



Installation et configuration d'un routeur virtuel Pfsense





Table des matières

1. Définition.....	2
2. Prérequis.....	3
3. Installation.....	4
4. Configuration	10

1. Définition

Gratuit et open-source, PfSense est une pare-feu basé sur le système d'exploitation FreeBSD. Il est utilisé non seulement comme pare-feu mais également comme routeur. Le DHCP peut être activé dessus. Facile à utiliser et configurable il fournit non seulement des fonctions de routage mais permet aussi de connecter plusieurs réseaux. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. PfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

Après l'installation manuelle nécessaire pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web (appelé WebGUI) PfSense gère nativement les VLAN.

Comme sur les distributions Linux, PfSense intègre aussi un gestionnaire de paquets pour installer des fonctionnalités supplémentaires, comme un proxy ou un serveur de voix sur IP.

2. Prérequis

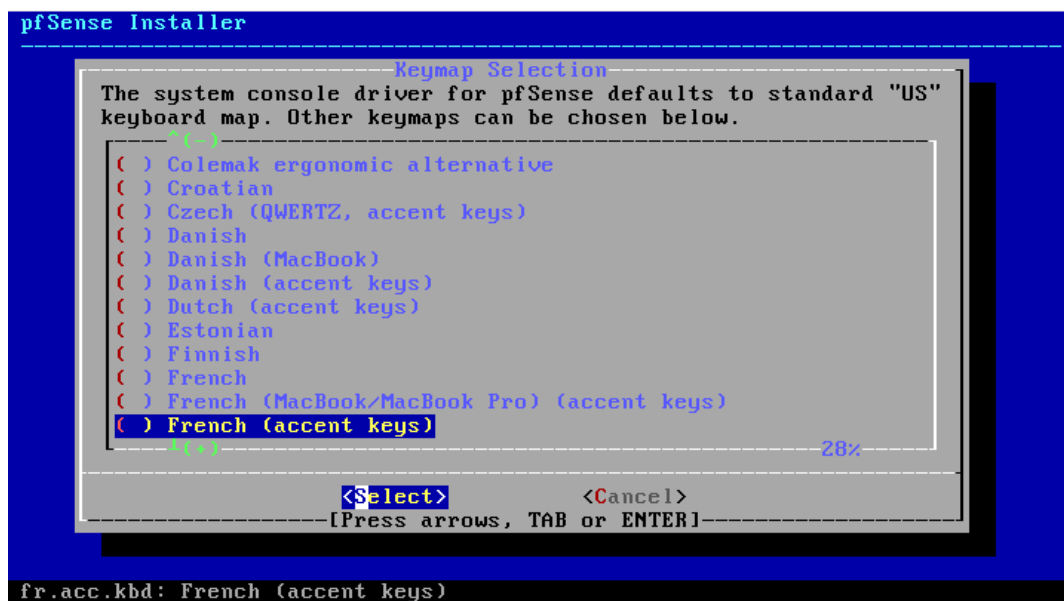
PfSense peut fonctionner sur du matériel de serveur ou domestique, sur des solutions embarquées, sans toutefois demander beaucoup de ressources ni de matériel puissant.

Notre choix a porté sur l'installation de Pfsense sur une machine virtuel sur notre hyperviseur Proxmox, se trouvant sur notre serveur. Sur notre serveur nous avons 2,5 terraoctets ainsi que 128 go de RAM. Pour la VM Pfsense nous mettrons 50 go de stockage ainsi que 8096 go de RAM pour limiter les latences.

3. Installation

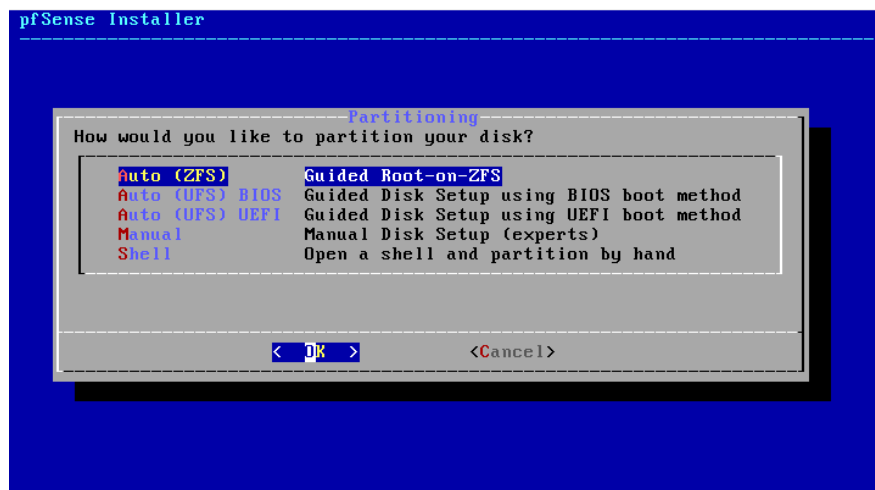
Tout d'abord, nous démarrons la machine Pfsense que nous avons créée avec l'image iso ce trouvant sur le site officiel de Pfsense.

