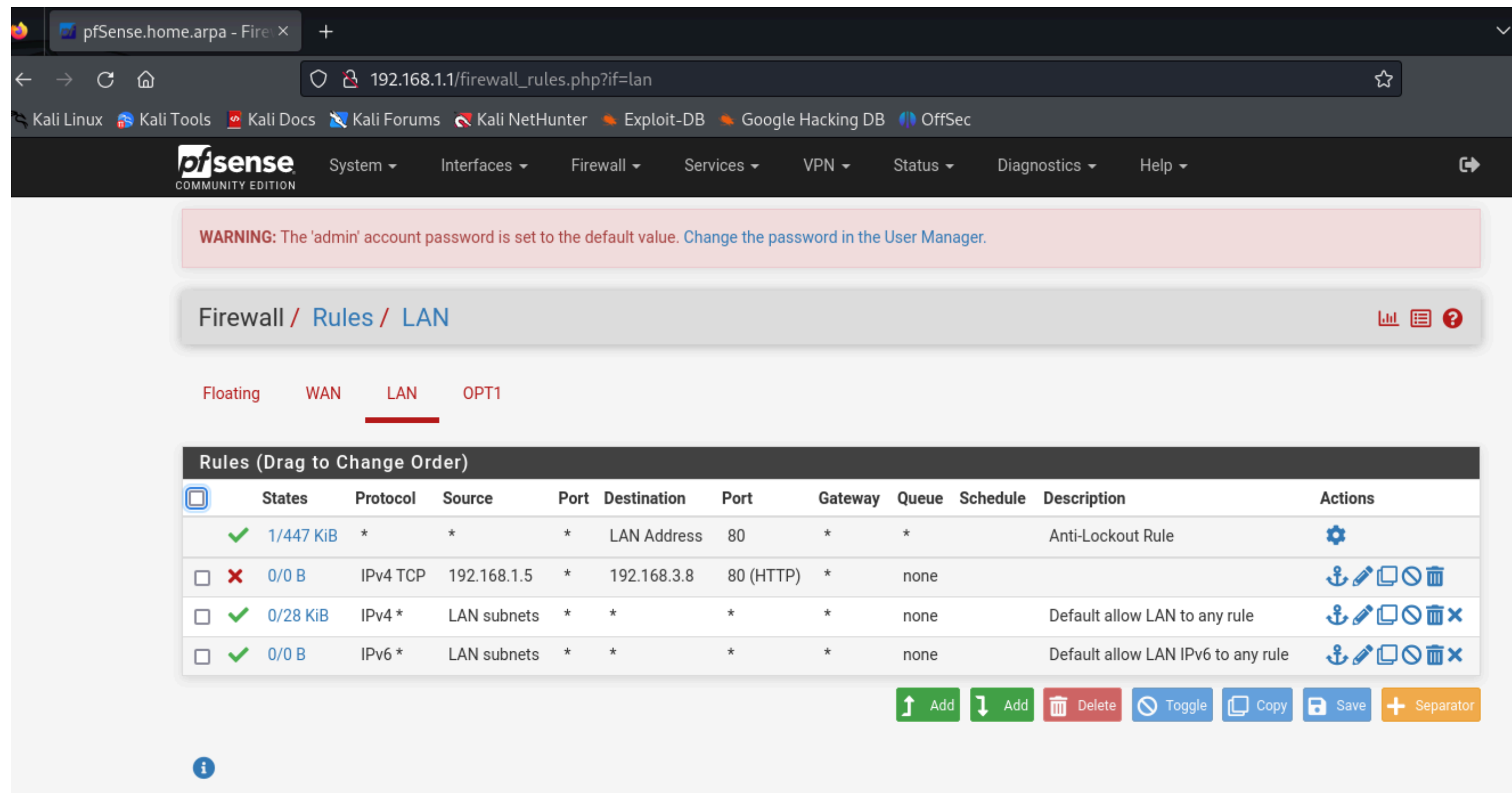


Creazione pratica di una regola Firewall. Esercizio Pfsense Per la creazione di una regola firewall, andare su Firewall > Rules. In questa sezione si può scegliere su quale interfaccia creare la regola: scegliamo LAN e clicchiamo su ADD (come vedete ci sono 2 add, il primo crea la regola in cima al policy set, la seconda in basso):

