

15/06/22

Installations, configuration, paramétrage PFsense



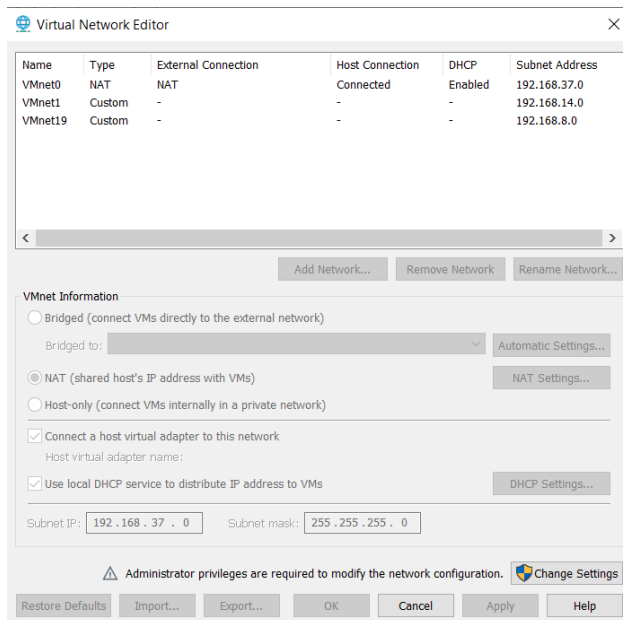
Réalisé par :

BOLIDUM Théo

Enseignants : KLEIN Dimitri.

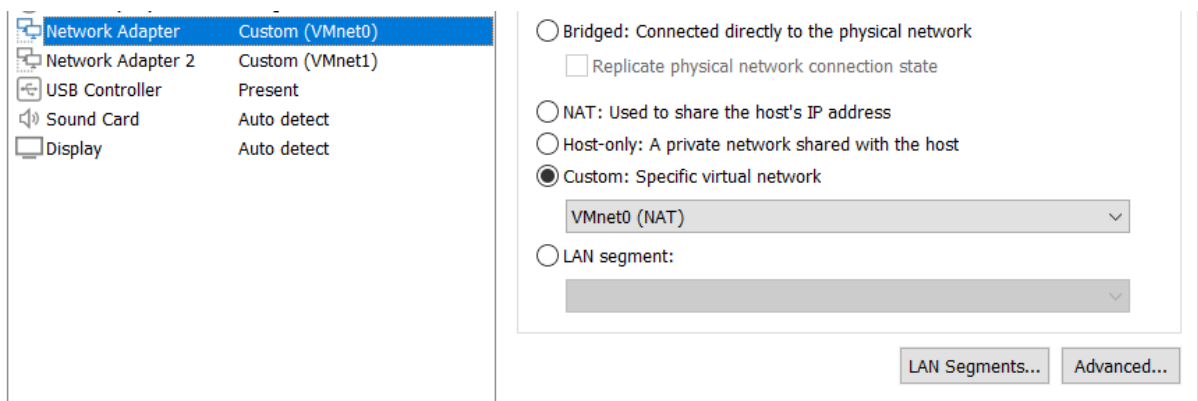
I) Installation de PfSense

Tout d'abord, je commence par configurer le réseau de ma machine virtuelle.



Nous avons deux cartes réseau :