Une fois fait, PfSense nous demande de choisir le clavier à utiliser :



Nous avons choisi le clavier Français.

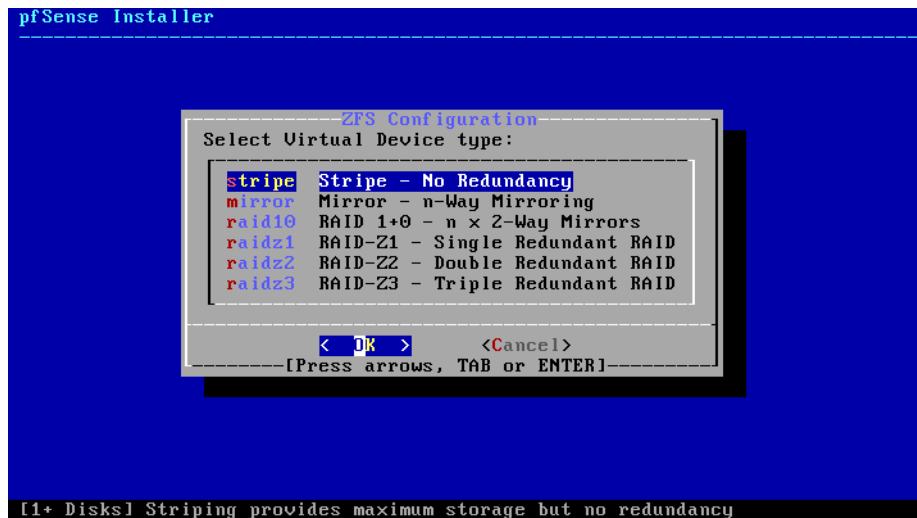
Puis nous devons choisir le format du disque dur :



Nous avons porté notre choix sur un format ZFS qui est open source et maintenu, des mises à jour régulières sont faites encore aujourd'hui.

A contrario, UFS est un ancien partitionnement qui n'est plus maintenue à jour et qui est voué à être remplacé par le ZFS.

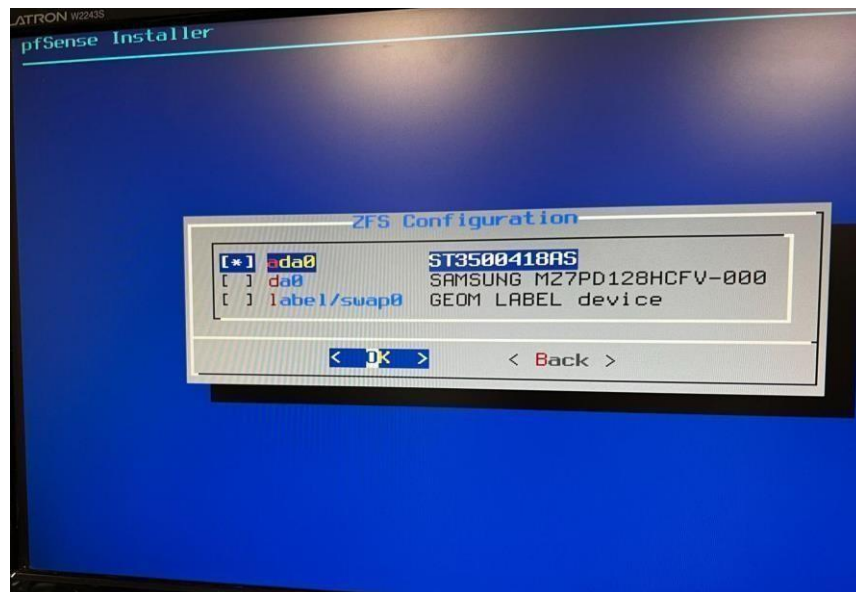
Viens ensuite le choix de redondance de données :



N'ayant qu'un seul disque dur dans notre machine, nous avons donc utilisé l'option stripe, qui ne fait pas de redondance.

Avec plus de moyen, il aurait été préférable de faire une redondance sur un deuxième disque.

