

# Configurazione Firewall su pfSense per Isolamento Metasploitable2

L'obiettivo dell'esercizio è stato quello di configurare un ambiente di rete segmentato tramite pfSense, in modo da bloccare l'accesso alla piattaforma DVWA presente sulla macchina Metasploitable2 quando la connessione proviene dalla macchina Kali Linux. Questo risultato è stato ottenuto creando una terza interfaccia di rete su pfSense, configurandola e applicando una regola firewall mirata. Pur impedendo l'accesso HTTP alla Metasploitable, era necessario che il traffico ICMP (ping) rimanesse consentito, così da verificare che il blocco riguardasse solo il servizio web e non la raggiungibilità generale.

## Struttura della Rete

Nel sistema pfSense sono state configurate tre interfacce:

**WAN** – Rete esterna

**LAN** – Rete Kali Linux

**METASPOIT** – Rete Metasploitable2

Durante l'avvio della macchina di pfSense è stato possibile verificare la loro corretta assegnazione e gli indirizzi IP associati.

```
(Local Database)

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

VirtualBox Virtual Machine - Netgate Device ID: c4b271b1b63c682a735d

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

WAN (wan)      -> vtne0      -> v4/DHCP4: 192.168.1.112/24
LAN (lan)      -> vtne1      -> v4: 192.168.50.1/24
METASPLOIT (opt1) -> em0      -> v4: 192.168.60.1/24

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: [
```

La macchina Kali è stata collegata alla rete LAN mentre Metasploitable è stata collegata alla OPT1(METASPLOIT), garantendo così una separazione fisica e logica tra i due host vulnerabile e attaccante.

## Configurazione WebGUI di pfSense

Accedendo alla WebGUI di pfSense dalla Kali, è stata attivata l'interfaccia OPT1 e configurata con un indirizzo IP statico coerente con la rete dedicata a Metasploitable2. Successivamente sono state analizzate le regole firewall predefinite di ciascuna interfaccia.

### Regole Firewall – WAN

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	X 0/718 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	X 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

La WAN mantiene le sue regole standard e non richiede modifiche poiché il traffico che ci interessa filtrare è quello proveniente dalla LAN verso OPT1.

## Regole Firewall – LAN

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 14/246 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✗ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Sulla LAN è presente la regola che permette il traffico in uscita verso qualsiasi destinazione. Questa regola permette inizialmente alla Kali di accedere alla DVWA sulla Metasploitable.

## Regole Firewall – OPT1

No rules are currently defined for this interface.  
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

## Test prima dell'applicazione della regola

Prima di introdurre il blocco, ho verificato che la Kali fosse in grado di:

## Accedere alla pagina DVWA esposta dalla Metasploitable2

The screenshot shows a Firefox browser window with the address bar set to 192.168.60.10. The title bar says "Metasploitable2 - Linux". The page content is a login form for DVWA. At the top left, there is a warning message: "Warning: Never expose this VM to an untrusted network!". Below it, contact information: "Contact: msfdev[at]metasploit.com" and "Login with msfadmin/msfadmin to get started". A navigation menu on the right lists: TWiki, phpMyAdmin, Mutilidae, DVWA, and WebDAV.

