

Configurazione di una Regola Firewall in pfSense

Catalin Ardelean Pop

Obiettivo del documento

Configurare su pfSense una regola firewall che blocchi l'accesso da Kali Linux alla DVWA (in esecuzione su Metasploitable2), impedendo anche eventuali scansioni mirate al servizio HTTP. La configurazione richiede che Kali e Metasploitable si trovino su **reti distinte** tramite l'aggiunta di un'interfaccia OPT1 su pfSense.

1 Topologia della Rete

La rete è composta da tre macchine virtuali:

- **pfSense**: router e firewall con tre interfacce (WAN, LAN, OPT1).
- **Kali Linux**: collegata alla rete **LAN** di pfSense.
- **Metasploitable2**: collegata alla rete **OPT1** di pfSense.

2 Configurazione interfacce pfSense

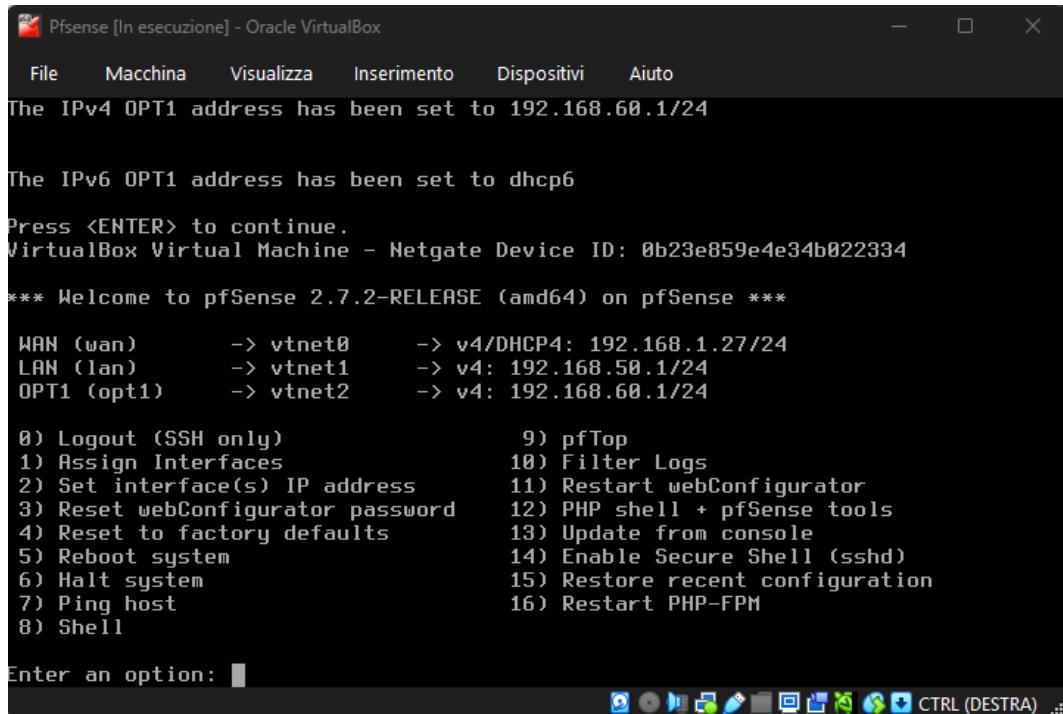


Figura 1: Interfacce e indirizzi IP configurati sulla VM pfSense.

3 Screenshot del Pannello di Controllo di pfSense

3.1 Firewall Rules — WAN

The screenshot shows the pfSense Firewall Rules configuration for the WAN interface. The interface has tabs for Floating, WAN, LAN, and OPT1, with WAN selected. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title "Firewall / Rules / WAN" is displayed. The main area shows a table of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/395 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

A yellow box below the table indicates: "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." At the bottom are standard toolbar buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Figura 2: Regole firewall configurate sulla WAN.

3.2 Firewall Rules — LAN

The screenshot shows the pfSense Firewall Rules configuration for the LAN interface. The interface has tabs for Floating, WAN, LAN, and OPT1, with LAN selected. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title "Firewall / Rules / LAN" is displayed. The main area shows a table of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
5/64 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
31/140 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	

At the bottom are standard toolbar buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Figura 3: Regole firewall configurate sulla LAN.