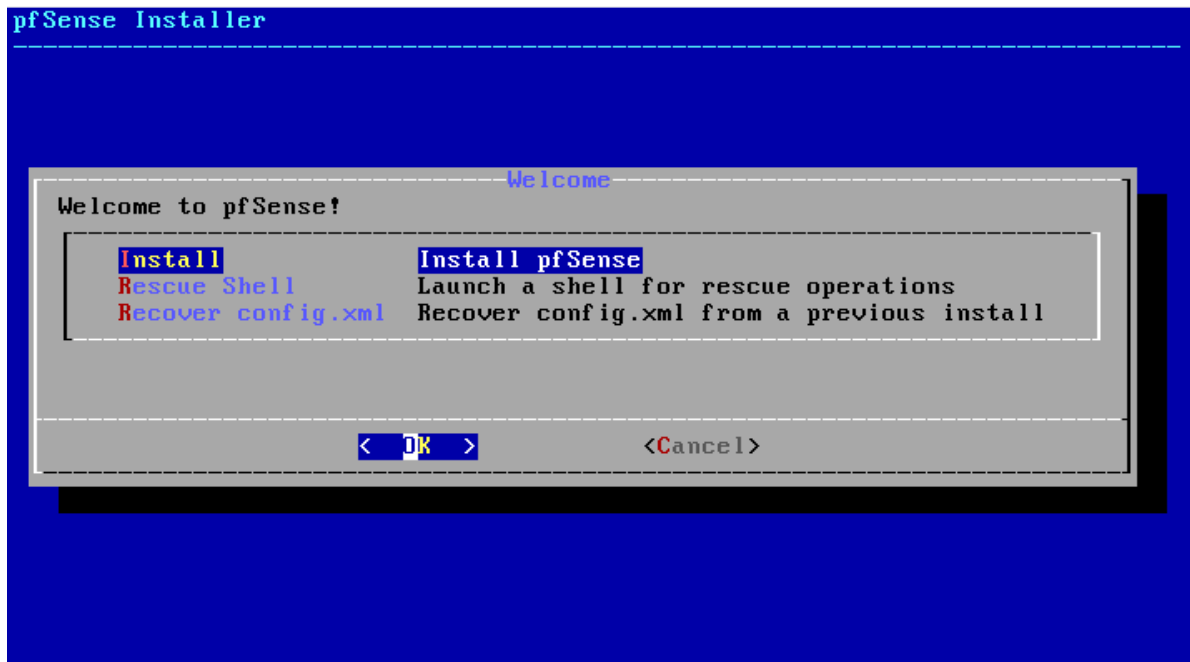
- Une carte VMnet0 en NAT
- Une carte VMnet1 en Custom



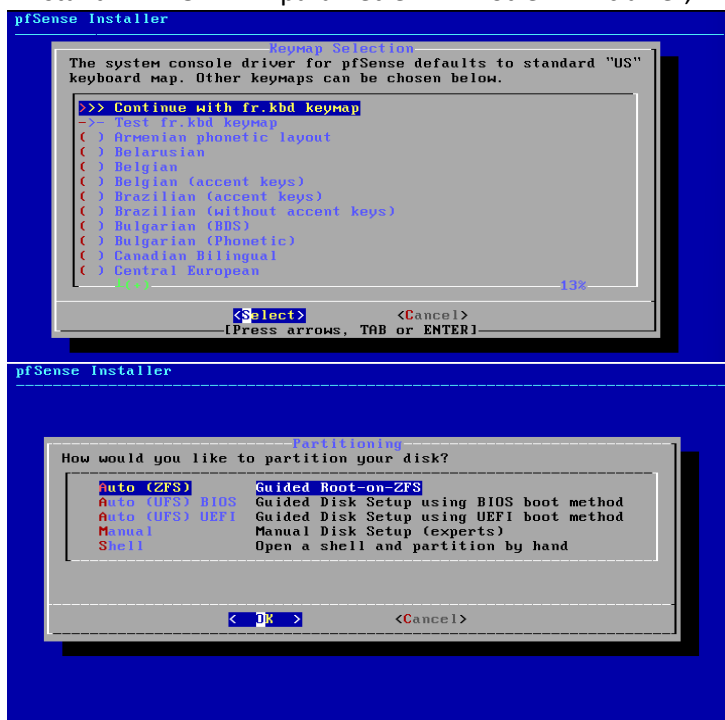
J'ai donc ajouté la carte réseau VMnet1 sur ma VM.

