



Pfsense Project

24.06.2020

Harshwardhan Mehrotra

Overview

This is a basic setup of pfsense firewall for an organization. I have used 2 ubuntu machines as examples of users.

Goals

1. To allow specific traffic to the network and save it from malicious activities.
2. To block some websites from normal user.
3. Setup load balancing for the web servers.

Specifications

- Admin and user machines:

OS:Ubuntu 16.04(x64)

Ram: 2gb

Hard drive:15gb

Processing cores:1

- pfsense machine:

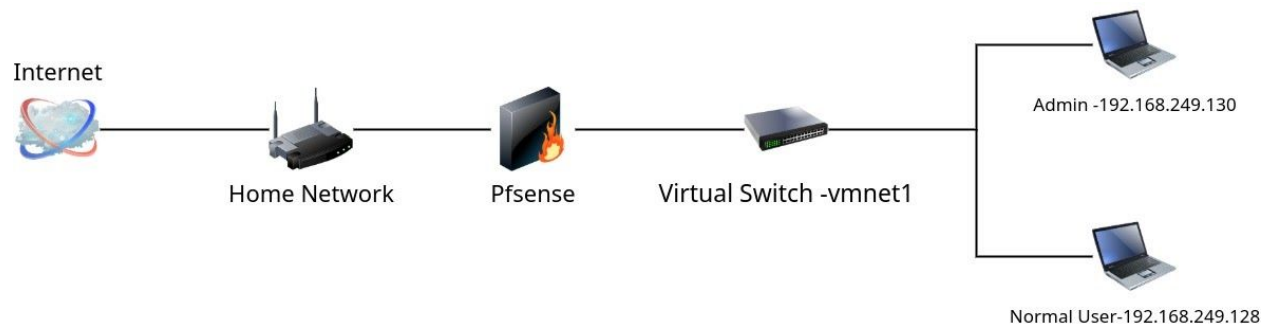
OS:pfsense

Ram:2gb

Hard drive:7gb

Processing cores:1

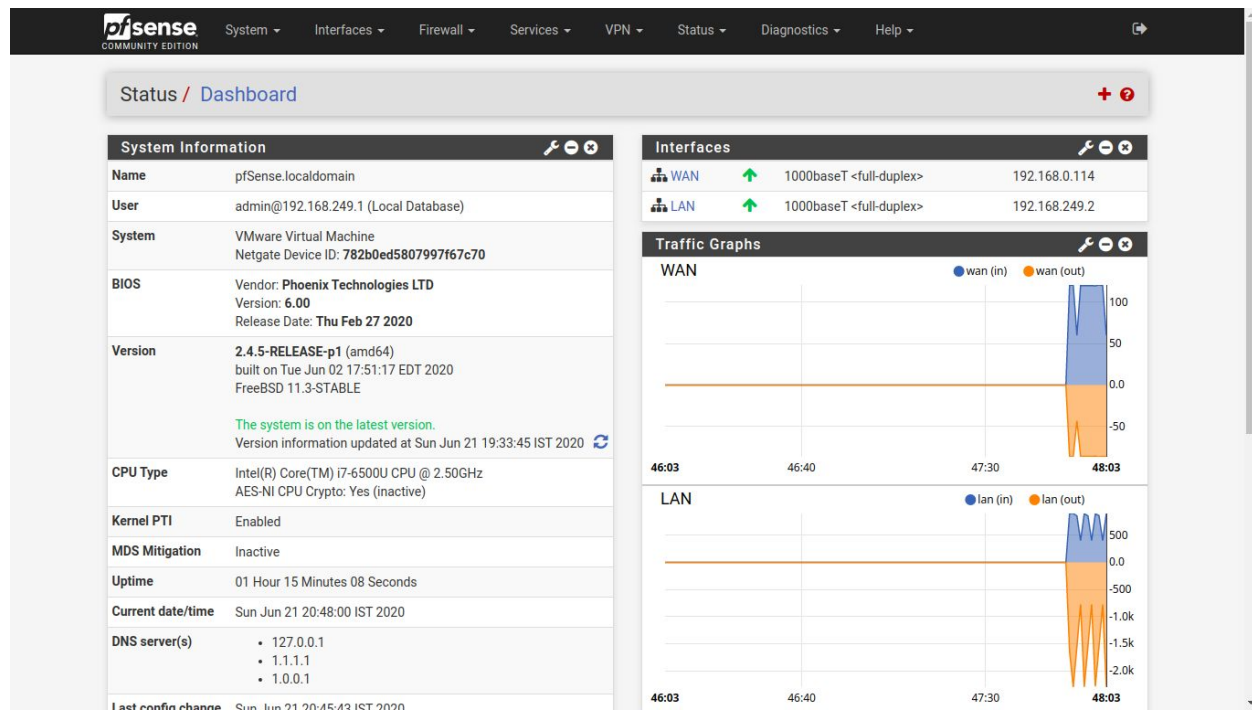
Network Setup



This is the network setup I used. Here the internet goes to my Main Home basic router. From there Wifi is used as Wan for the pf sense firewall and for the lan side of the firewall, I have used a virtual switch to which 2 virtual machines are connected.

