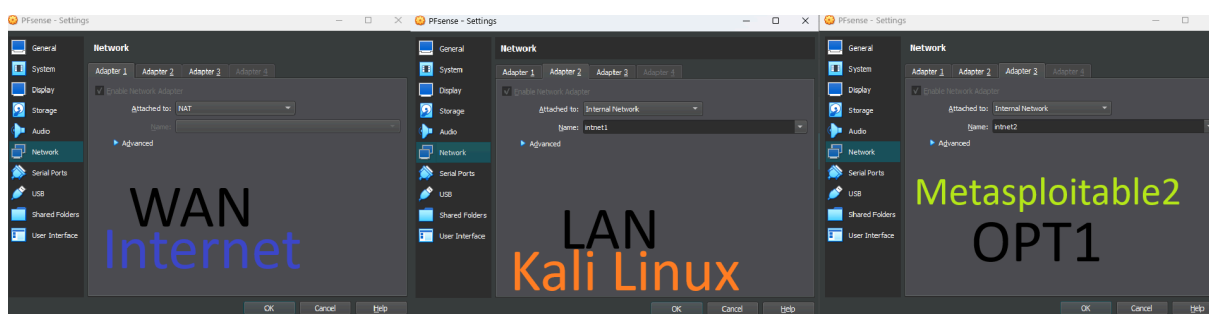


Network scheme

The result of this report is to learn to set a firewall rule between the local network (LAN) and the internet access (WAN) with a VM created in Oracle VM Virtualbox. In the VM there are PfSense installed.

How to set network adapters in Oracle VM Virtualbox to PfSense VM.



The setting are:

- Wan → NAT
- LAN → Intranet 1
- OPT1 → Intranet 2

Now, let's open the PfSense VM and configure the networks like the scheme viewed after.

```
DHCPD...

The IPv4 OPT1 address has been set to 192.168.49.1/24

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 8ea3b6f37256f529cbe2

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

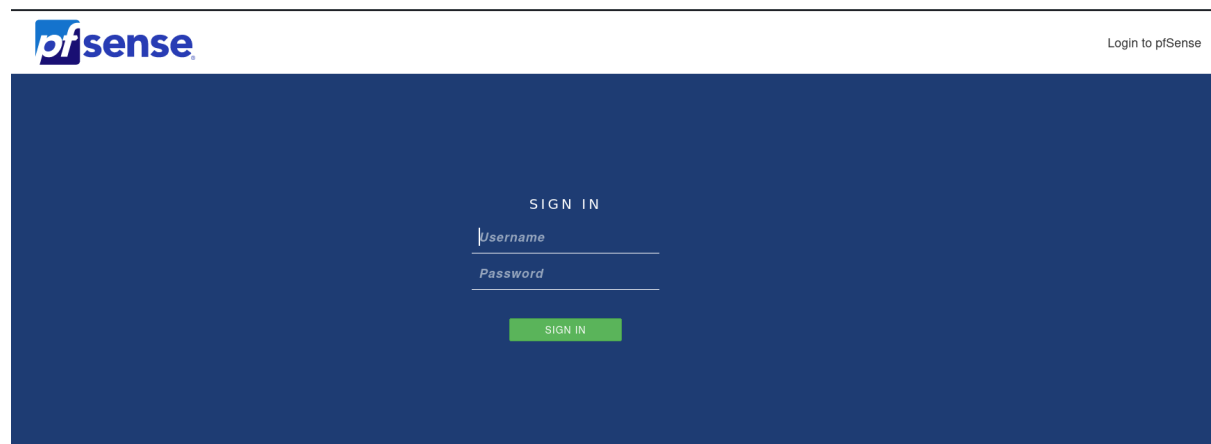
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.49.1/24

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

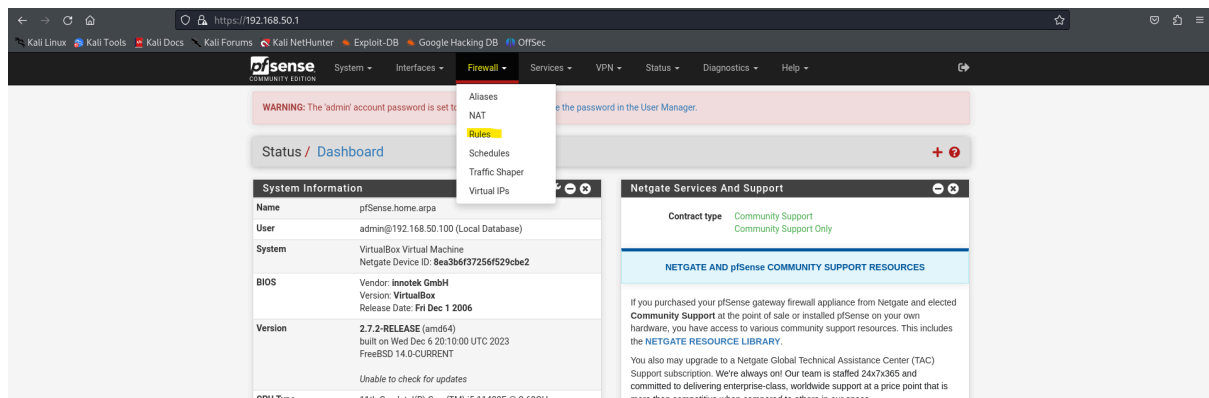
Enter an option: █
```

Set an IPv4 static address to all network's adapters.

To configure firewall rules, open the kali browser and insert a LAN gateway IP to access a PfSense web configurator.