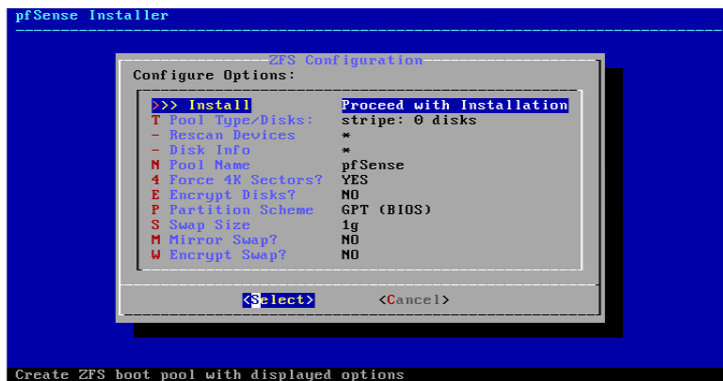
Ensuite nous pouvons passer à l'installation du système d'exploitation.

II) Installation du système d'exploitation

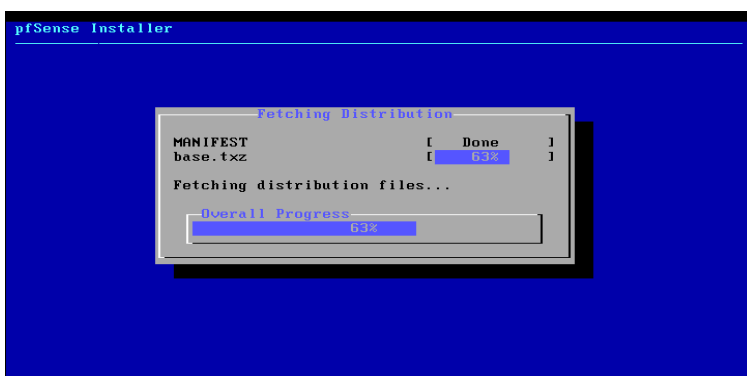
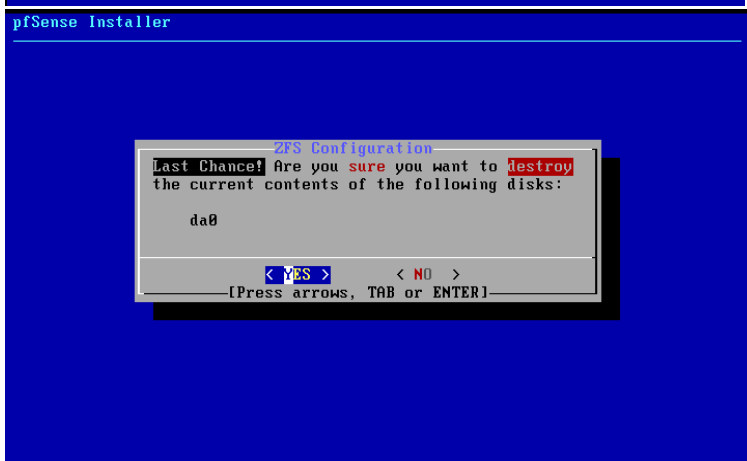
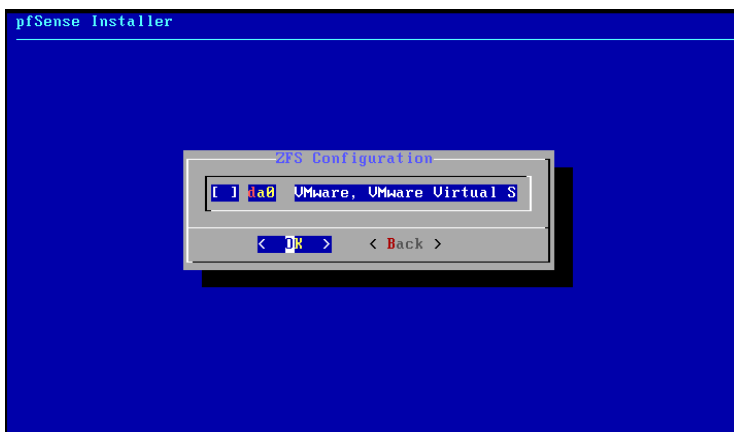


Suivons tout simplement le guide d'installation, il n'y a pas de paramètre particulier à configurer pour l'instant. On paramètre notre clavier, partitionning, et le ZFS.





