

Esercizio S5/L1

← → ↻ 🏠 🔍 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

pfSense
COMMUNITY EDITION

☰

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)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	1/1.14 MiB	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✗	0/3 KiB	IPv4	TCP	*	*	80 (HTTP)	*	none		📄 ⚙️ 🗑️
<input type="checkbox"/>	✓	1/389 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

📘

← → ↻ 🏠 🔍 192.168.49.101 ☆ 📧 📁 📄

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

The connection has timed out

The server at 192.168.49.101 is taking too long to respond.

- 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.

kali@kali ~

File Actions Edit View Help

```
(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=1.78 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=0.709 ms
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=0.747 ms
^C
--- 192.168.49.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.709/1.079/1.782/0.497 ms

(kali@kali)~$
```

Try Again

Timed Out

Abbiamo configurato la rete per filtrare i pacchetti indirizzati sulla dvwa, provenienti dalla lan, grazie alla policy inserita nel firewall. In questo caso il pacchetto viene filtrato sull'interfaccia LAN da ogni suo ip solo verso la porta HTTP.