

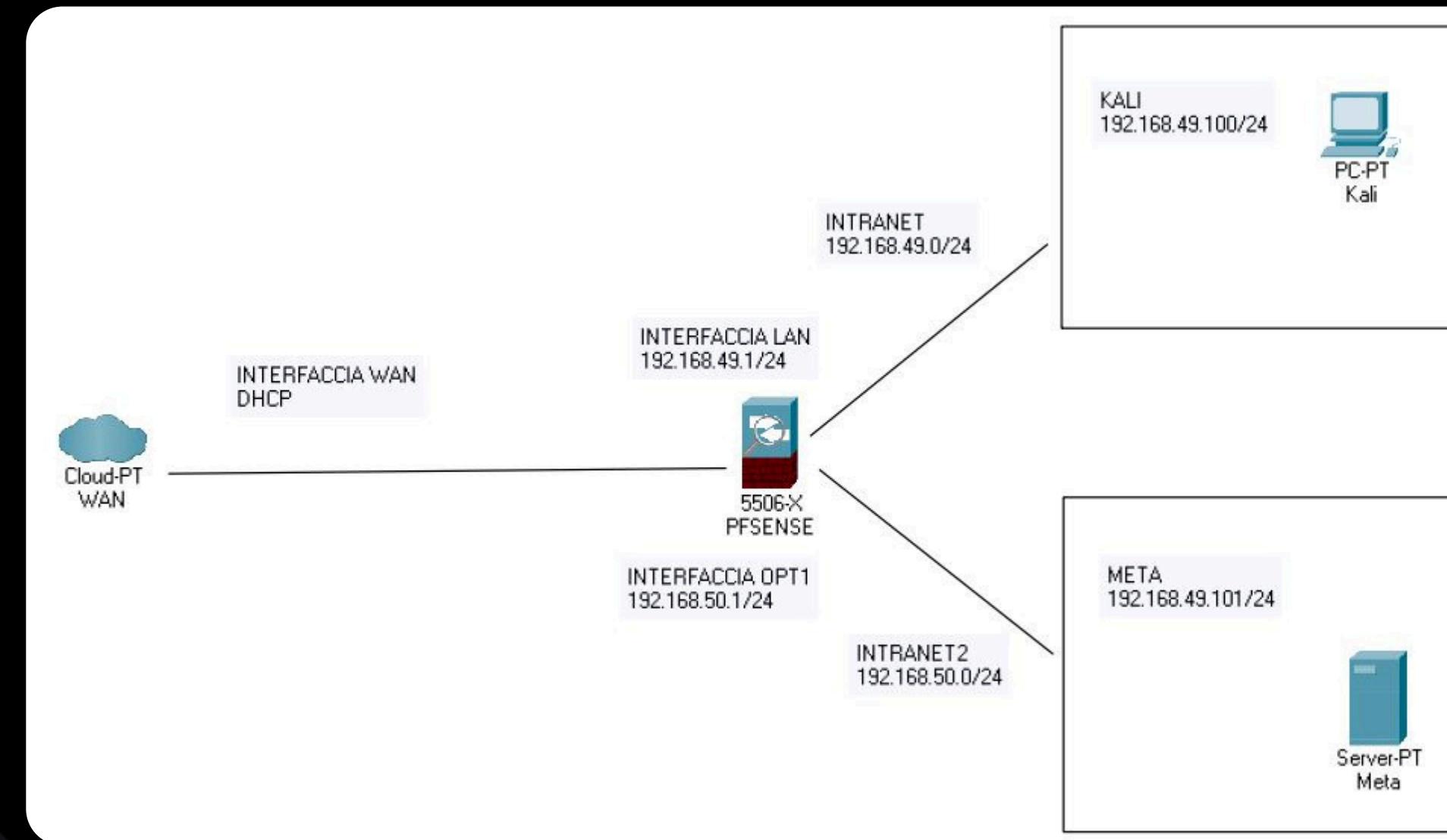
EPISODE

S5 - L1

1 TRACCIA

*CREARE UNA REGOLA FIREWALL CHE BLOCCHI
L'ACCESSO ALLA DVWA DALLA MACCHINA KALI
LINUX E NE IMPEDISCA LO SCAN.*

2 DESIGN RETE



```
**** Welcome to pfSense 2.0-RC3-cdrom (i386) on pfSense ****  
WAN (wan)          -> em0           -> 10.0.2.15 (DHCP)  
LAN (lan)          -> em1           -> 192.168.49.1  
OPT1 (opt1)        -> em2           -> 192.168.50.1
```

Impostazione PfSense

- 1 Installazione di PfSense
- 2 Impostazione delle interfacce di rete

3 PING SENZA FIREWALL RULES

- PfSense pinga con Meta

```
Enter a host name or IP address: 192.168.50.101
PING 192.168.50.101 (192.168.50.101): 56 data bytes
64 bytes from 192.168.50.101: icmp_seq=0 ttl=64 time=0.132 ms
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.126 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.123 ms
```

```
(kali㉿kali)-[~/Desktop]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=63 time=6.80 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=63 time=0.194 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=63 time=0.228 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=63 time=0.199 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=63 time=0.189 ms
```

- PfSense pinga con Kali

- Kali pinga con Meta

```
Enter a host name or IP address: 192.168.49.100
PING 192.168.49.100 (192.168.49.100): 56 data bytes
64 bytes from 192.168.49.100: icmp_seq=0 ttl=64 time=0.145 ms
64 bytes from 192.168.49.100: icmp_seq=1 ttl=64 time=0.136 ms
64 bytes from 192.168.49.100: icmp_seq=2 ttl=64 time=0.391 ms

--- 192.168.49.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.136/0.224/0.391/0.118 ms
```

4 PFSENSE SETTING FIREWALL RULES

Firewall: Rules: Edit

Edit Firewall rule

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 on which interface packets must come in to match this rule.

