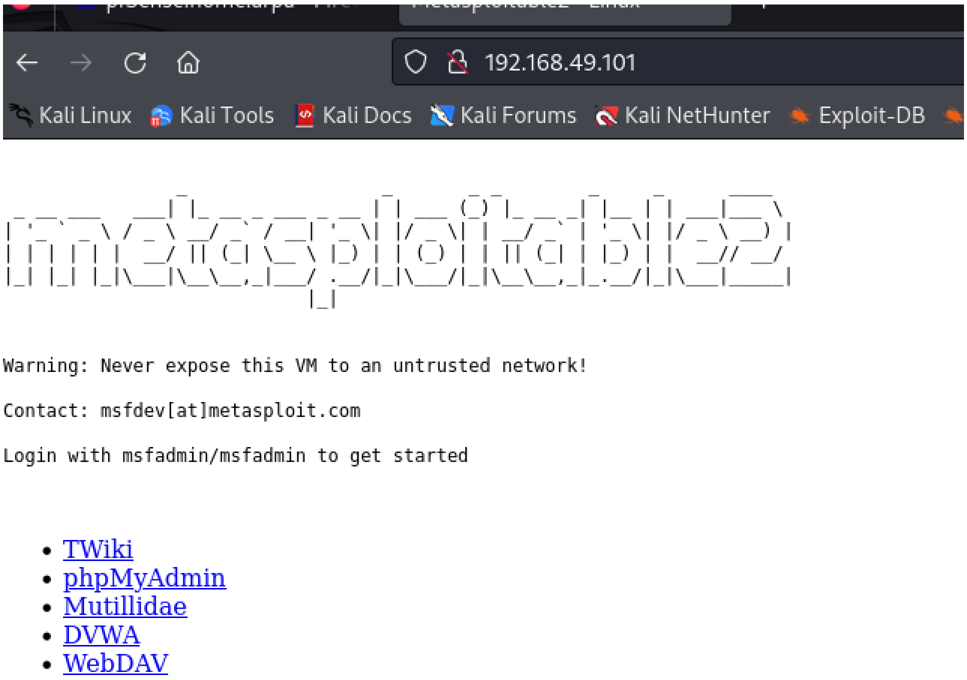
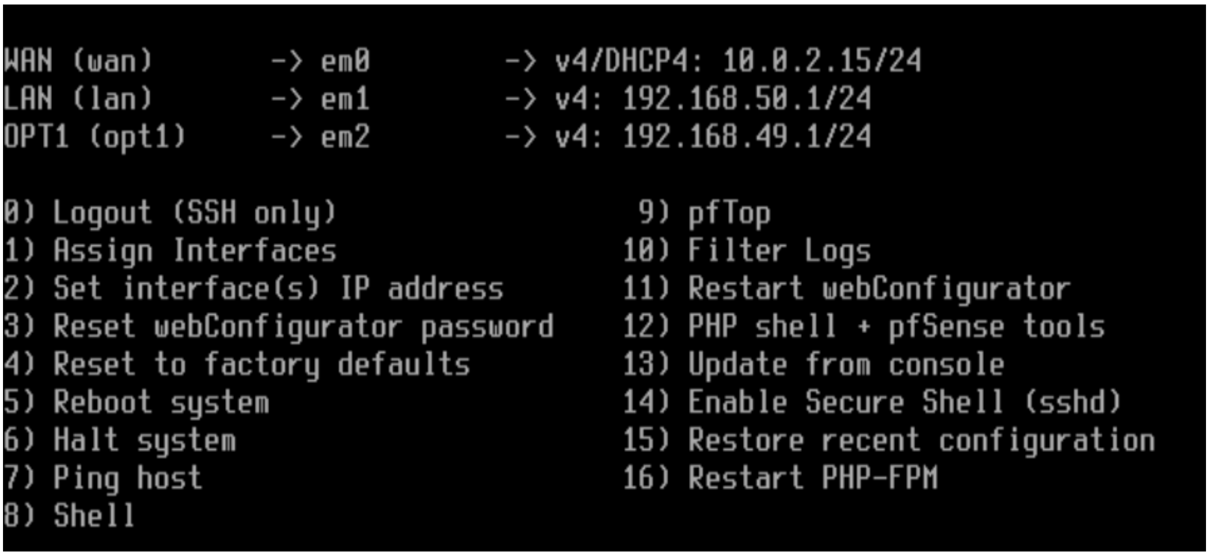
Dopo aver configurato le macchine virtuali dobbiamo creare un firewall che blocchi l'accesso da kali alla DVWA.



