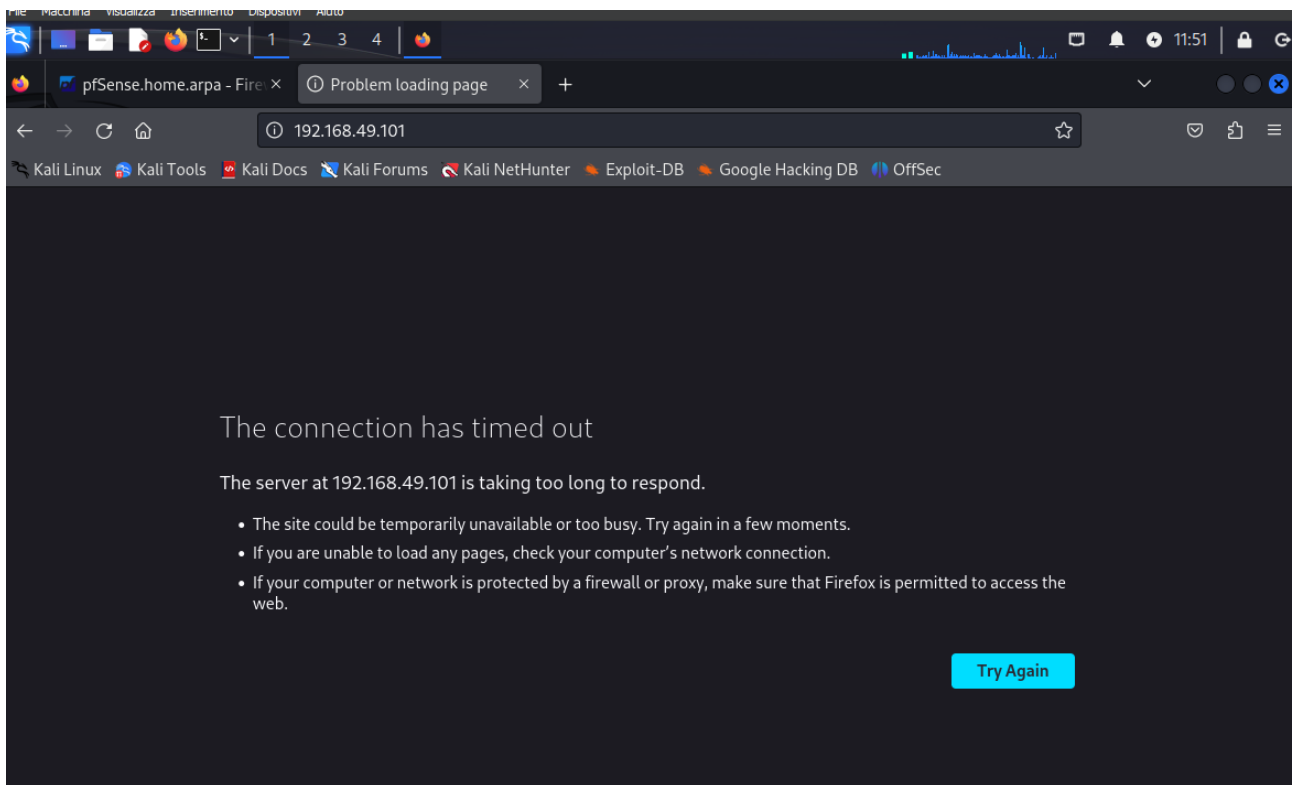
The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor the filter reload progress.](#)

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/886 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 ICMP any	*	*	192.168.49.101	*	*	none			
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	*	*	192.168.49.101	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 1/271 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator



## Report

Questo esercizio richiede l'inserimento di una regola nel firewall che deve bloccare l'accesso al DVWA tramite la macchina virtuale metasploitable.

Come prima ho installato e configurato pfsense (img 1).

Successivamente nelle Instances ho aggiunto la seconda rete (metasploitable) chiamata OPT1

Dopodiché ho aggiunto due regole: la prima consiste nel bloccare l'accesso dell'indirizzo IP di meta attraverso la porta 80 la seconda ne blocca il ping

Infine ho verificato il funzionamento delle regole