3.3 Firewall Rules — OPT1

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	IPv4 *	*	*	*	*	*	none			

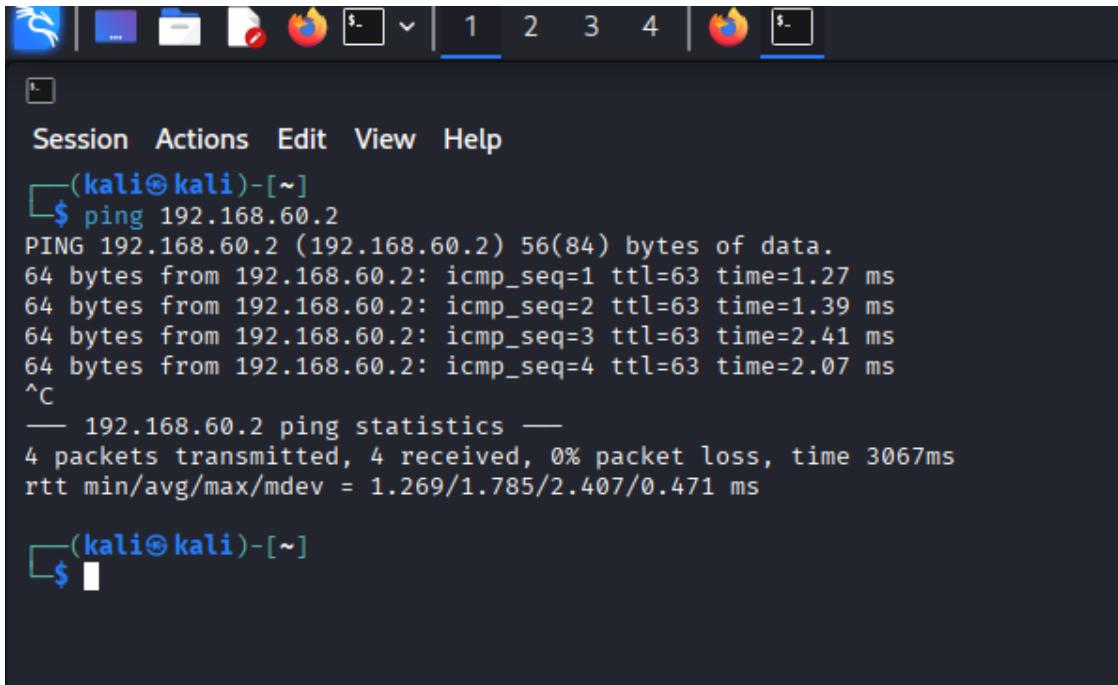
Figura 4: Regole firewall configurate sulla OPT1.

4 Accesso alla DVWA prima della Regola

4.1 Kali che visualizza la pagina DVWA

Figura 5: Accesso alla pagina DVWA correttamente funzionante prima dell'applicazione della regola.

4.2 Ping prima della regola



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a menu bar with icons for file, terminal, and browser. Below the menu, the terminal title is '(kali㉿kali)-[~]'. The user has run the command '\$ ping 192.168.60.2' and received a response showing four successful PING requests and their times. After the responses, the user types '^C' to stop the ping. Then, they type 'ping statistics' and see the summary: 4 packets transmitted, 4 received, 0% packet loss, time 3067ms, and rtt min/avg/max/mdev values.

```
$ ping 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=63 time=1.39 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=63 time=2.41 ms
64 bytes from 192.168.60.2: icmp_seq=4 ttl=63 time=2.07 ms
^C
--- 192.168.60.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 1.269/1.785/2.407/0.471 ms

$
```

Figura 6: Kali riesce a pingare Metasploitable prima dell'applicazione della regola.