```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

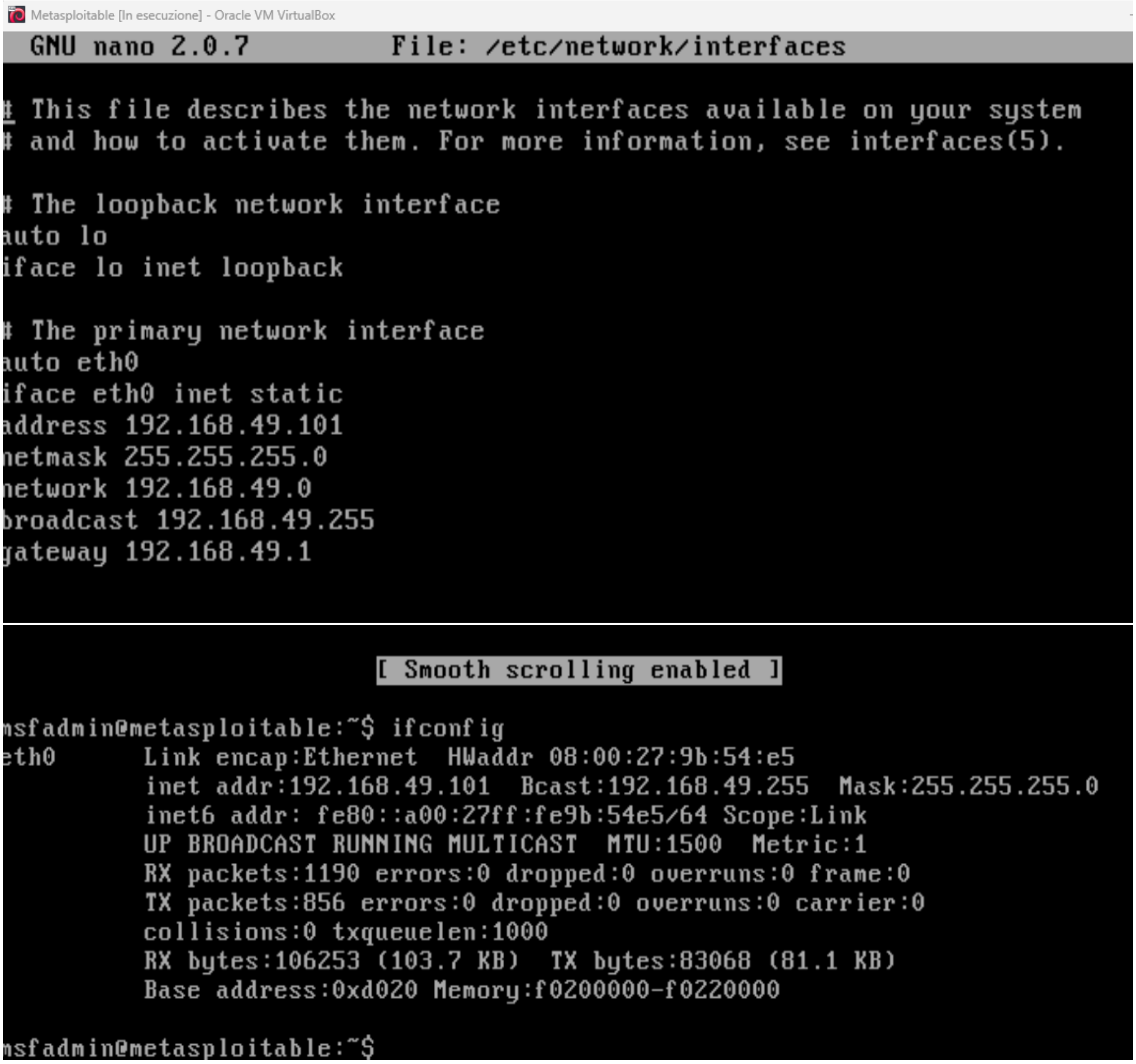
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Configurazione pfsense:



```
WAN (wan)       -> em0          -> v4/DHCP4: 10.0.2.15/24
LAN (lan)       -> em1          -> v4: 192.168.50.1/24
OPT1 (opt1)     -> em2          -> v4: 192.168.49.1/24

0) Logout (SSH only)                  9) pfTop
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
```

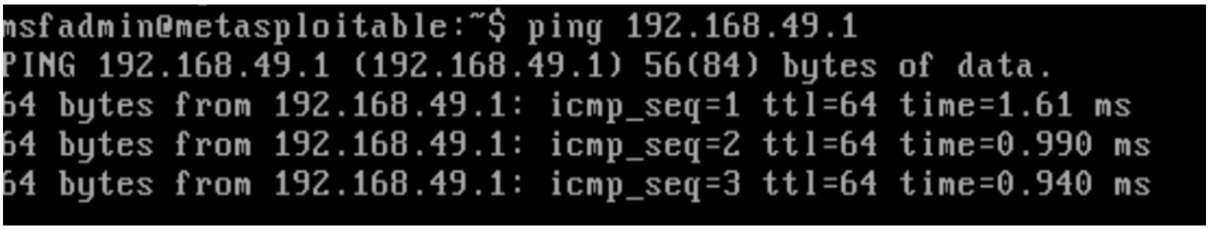
Andimao poi a cambiare l'indirizzo di Metasploitable:



```
  GNU nano 2.0.7          File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.49.101
netmask 255.255.255.0
network 192.168.49.0
broadcast 192.168.49.255
gateway 192.168.49.1


                        [ Smooth scrolling enabled ]