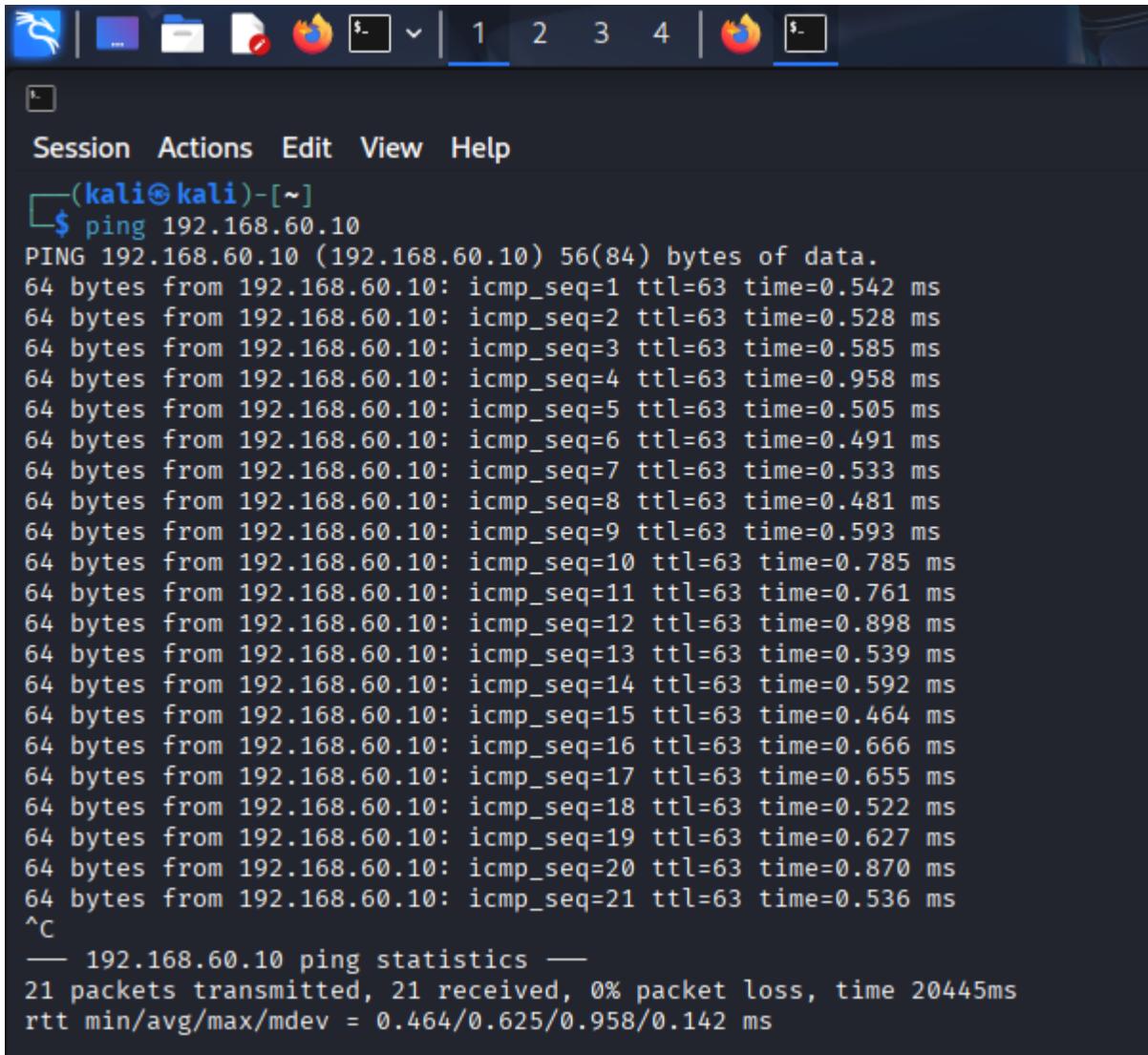
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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