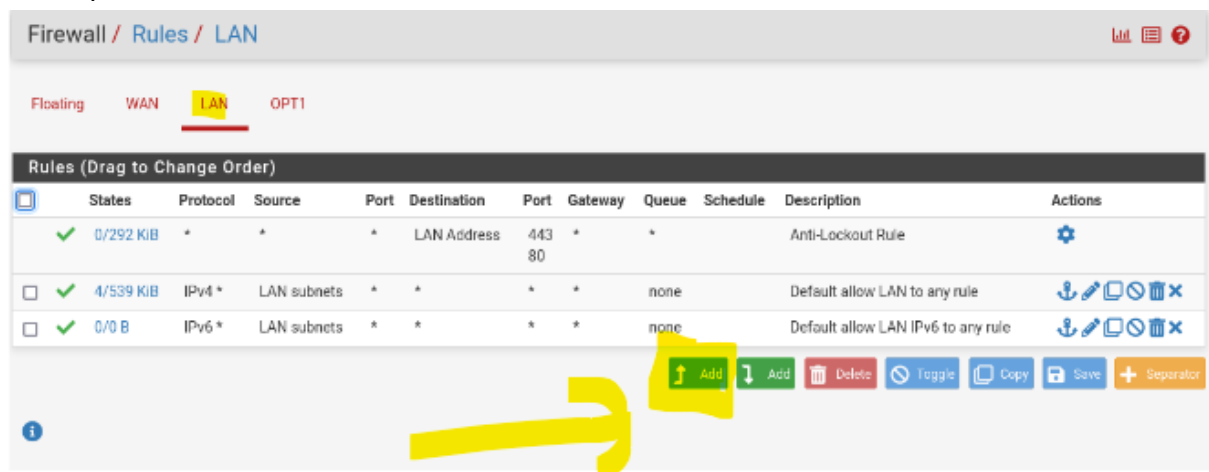


Standard username and password are admin - pfsense to access in web configurator.



Open Firewall tab and select Rules.

Let's open the LAN tab and ADD a new rule.



The goal is blocking the access from Kali (in intranet1) to Metasploitable 2 port 80 in section DVWA (in intranet 2).

metasploitable2

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](#)

This section will be unreachable because we'll be blocking access with PFsense .
For example this block will set from Kali.

Firewall / Rules / Edit

Edit Firewall Rule

Action Reject
 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.

Details of yellow highlighted titles:

- Action: Reject, reject all packages that will be sent from kali to external networks.
- 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 LAN 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 OPT1 address Destination Address /


Destination Port Range HTTP (80) From Custom HTTP (80) 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

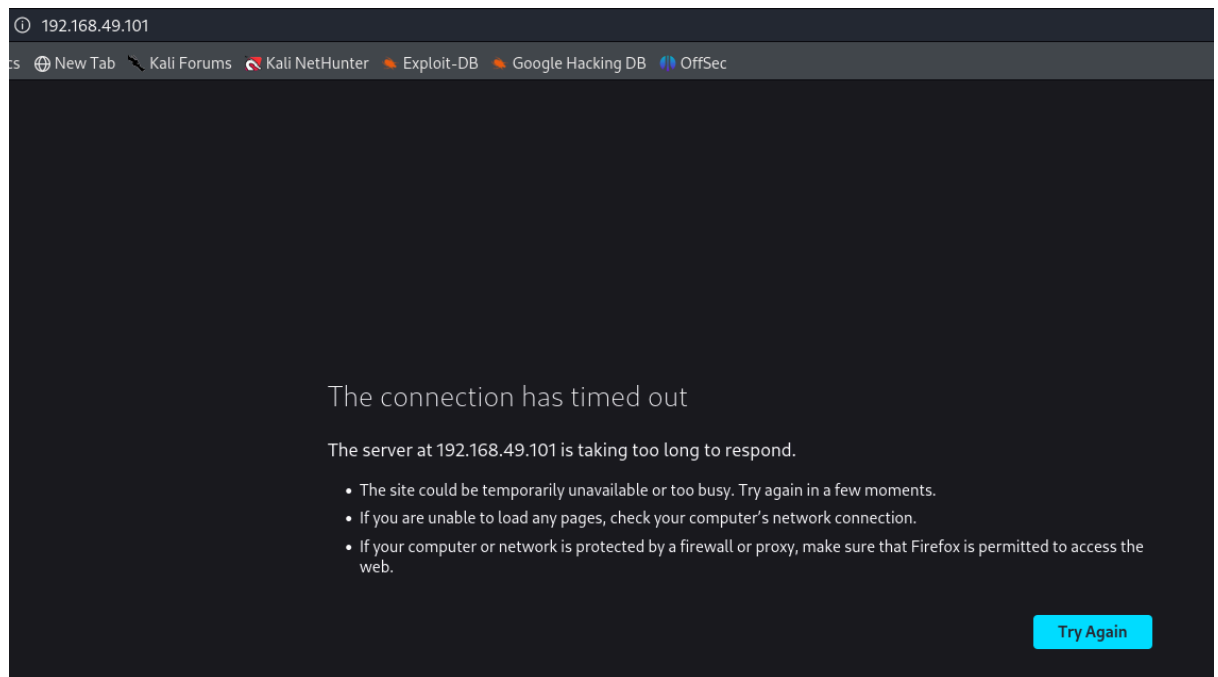
Log ☐ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Save 

At the end of configuration, save and try connecting to the Metasploitable2 address.



Can't connect to address because we set a rule that block all packages to try exit from firewall.