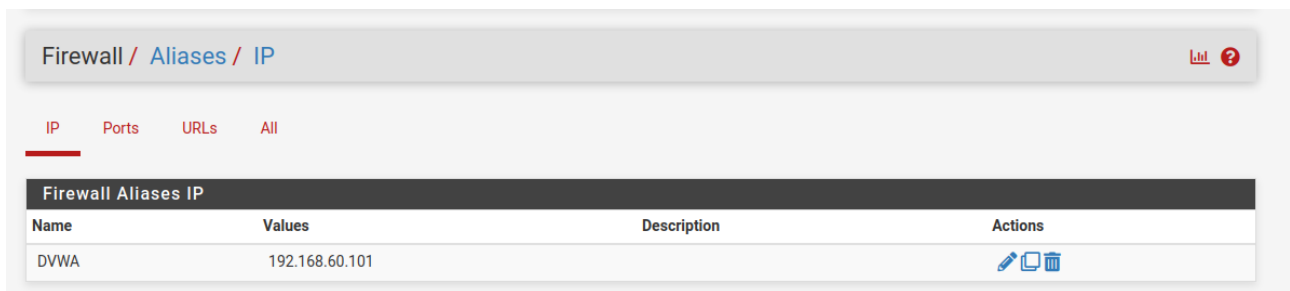


## Creazione Policy Pfsense:

Per prima cosa abbiamo creato un Alias in maniera da avere un riferimento più veloce nel caso dovessimo riutilizzarlo. In questa maniera ci basterà cercare ciò che ci serve, in questo caso DVWA



Nella pagina del Firewall -> Rules -> Creeremo una Regola che ci permetterà di bloccare oppure rendere attivo l'accesso verso il sito di nostro interesse, configurandolo quanto segue.

**Action** Block ▼  
Pass  
Block  
Reject

**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.

Qui inseriamo la Porta oppure il range di porte.

**Destination**

**Destination** ☐ Invert match Single host or alias ▼ DVWA / ▼

**Destination Port Range** HTTP (80) ▼ From Custom To HTTP (80) ▼ Custom

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

Qui sotto possiamo vedere se viene attivato "Block" nelle regole del Firewall

```
(kali㉿kali)-[~]
$ nmap 192.168.60.101
(kali㉿kali)-[~]
$ nmap 192.168.60.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 11:01 EST
Nmap scan report for 192.168.60.101
Host is up (0.041s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
```

Qui se viene  
acconsentito  
l'accesso