Enfin, nous avons une fenêtre qui nous permet de sélectionner le disque à formater. Pour pouvoir le sélectionner, il faut que l'on fasse espace puis entrée. Ensuite il demandera confirmation pour détruire les données du disque sélectionné. L'installation commencera par la suite, et il faudra redémarrer la machine.



PFsense démarre.

```
Setting up extended sysctls...done.  
Setting timezone...done.  
Configuring loopback interface...done.  
Starting syslog...done.  
Setting up interfaces microcode...done.  
Configuring loopback interface...done.  
Configuring LAN interface...done.  
Configuring WAN interface...done.  
Configuring CARP settings...done.  
Syncing OpenVPN settings...done.  
Configuring firewall.....done.  
Starting PFLOG...done.  
Setting up gateway monitors...done.  
Setting up static routes...done.  
Setting up DNSs...  
Starting DNS Resolver...done.  
Synchronizing user settings...done.  
Configuring CRON...done.  
Bootstrapping clock...done.  
Starting NTP Server...done.  
Starting webConfigurator...done.  
Starting DHCP service...done.  
Starting DHCPv6 service...done.  
Configuring firewall.....done.  
█
```

III) Configuration de PfSense.

Une fois l'installation de PfSense terminée, nous allons pouvoir commencer la configuration de celui-ci.

Voici les différents paramétrage que PfSense propose :

```
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
```

L'option 2 nous intéresse, il s'agit de la configuration de l'adresse IP.

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
```

Sur ce menu, nous allons configurer la LAN et lui attribuer une IP

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.14.1
```

Il nous demandera ensuite le masque, étant donné que j'ai une adresse IP 192.168.14.1, il est logique de prendre le masque 255.255.255.0 en 24.

La configuration souhaite activer le DHCP, je dis non, nous allons la configurer plus tard sur le site.

```
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.14.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.14.1/
```

Nous ne configurons pas l'IP V6 et le Gateway.

Bien-sûr nous activons le site http.