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:54:e5
          inet addr:192.168.49.101  Bcast:192.168.49.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:54e5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1190 errors:0 dropped:0 overruns:0 frame:0
          TX packets:856 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:106253 (103.7 KB)  TX bytes:83068 (81.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

msfadmin@metasploitable:~$
```

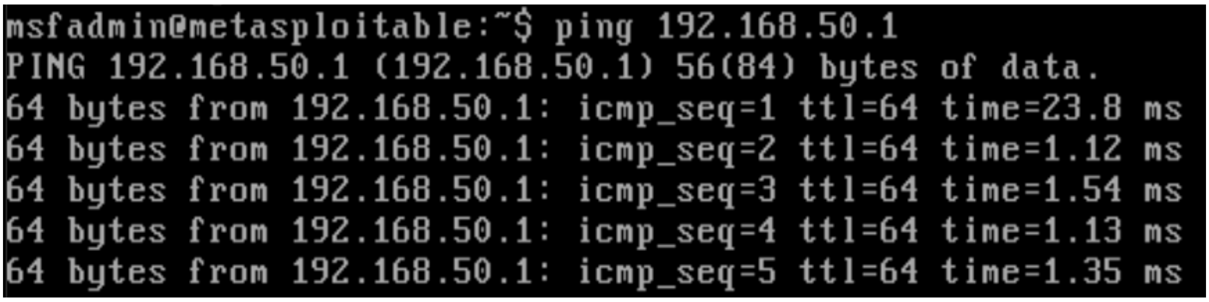
Verifichiamo che tutte le macchine comunichino tra di loro:

Da Metasploitable al opt di pfsense:



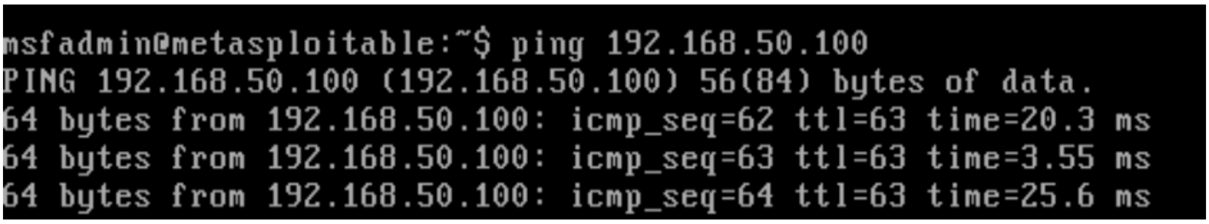
```
msfadmin@metasploitable:~$ ping 192.168.49.1
PING 192.168.49.1 (192.168.49.1) 56(84) bytes of data.