Protocol: **TCP/UDP**
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.

Source: **not**
Use this option to invert the sense of the match.
Type: **Single host or alias**
Address: **192.168.49.100** /

Advanced - Show source port range

Destination: **not**
Use this option to invert the sense of the match.
Type: **Single host or alias**
Address: **192.168.50.101** /

Destination port range:
from: **HTTP**
to: **HTTP**
Specify the port or port range for the destination of the packet for this rule.
Hint: you can leave the 'to' field empty if you only want to filter a single port

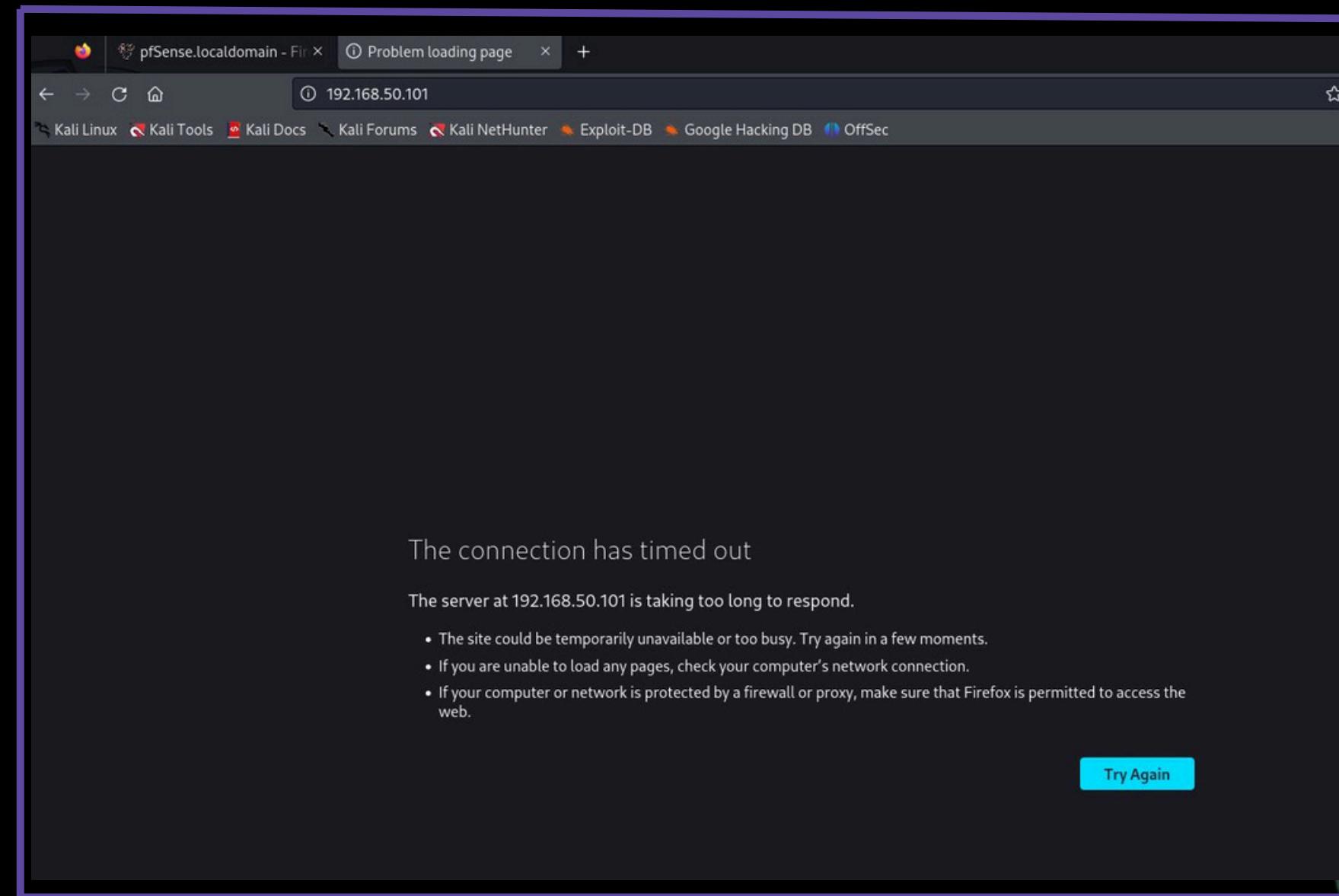
Log: **Log packets that are handled by this rule**
Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

Floating WAN LAN OPT1

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
1	*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule
2	*	LAN net	*	*	*	*	none		Default allow LAN to any rule
3	TCP/UDP	192.168.49.100	*	192.168.50.101	80 (HTTP)	*	none		

- Creiamo una regola che blocca ogni richiesta destinata all'indirizzo **192.168.50.101** sulla porta **80**.
- Disabilitiamo la regola precedente per permettere alla nuova di poter agire.

5 CONNECTION FAILED



A screenshot of a terminal window titled "kali@Team1-BuildWeek-Epicode: ~". The terminal shows the following output:

```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿Team1-BuildWeek-Epicode)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
^C
— 192.168.50.101 ping statistics —
588 packets transmitted, 0 received, 100% packet loss, time 605321ms

(kali㉿Team1-BuildWeek-Epicode)-[~]
$
```

TEAM



IOSIF
CASTRUCCI

DONATO TRALLI

GIANPAOLO
MILICCIA
MENDOZA