5 Accesso alla DVWA dopo l'Aggiunta della Regola Firewall

5.1 Kali che non riesce più a caricare la DVWA

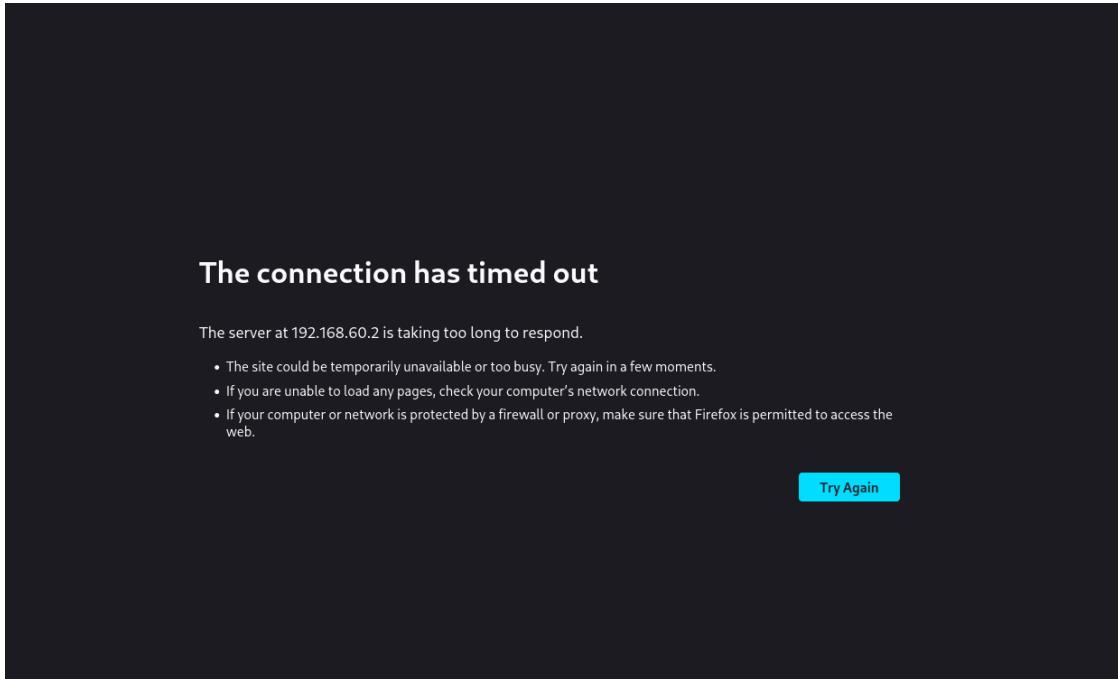


Figura 7: L'accesso alla DVWA è bloccato dalla nuova regola firewall applicata sulla LAN.

5.2 Ping dopo la regola

```
(kali㉿kali)-[~]
└─$ ping 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=63 time=1.43 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=63 time=1.21 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=63 time=1.33 ms
64 bytes from 192.168.60.2: icmp_seq=4 ttl=63 time=1.73 ms
64 bytes from 192.168.60.2: icmp_seq=5 ttl=63 time=1.30 ms
^C
--- 192.168.60.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 1.208/1.399/1.733/0.180 ms

(kali㉿kali)-[~]
└─$
```

Figura 8: Il ping continua a funzionare perché ICMP non è stato filtrato.

6 Descrizione della Regola Firewall

La regola è stata creata **sulla LAN** (interfaccia in cui è collegata Kali) con l'obiettivo di bloccare le richieste HTTP originate da Kali verso la Metasploitable2. Bloccare il traffico alla sorgente è la pratica raccomandata: filtri posti sull'interfaccia di origine impediscono che il traffico esca verso la rete di destinazione.

Parametri della regola
<ul style="list-style-type: none"> Interface: LAN Action: Block Protocol: TCP Source: IP Kali (192.168.50.151/24) Destination: IP Metasploitable (192.168.60.20/24) Port: 80

Comportamento ottenuto

- Le richieste HTTP (porta 80) dalla Kali verso Metasploitable sono bloccate: la pagina DVWA non risulta più raggiungibile dalla Kali.
- Il ping (ICMP) continua a funzionare perché non è stato filtrato dalla regola (ICMP lasciato consentito per scopi di verifica connettività).

Limiti e considerazioni sullo scanning

La regola blocca efficacemente l'accesso a HTTP (porta 80). Tuttavia:

- Lo scanning non si limita alla porta 80:** uno scanner come `nmap` può scansionare altre porte o usare tecniche TCP (SYN scan, ACK scan, ecc.). Se l'obiettivo è impedire qualsiasi tipo di scansione da Kali verso Metasploitable, è necessario:

- bloccare l'intero traffico TCP/UDP dalla fonte (LAN) verso la destinazione (Metasploitable), oppure
 - creare un set di regole più restrittive che bloccano un intervallo di porte o tutte tranne quelle necessarie.
- In alternativa, per controlli più sofisticati, si può impiegare un IDS/IPS o monitorare i log di pfSense per rilevare tentativi di scansione.

7 Raccomandazioni

- Se lo scopo è solo impedire l'accesso alla DVWA, la regola così com'è è sufficiente.
- Se si vuole impedire ogni tipo di scansione, si consiglia di bloccare tutto il traffico dalla sorgente Kali verso la destinazione Metasploitable e permettere solo eccezioni strettamente necessarie (ad esempio solo ICMP per debug).
- Mettere la regola in cima alle regole LAN (above default allow) per garantire che venga valutata per prima.
- Conservare screenshot dei log pfSense (Diagnostics → System Logs → Firewall) per dimostrare i pacchetti bloccati durante la prova.

8 Conclusione

L'esercizio dimostra l'importanza della segmentazione e dell'applicazione delle regole alla giusta interfaccia: posizionare la regola sulla LAN è la scelta più chiara e gestibile. La regola attuale blocca l'accesso HTTP alla Metasploitable2 mantenendo il ping attivo per verifiche diagnostiche.