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Voici la config' finale de PfSense :

```
The IPv4 LAN address has been set to 192.168.14.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.14.1/

Press <ENTER> to continue.S
VMware Virtual Machine - Netgate Device ID: fd174670adaa68831129

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.37.128/24
LAN (lan)      -> em1      -> v4: 192.168.14.1/24

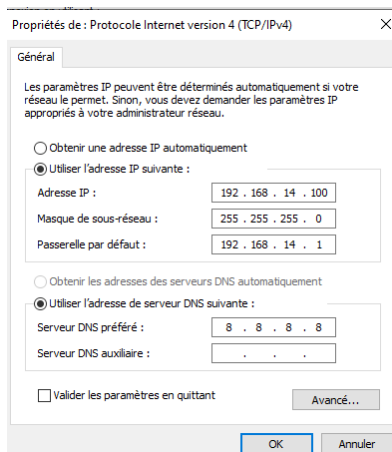
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Enfin, on reboot la machine à l'aide de l'option 5 et on confirme le reset normal.

IV) Configuration de la machine cliente

Pour ma machine cliente, j'ai choisi une VM windows 10. Je la configure en IP statique pour me connecter sur le site PfSense la première fois avec l'IP ci-dessous :



Bien évidemment, ma VM est sur le VMnet1.

Passage de PfSense en DHCP ainsi que la machine cliente.

Pour cela, tout ce passe sur le site. Tout d'abord, on configure PfSense via la page de configuration, nous mettons les DNS google et on laisse les paramètres par défaut pour le reste.

General Information

On this screen the general pfSense parameters will be set.

Hostname

EXAMPLE: myserver

Domain

EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS

☒

Allow DNS servers to be overridden by DHCP/PPP on WAN

SelectedType

General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxx:xx:xx:xx:xx:xx or leave blank.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

Check for updates

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

Pour passer en DHCP nous allons dans « services » « DHCP server » et « LAN », on coche « Enable DHCP server on LAN interface » et on « Allow known clients from only this interface »

General Options

Enable

☒ Enable DHCP server on LAN interface

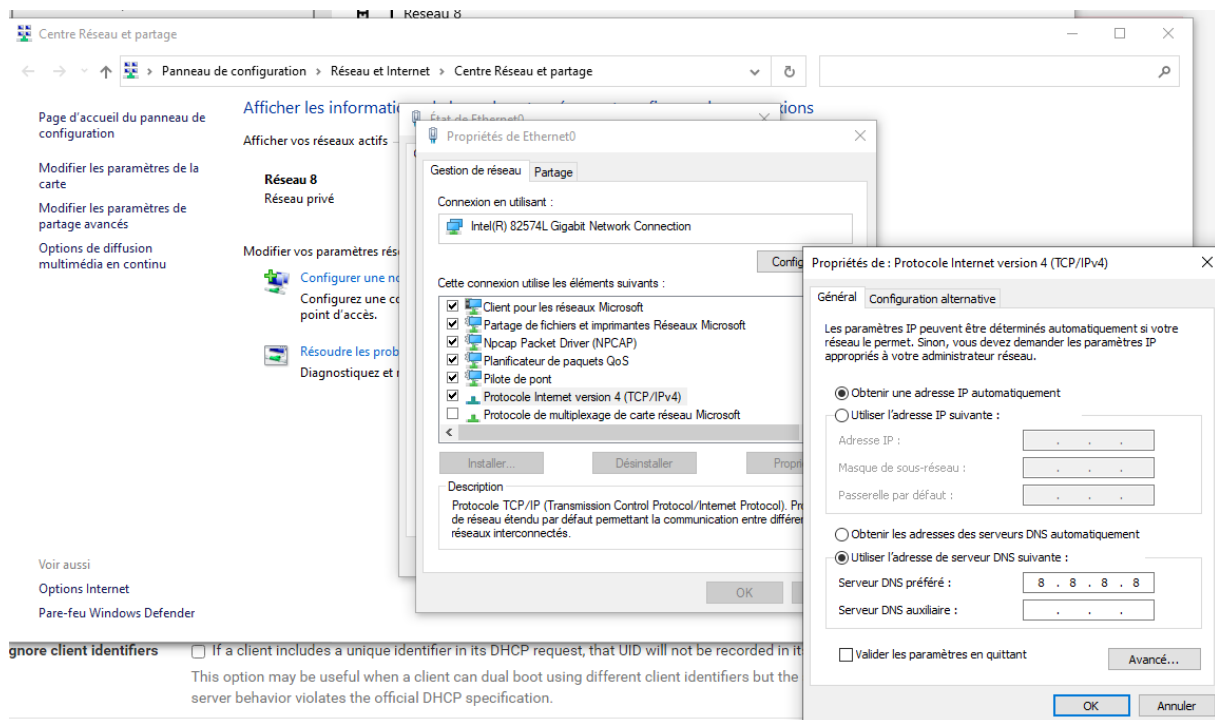
BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Enfin, on repasse notre machine cliente en DHCP



Et voilà, nous avons enfin fini l'installation et la configuration de PfSense ainsi que la machine cliente.

V) Paramétrage PfSense

PfSense est un firewall permettant de filtrer les ports voulus. Pour cette première partie, nous allons configurer une règle qui bloque n'importe quel port. Pour cela on va dans « Firewall », « Rules », « edit ».

Edit Firewall Rule

Action

Block

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.