Pfsense Setup

- Dashboard



- Aliases

The screenshot displays the pfSense Firewall Aliases IP configuration page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two sections:

- Firewall Aliases IP:**
 - IP:** Selected tab.
 - Ports:** Unselected tab.
 - URLs:** Unselected tab.
 - All:** Unselected tab.
- Table:**

Name	Values	Description	Actions
facebook	102.132.100.0/24, 102.132.101.0/24, 102.132.102.0/24, 102.132.103.0/24, 102.132.104.0/24, 102.132.105.0/24, 102.132.106.0/24, 102.132.107.0/24, 102.132.108.0/24, 102.132.109.0/24...		Edit Delete
Normal_Users	192.168.249.128		Edit Delete
Wifi_routers	192.168.0.1, 192.168.0.22, 192.168.0.33		Edit Delete

At the bottom right, there are buttons for **Add** and **Import**.

Aliases in pfSense are used for using just a name for a set of ip addresses to ease the process of making rules . In my case I have made 3 aliases first for Normal users in which ip addresses of normal users are present ,as more users are added to the network instead of adding a new rule for each user we can just add their ip address to this alias. Second is for facebook in which all the ip addresses of facebook are present this is used while making rule for normal users to block facebook.and the third is just for my wifi network this is just for my case and won't be required when used in an organization's network.

● Rules

○ Lan

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 / 14.70 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	⚙️
✓	1 / 4.40 MiB	IPv4 *	192.168.249.130	*	*	*	*	none		full access to admin	⚙️
✗	0 / 7 KiB	IPv4 TCP/UDP	Normal_Users	*	facebook	*	*	none		block facebook	⚙️
✓	3 / 8.46 MiB	IPv4 TCP/UDP	Normal_Users	*	*	*	*	none		normal user	⚙️

↑ Add ↓ Add Delete Save Separator

These are the rules set for the users in lan. I have made 3 rules first is to allow full access to the admin , second is for normal users which will block facebook any request made for facebook and the last is for normal users to allow all requests from normal users. Now the last rule allows all the request from normal users but the second rule is checked first before the third rule hence if any request is made the firewall first checks if the request is being made to facebook it gets blocked, if not then it goes to the third rule and allows the request.there is one more rule which is made by default which is used to allow access to the web ui through http and https ports.

○ WAN

The screenshot shows the pfSense Firewall Rules configuration page for the WAN interface. The 'Rules' tab is selected, and the 'WAN' interface is chosen. The table lists three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogus networks	[Settings]
10 / 381.87 MiB	IPv4 TCP/UDP	*	*	192.168.249.2	8080	*	none		nginx	[Add] [Edit] [Delete]
0 / 221 KiB	IPv4 TCP	*	*	192.168.249.130	22 (SSH)	*	none		ssh	[Add] [Edit] [Delete]
1 / 0 B	IPv4 IGMP	Wifi_routers	*	*	*	*	none			[Add] [Edit] [Delete]

At the bottom, there are buttons for 'Add', 'Add', 'Delete', 'Save', and 'Separator'.

These rules are for the ip addresses which try to make a request from the internet (basically outside your lan network). I have made 3 rules the first rule allows ip address from the WAN side to send requests to the web server on 192.168.249.2 at port 8080 , second is to allow access to 192.168.249.130 on port 22 through ssh and last is to allow IGMP requests made by router to talk to each other , again this rule won't be required in an organization's network as there won't be a middle router, pfSense will directly connect to the isp and route everything.

○ Port Forward

The screenshot shows the pfSense Port Forward configuration page for the WAN interface. The 'Port Forward' tab is selected, and the 'WAN' interface is chosen. The table lists two rules:

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
WAN	TCP	*	*	WAN address	1678	192.168.249.130	22 (SSH)		[Add] [Edit] [Delete]
WAN	TCP/UDP	*	*	WAN address	8080	192.168.249.2	8080	web server	[Add] [Edit] [Delete]