## Eseguire un ping verso l'indirizzo IP della Metasploitable



The screenshot shows a terminal window titled '(kali㉿kali)-[~]' with a session number '1'. The user has run the command '\$ ping 192.168.60.10'. The output displays 21 successful ICMP echo requests sent to the target host at 192.168.60.10, with round-trip times ranging from approximately 0.464 ms to 0.958 ms. After the ping test, the user types '^C' to stop the process. The terminal then displays statistics for the ping test, showing 21 packets transmitted, 21 received, 0% packet loss, and a total time of 20445ms.

```
$ ping 192.168.60.10
PING 192.168.60.10 (192.168.60.10) 56(84) bytes of data.
64 bytes from 192.168.60.10: icmp_seq=1 ttl=63 time=0.542 ms
64 bytes from 192.168.60.10: icmp_seq=2 ttl=63 time=0.528 ms
64 bytes from 192.168.60.10: icmp_seq=3 ttl=63 time=0.585 ms
64 bytes from 192.168.60.10: icmp_seq=4 ttl=63 time=0.958 ms
64 bytes from 192.168.60.10: icmp_seq=5 ttl=63 time=0.505 ms
64 bytes from 192.168.60.10: icmp_seq=6 ttl=63 time=0.491 ms
64 bytes from 192.168.60.10: icmp_seq=7 ttl=63 time=0.533 ms
64 bytes from 192.168.60.10: icmp_seq=8 ttl=63 time=0.481 ms
64 bytes from 192.168.60.10: icmp_seq=9 ttl=63 time=0.593 ms
64 bytes from 192.168.60.10: icmp_seq=10 ttl=63 time=0.785 ms
64 bytes from 192.168.60.10: icmp_seq=11 ttl=63 time=0.761 ms
64 bytes from 192.168.60.10: icmp_seq=12 ttl=63 time=0.898 ms
64 bytes from 192.168.60.10: icmp_seq=13 ttl=63 time=0.539 ms
64 bytes from 192.168.60.10: icmp_seq=14 ttl=63 time=0.592 ms
64 bytes from 192.168.60.10: icmp_seq=15 ttl=63 time=0.464 ms
64 bytes from 192.168.60.10: icmp_seq=16 ttl=63 time=0.666 ms
64 bytes from 192.168.60.10: icmp_seq=17 ttl=63 time=0.655 ms
64 bytes from 192.168.60.10: icmp_seq=18 ttl=63 time=0.522 ms
64 bytes from 192.168.60.10: icmp_seq=19 ttl=63 time=0.627 ms
64 bytes from 192.168.60.10: icmp_seq=20 ttl=63 time=0.870 ms
64 bytes from 192.168.60.10: icmp_seq=21 ttl=63 time=0.536 ms
^C
--- 192.168.60.10 ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20445ms
rtt min/avg/max/mdev = 0.464/0.625/0.958/0.142 ms
```

Questi test dimostrano che inizialmente non esiste alcun filtraggio tra le due macchine e che la Kali può liberamente comunicare con Metasploitable.

## Creazione della regola di blocco

Per impedire l'accesso HTTP, ho inserito una regola firewall sull'interfaccia OPT1 che:

- Blocca il traffico TCP
- Proveniente dalla rete LAN
- Diretto alla macchina Metasploitable2
- Sulla porta 80 (HTTP)

La regola è stata posizionata in testa alla lista, così da essere applicata prima delle regole generiche di allow.

Dopo aver salvato le modifiche, pfSense ha applicato il nuovo comportamento immediatamente.

The screenshot shows the pfSense firewall configuration interface. At the top, the URL is 192.168.1.112/firewall\_rules\_edit.php?d=0. The main window is titled 'Edit Firewall Rule' and contains fields for Action (Block), Disabled (unchecked), Interface (LAN), Address Family (IPv4), and Protocol (TCP). Below these are sections for Source and Destination, both set to 192.168.50.151 and 192.168.60.10 respectively. A note about source port range is present. The bottom part shows the 'Rules' table with four entries:

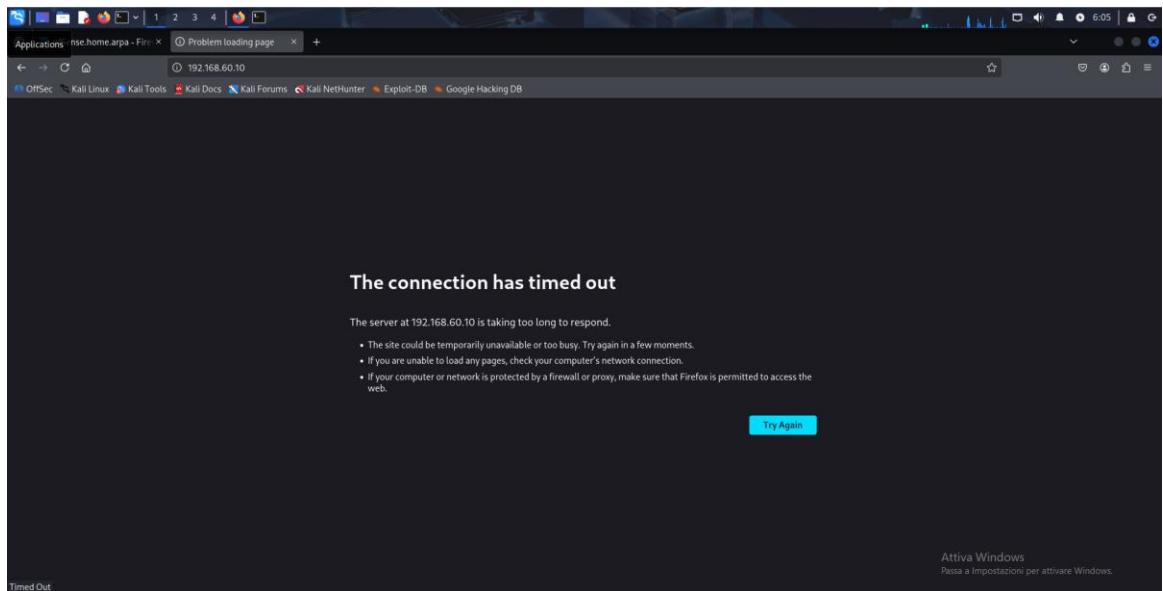
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 0/3 KiB	IPv4 TCP	192.168.50.151	*	192.168.60.10	80 (HTTP)	*	none			
✓ 4/1.51 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

A red oval highlights the first two rows of the table, specifically the columns for 'Source', 'Protocol', 'Destination', and 'Port'. The last two rows are also highlighted with a red oval.

## Test dopo l'applicazione della regola

Dopo l'inserimento della regola firewall, ho eseguito nuovamente i test:

Il browser della Kali non riesce più ad accedere alla DVWA, ricevendo timeout o connection refused.



Il ping verso Metasploitable continua a funzionare, confermando che è stato bloccato solo il traffico HTTP.

```
(kali㉿kali)-[~]
$ ping 192.168.60.10
PING 192.168.60.10 (192.168.60.10) 56(84) bytes of data.
64 bytes from 192.168.60.10: icmp_seq=1 ttl=63 time=8.21 ms
64 bytes from 192.168.60.10: icmp_seq=2 ttl=63 time=0.512 ms
^[[B^[[B^[[B^[[B^[[B64 bytes from 192.168.60.10: icmp_seq=3 ttl=63 time=1.14 ms
64 bytes from 192.168.60.10: icmp_seq=4 ttl=63 time=0.466 ms
64 bytes from 192.168.60.10: icmp_seq=5 ttl=63 time=0.438 ms
64 bytes from 192.168.60.10: icmp_seq=6 ttl=63 time=0.932 ms
64 bytes from 192.168.60.10: icmp_seq=7 ttl=63 time=0.419 ms
64 bytes from 192.168.60.10: icmp_seq=8 ttl=63 time=0.491 ms
64 bytes from 192.168.60.10: icmp_seq=9 ttl=63 time=0.431 ms
64 bytes from 192.168.60.10: icmp_seq=10 ttl=63 time=0.455 ms
64 bytes from 192.168.60.10: icmp_seq=11 ttl=63 time=0.442 ms
64 bytes from 192.168.60.10: icmp_seq=12 ttl=63 time=0.482 ms
64 bytes from 192.168.60.10: icmp_seq=13 ttl=63 time=0.485 ms
^C
--- 192.168.60.10 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12192ms
rtt min/avg/max/mdev = 0.419/1.145/8.208/2.049 ms
```

Questi risultati confermano che il firewall è stato configurato correttamente e in modo granulare.