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**.

Destination

Destination

☐ Invert match

any

Destination Address

/

Destination Port Range

any

From

Custom

any

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.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 4 / 2.05 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	*	*	*	*	*	none		Blocage de tout les ports	📌✏️🔒🗑️

Dans action, je choisi bien évidemment « block » et je mets « any » dans la source et les destinations pour tout bloquer. Après un reboot, je constate bien que je n'ai plus internet sur ma machine cliente.

Ensuite, passons à la règle qui nous permettra d'aller sur internet. Pour cela, allons re-crée une règle qui ira au dessus de celle qui bloque tout les accès (voir screen) avec les paramètres suivant :

Edit Firewall Rule

Action

Pass

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/UDP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN net

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

any

Destination Address

/

Destination Port Range

(other)

Internet

(other)

Internet

From

Custom

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.

Cette fois-ci nous voulons laisser passer la connexion, donc dans « action » nous choisissons « pass », protocole TCP/UDP, source LAN net et dans destination nous mettons l'alias qu'on a créé (que je vais vous montrer plus en détail en dessous) dans la destination. Si nous ne mettons pas cette alias, nous pourrions que faire une recherche google.

Passons à l'alias :

Firewall / Aliases / Edit

Properties

Name Internet
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
A description may be entered here for administrative reference (not parsed).

Type Port(s)

Port(s)

Hint Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

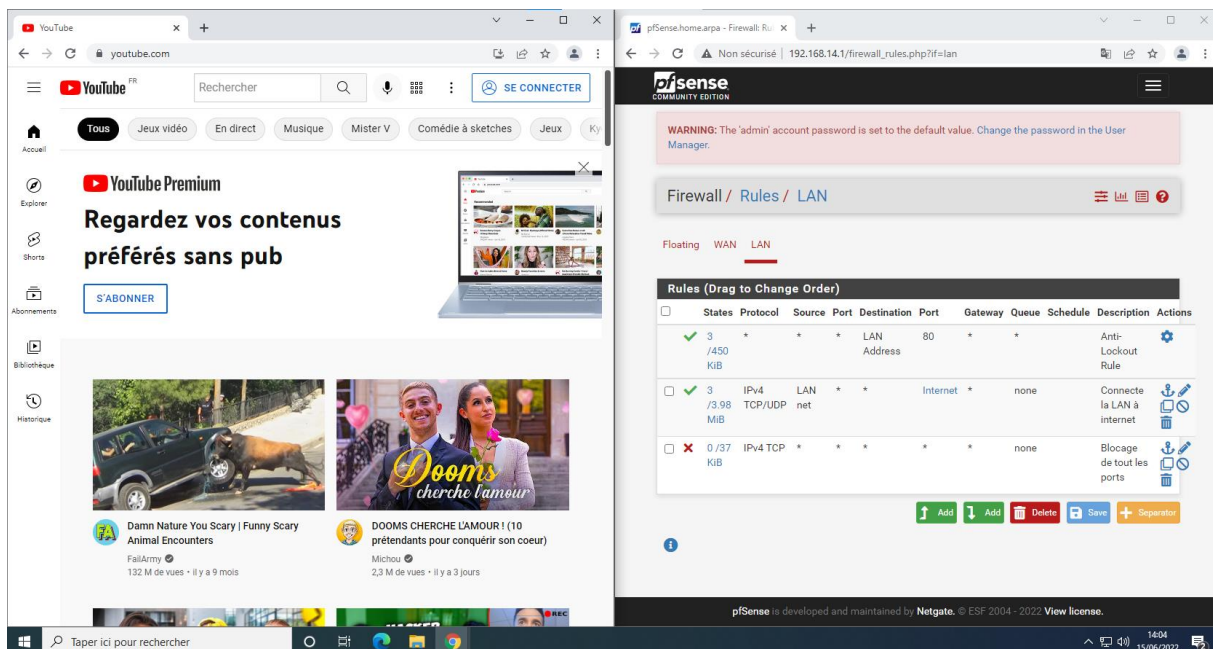
Port	Entry added	Action
80	Wed, 15 Jun 2022 11:41:51 +0000	Delete
443	Wed, 15 Jun 2022 11:41:51 +0000	Delete
53	Wed, 15 Jun 2022 11:41:51 +0000	Delete

Allons dans Firewall, Aliases, Edit et ajoutons un alias.

Comme nom, j'ai choisi Internet afin de mieux me repérer si jamais je souhaite en faire plus. En type, j'ai mis ports, car nous autorisons les ports internet. (voir screen pour les 3 ports que l'on doit laisser passer)

Et notre Aliase est créé !

Voici la preuve que je peux bien accéder à internet :



Cette dernière capture d'écran signe la fin du TP.