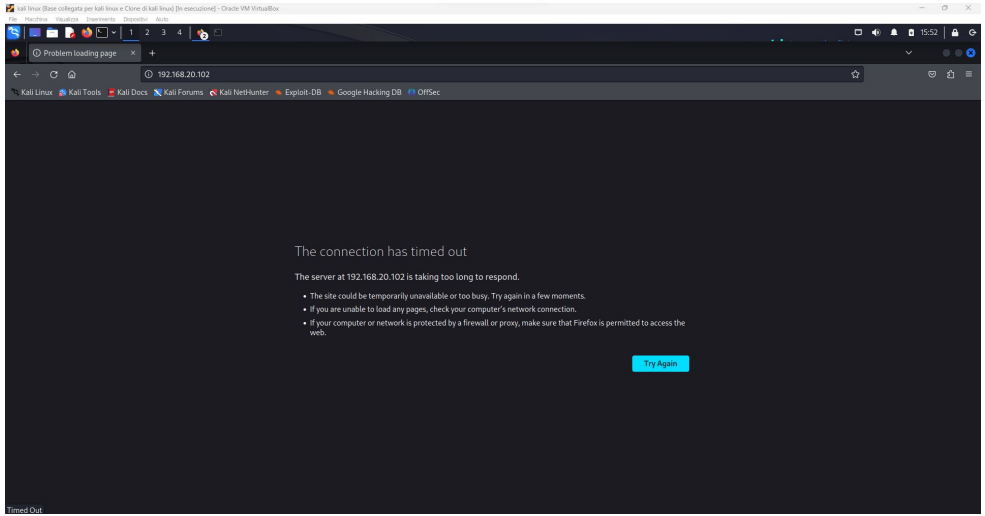
S5-L1

```
 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: 7


Enter a host name or IP address: www.google.com

PING www.google.com (216.58.204.228): 56 data bytes
64 bytes from 216.58.204.228: icmp_seq=0 ttl=114 time=17.667 ms
64 bytes from 216.58.204.228: icmp_seq=1 ttl=114 time=17.445 ms
64 bytes from 216.58.204.228: icmp_seq=2 ttl=114 time=16.013 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 16.013/17.042/17.667/0.733 ms

Press ENTER to continue.
```

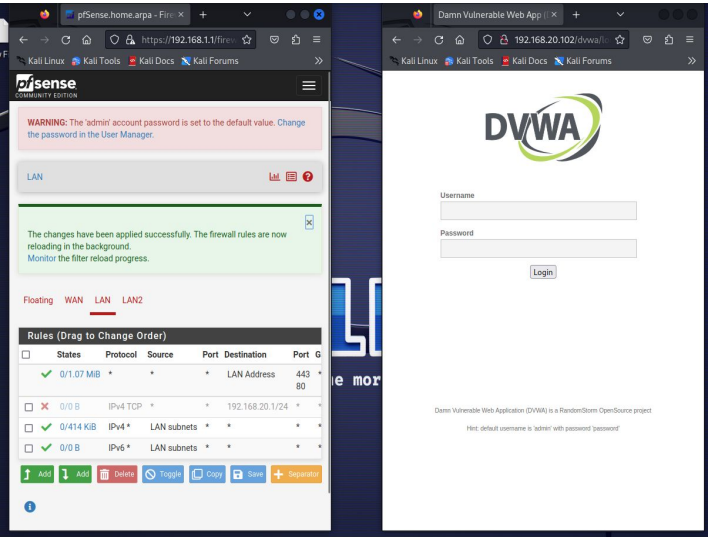
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.102
PING 192.168.20.102 (192.168.20.102) 56(84) bytes of data.
```

qui ho provato ad effettuare il ping a meta con la regola attiva



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.102
PING 192.168.20.102 (192.168.20.102) 56(84) bytes of data.
64 bytes from 192.168.20.102: icmp_seq=1 ttl=63 time=1.07 ms
64 bytes from 192.168.20.102: icmp_seq=2 ttl=63 time=0.396 ms
64 bytes from 192.168.20.102: icmp_seq=3 ttl=63 time=0.600 ms
64 bytes from 192.168.20.102: icmp_seq=4 ttl=63 time=0.397 ms
^C
── 192.168.20.102 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.396/0.614/1.065/0.273 ms

┌──(kali㉿kali)-[~]
└─$
```

ping con regola disattiva



Action Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface LAN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol TCP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match | Any | Source Address | /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match | Address or Alias | 192.168.20.1 | /

Destination Port Range

From	Custom	To	Custom
any		any	

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.