Enable	<input checked="" type="checkbox"/> Enable interface		
Description	<input type="text" value="OPT1"/> <small>Enter a description (name) for the interface here.</small>		
IPv4 Configuration Type	Static IPv4		
IPv6 Configuration Type	None		
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> <small>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.</small>		
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>		
MSS	<input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.</small>		
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> <small>Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</small>		
Static IPv4 Configuration			
IPv4 Address	<input type="text" value="192.168.3.1"/>	/	<input type="text" value="24"/>
IPv4 Upstream gateway	<input type="text" value="None"/> <input type="button" value="+ Add a new gateway"/> <small>If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.</small>		

anando su kalo ho cliccato fire fox e sulla barra di ricerca ho inserito l’ip di pfsense.dopo di che clicchiamo interfaces e lan e ci troveremo in questa schermata. abilitiamo interface. anado giu inserisco l’ip 192.168.3.1/24

Creazione pratica di una regola Firewall. Esercizio Pfsense Per la creazione di una regola firewall, andare su Firewall > Rules. In questa sezione si può scegliere su quale interfaccia creare la regola: scegliamo LAN e clicchiamo su ADD (come vedete ci sono 2 add, il primo crea la regola in cima al policy set, la seconda in basso):



qui andremo ad aggiungere cio che abbiamo creato al task precedente.andando su
firewall/rules/lan

Cliccando su add, possiamo aggiungere: Informazioni generiche:

- Action : in questa sezione si può scegliere come gestire il traffico analizzato.

- Interface : l'interfaccia da dove arrivano i pacchetti.
- Address family : Ipv4 oppure ipv6, si sceglie la versione di protocolli ip ai quali applicare la policy.
- Protocol : si sceglie il protocollo (e.g., tcp, udp, icmp).

The screenshot shows the 'Edit Firewall Rule' configuration page. It is divided into several sections:

- Action:** A dropdown menu is set to 'Block'. Below it, a hint states: '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:** A checkbox labeled 'Disable this rule' is unchecked. Below it, text says: 'Set this option to disable this rule without removing it from the list.'
- Interface:** A dropdown menu is set to 'LAN'. Below it, text says: 'Choose the interface from which packets must come to match this rule.'
- Address Family:** A dropdown menu is set to 'IPv4'. Below it, text says: 'Select the Internet Protocol version this rule applies to.'
- Protocol:** A dropdown menu is set to 'TCP'. Below it, text says: 'Choose which IP protocol this rule should match.'

Below these sections are two main configuration areas:

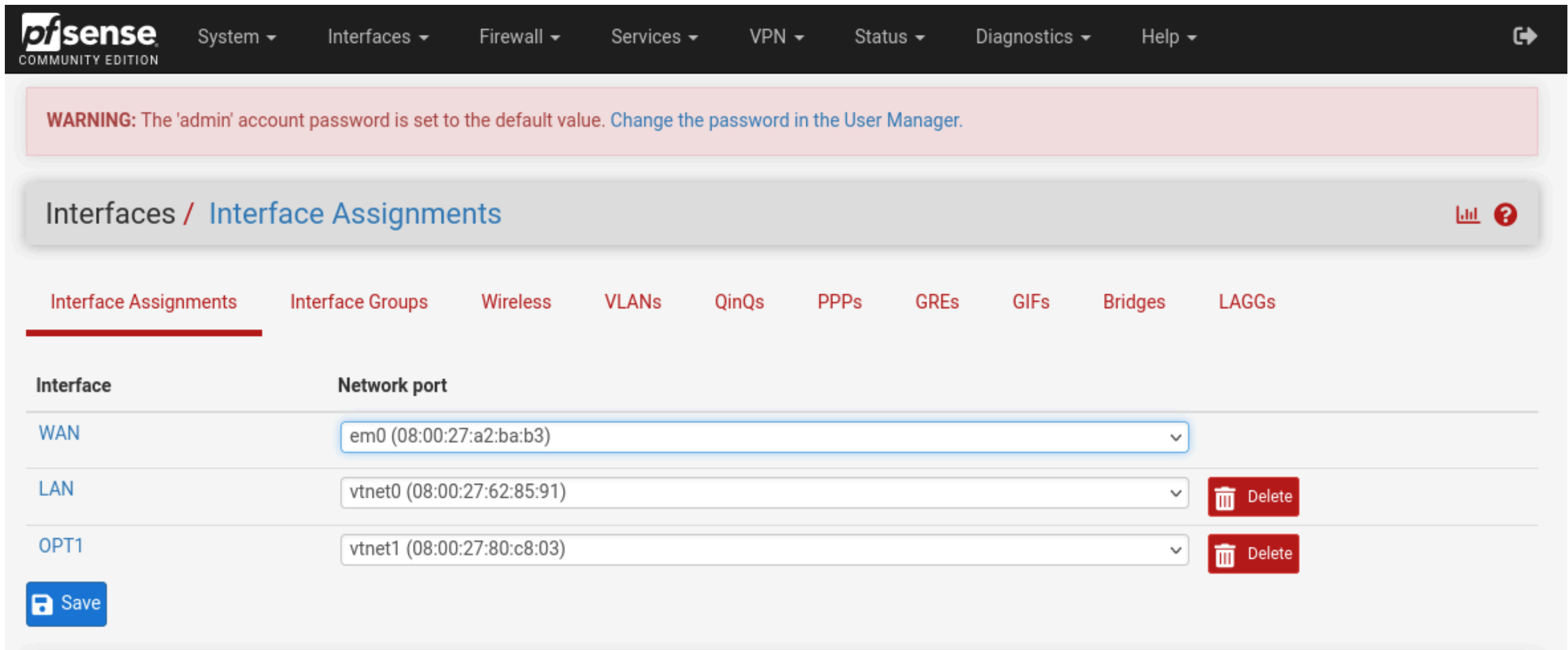
- Source:** Includes a checkbox for 'Invert match' (unchecked), a dropdown for 'Address or Alias' (set to 'Address or Alias'), and a text input for '192.168.1.5'. Below this is a 'Display Advanced' button and a note: 'The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.'
- Destination:** Includes a checkbox for 'Invert match' (unchecked), a dropdown for 'Address or Alias' (set to 'Address or Alias'), and a text input for '192.168.3.8'.

su Action: block
destination port range:http80
interface:lan
adress family:ipv4
protocol:TCP

Source : in questa sezione scelgo che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera. Nel campo valorizzato con «source address» vado ad inserire e ventualmente gli indirizzi IP o indirizzi rete in notazione CIDR.

Source				
<u>Source</u>	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.5 /	
<div>⚙ Display Advanced</div> <p>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.</p>				
Destination				
<u>Destination</u>	<input type="checkbox"/> Invert match	Address or Alias	192.168.3.8 /	
Destination Port Range	HTTP (80) From	Custom Custom	HTTP (80) To	Custom 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	<input type="checkbox"/> 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).			
Description				

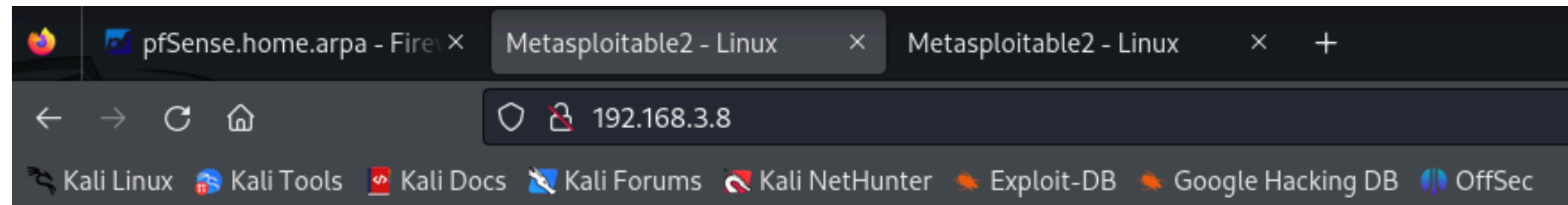
Sulla base di quanto visto, creare una regola firewall che blocchi l’accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell’esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.



qui avevo gia aggiunto opt1
su interfaces/assignments

l'ostacolo che non sono riuscito a fare e' bloccare metasploitable 2

Antre Mark Calabon



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)