64 bytes from 192.168.49.1: icmp_seq=1 ttl=64 time=1.61 ms
64 bytes from 192.168.49.1: icmp_seq=2 ttl=64 time=0.990 ms
64 bytes from 192.168.49.1: icmp_seq=3 ttl=64 time=0.940 ms
```

Da Metasploitable alla lan di pfsense:



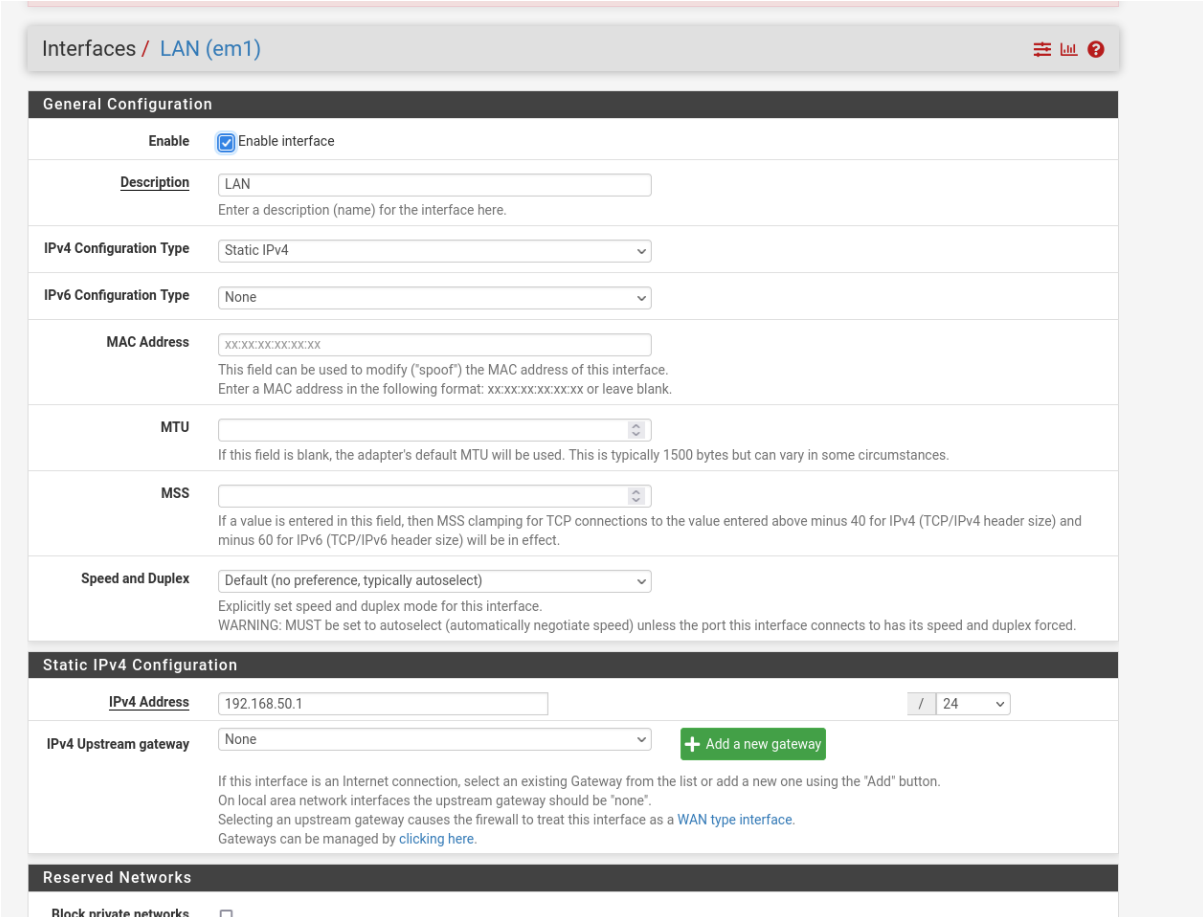
```
msfadmin@metasploitable:~$ ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=23.8 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=1.12 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=64 time=1.54 ms
64 bytes from 192.168.50.1: icmp_seq=4 ttl=64 time=1.13 ms
64 bytes from 192.168.50.1: icmp_seq=5 ttl=64 time=1.35 ms
```

Da Metasploitable a Kali:



```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=62 ttl=63 time=20.3 ms
64 bytes from 192.168.50.100: icmp_seq=63 ttl=63 time=3.55 ms
64 bytes from 192.168.50.100: icmp_seq=64 ttl=63 time=25.6 ms
```

Creiamo le regole del firewall sia per la lan che opt:



Interfaces / LAN (em1)

General Configuration

Enable ☑ Enable interface

Description LAN
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx
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.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
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.

Speed and Duplex Default (no preference, typically autoselect)
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.

