

## S3L5 BONUS

Impostare una regola su pfsense per bloccare da kali il telnet verso metasploitable.

Come per l'esercizio precedente avvio pfsense e apro il mio browser per usare la web gui.

Vado nuovamente nella sezione Firewall e poi Rules.

Imposto la nuova regola per la LAN1(metasploitable) bloccando i pacchetti indirizzati alla porta 23(telnet) da parte della LAN2.

The screenshot shows the 'Edit Firewall Rule' configuration page in pfSense. The rule is named 'Block' and is set to 'Block' action. It is disabled. The interface is set to 'LAN'. The address family is 'IPv4' and the protocol is 'TCP'. The source is 'LAN2 address' and the destination is 'LAN2 address'. The destination port range is 'Telnet (23)' to 'Telnet (23)'. The log checkbox is unchecked.

**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 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 LAN2 address 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 LAN2 address Destination Address /

**Destination Port Range** Telnet (23) From Custom Telnet (23) To Custom  
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**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 doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Infine salvo la regola e faccio una prova per vedere se il firewall è stato configurato correttamente

```
(kali@kali)-[~]
$ telnet 192.168.1.20 23
Trying 192.168.1.20 ...
telnet: Unable to connect to remote host: No route to host

(kali@kali)-[~]
$
```