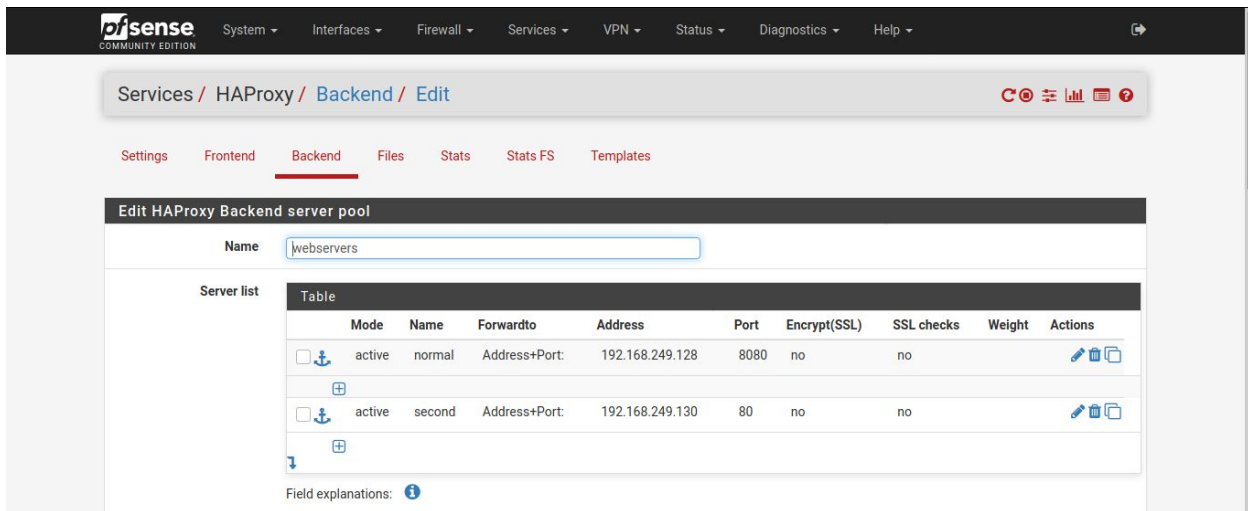
At the bottom, there are buttons for 'Add', 'Add', 'Delete', 'Save', and 'Separator'.

This is used to forward requests made on a specific port to a specific ip address. Here I have made 2 such rules first is to forward request to ip address 192.168.243.130 on port 22 if a request is made on pfSense's wan address on port 1678 (I chose port 1678 just for a little safety as it will get hidden from a basic nmap scan) and second is to forward request to ip address 192.168.243.2 on port 8080 if a request is made on pfSense's wan address on port 8080.

○ Load Balancing

I have used HAProxy to handle load balancing for the webserver.

○ Backend



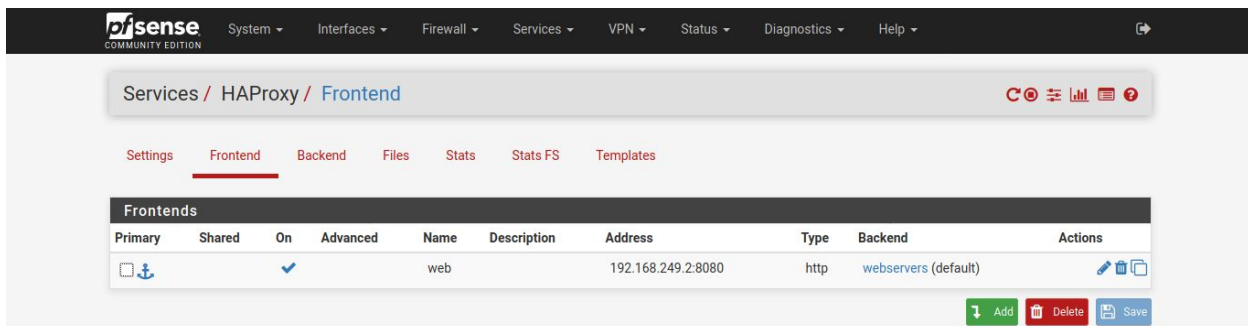
The screenshot shows the pfSense HAProxy Backend configuration page. The breadcrumb trail is Services / HAProxy / Backend / Edit. The 'Backend' tab is selected. The 'Name' field is set to 'webservers'. Below the name field is a 'Server list' table with the following data:

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions
active	normal	Address+Port	192.168.249.128	8080	no	no		[Edit] [Delete] [Copy]
active	second	Address+Port	192.168.249.130	80	no	no		[Edit] [Delete] [Copy]

Field explanations: ⓘ

On the backend side of the HAProxy I have added two web servers one working on admin machine and the other on normal user machine. Both the servers are setup in Round robin configuration which means everytime a new connection is made to the server the requests will be passed in turns to the web servers.

○ Frontend



The screenshot shows the pfSense HAProxy Frontend configuration page. The breadcrumb trail is Services / HAProxy / Frontend. The 'Frontend' tab is selected. The 'Frontends' table has the following data:

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		web		192.168.249.2:8080	http	webservers (default)	[Edit] [Delete] [Copy]

At the bottom right, there are buttons for Add, Delete, and Save.

On the front end side i have set up 192.168.249.2:8080 as the listening address and set the backend server.

Conclusion

In conclusion after setting up this basic pfsense firewall we can secure the machines on our network. After setting up this firewall if we do a basic nmap scan we only see one port open that is 8080 that is for our web server.

```
~ >>> nmap 192.168.0.114
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-23 21:28 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
~ >>> nmap -Pn 192.168.0.114
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-23 21:28 IST
Nmap scan report for 192.168.0.114
Host is up (0.0014s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 21.15 seconds
```

It does not show the ssh port because this is a basic scan and it does not scan all the ports. This reduces the surface area for an attacker to attack on.

If you want configuration file for this firewall setup you can get it on:-

https://github.com/harsh18262/basic_pfsense

Thank You