Static IPv4 Configuration

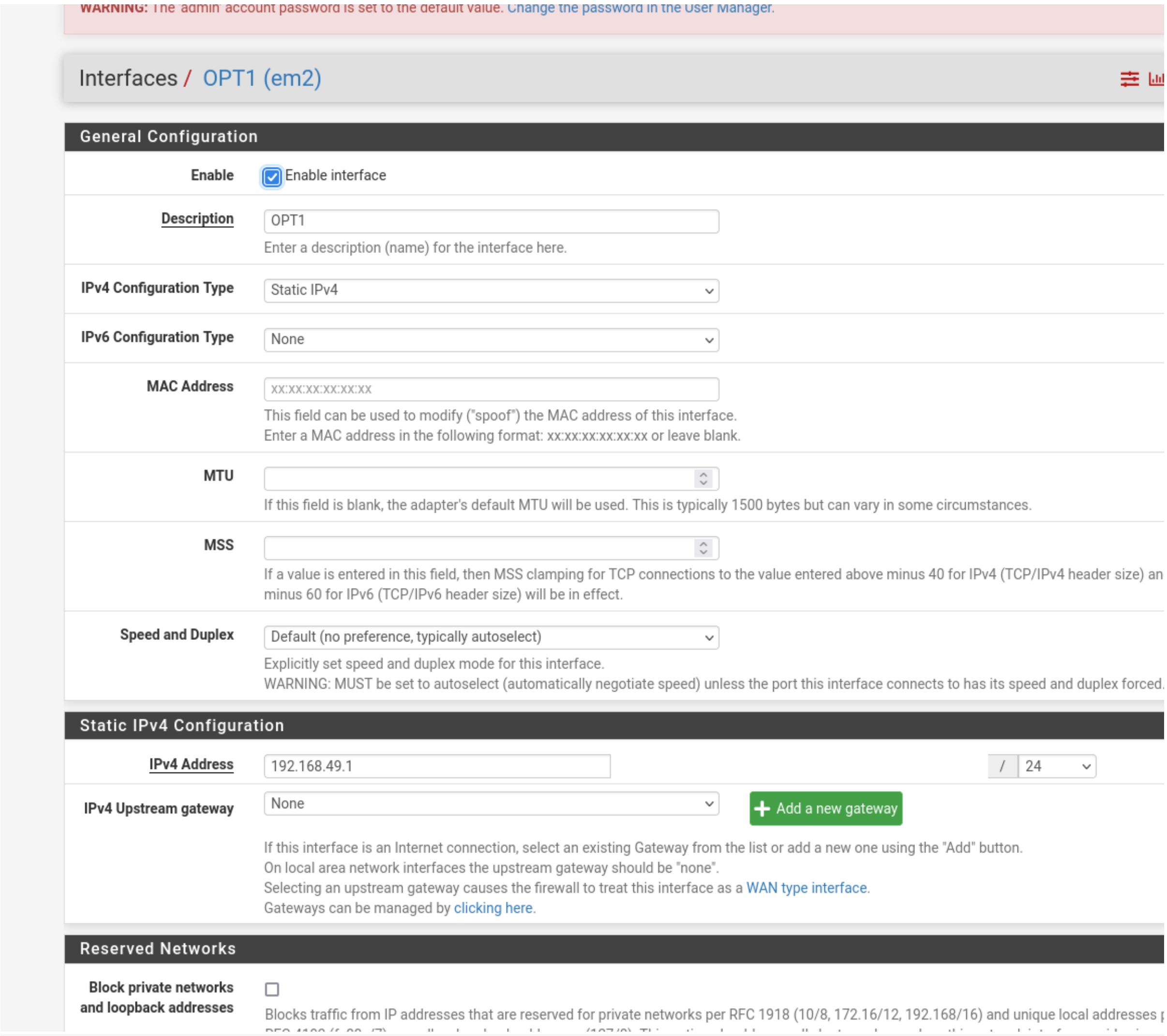
IPv4 Address 192.168.50.1 / 24

IPv4 Upstream gateway None

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.

Reserved Networks

Block private networks □



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces / OPT1 (em2)

General Configuration

Enable ☑ Enable interface

Description OPT1
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx
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.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
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) an minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
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.

Static IPv4 Configuration

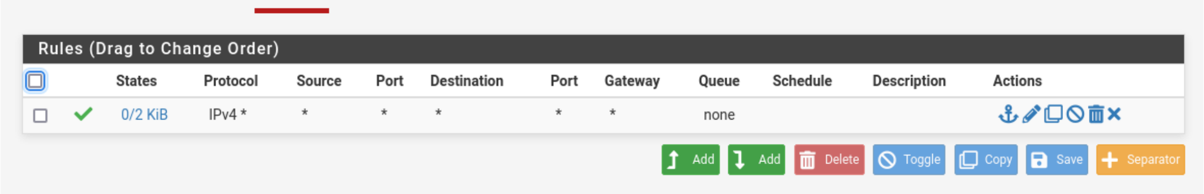
IPv4 Address 192.168.49.1 / 24

IPv4 Upstream gateway None

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.

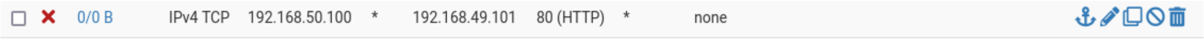
Reserved Networks

Block private networks and loopback addresses ☐
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses p



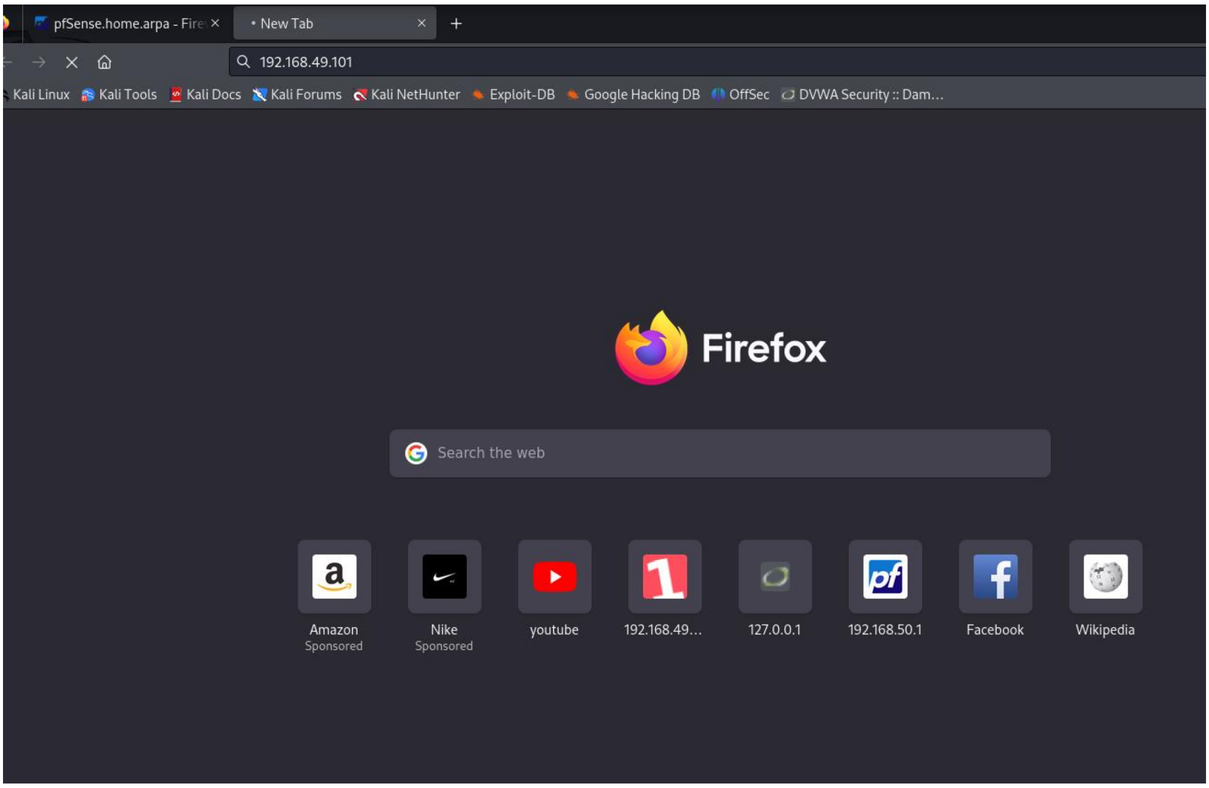
Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/2 KiB	IPv4 *	*	*	*	*	*	none			



☐	✗	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.49.101	80 (HTTP)	*	none

Andando poi ad attivarlo noteremo che non avremo piú accesso alla DVWA:


pfSense.home.arpa - Fire
New Tab
192.168.49.101
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA Security :: Dam...
Firefox
Search the web
Amazon
Sponsored
Nike
Sponsored
youtube
192.168.49...
127.0.0.1
192.168.50.1
Facebook
Wikipedia