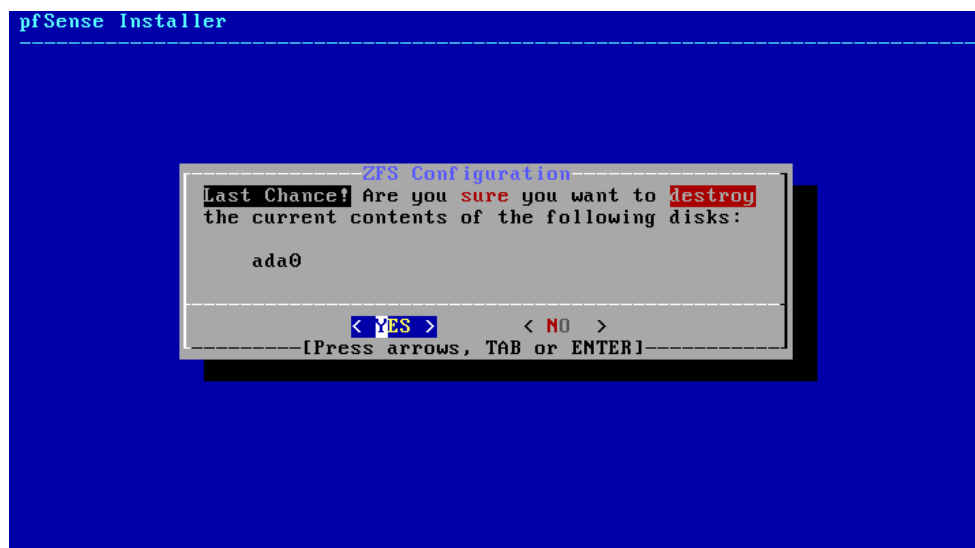
Viens alors le choix de disque sur lequel installer l'OS :



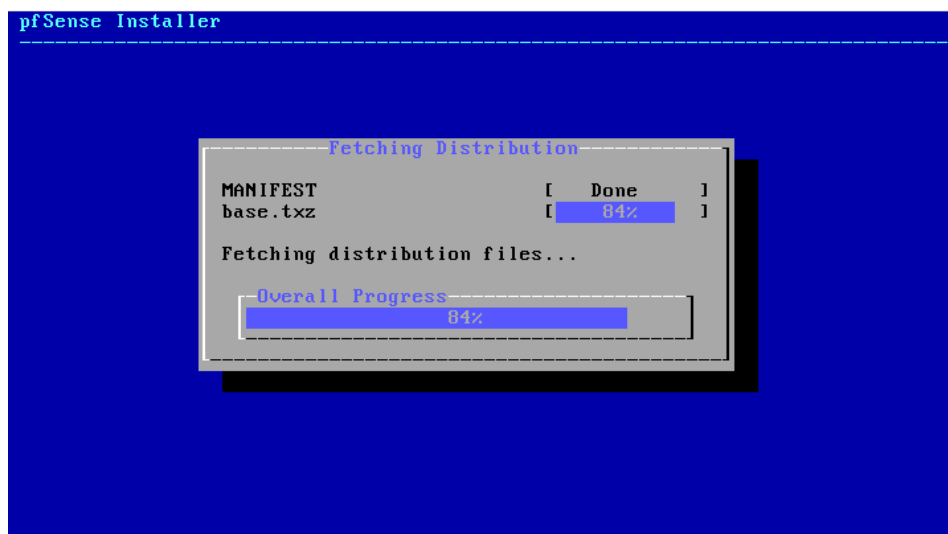
ici, ada0 est le disque de notre serveur

label/swap0 est le fichier de swap créé suite à la redondance de données

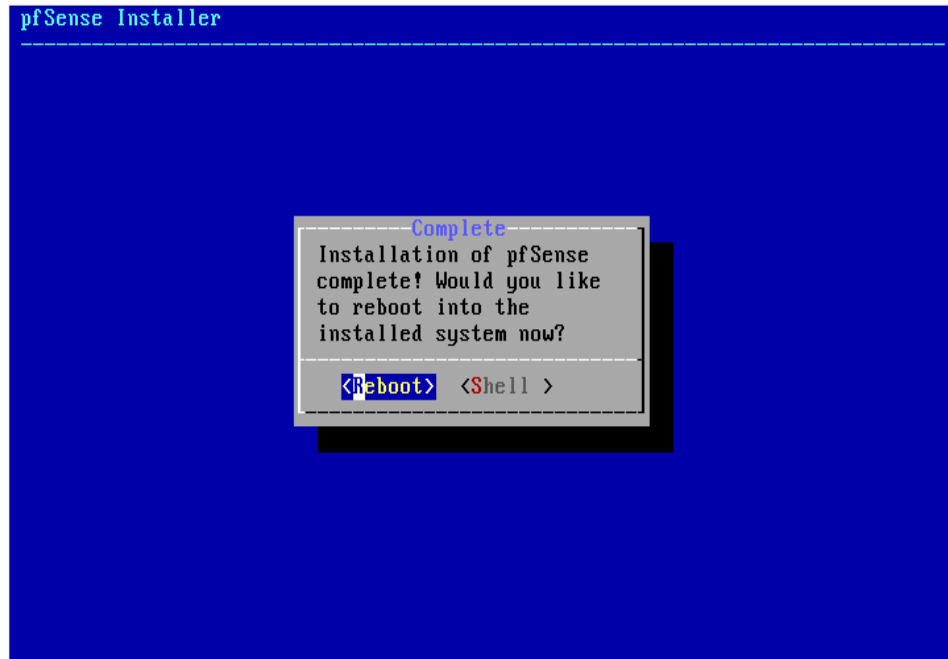
PfSense demande alors si nous sommes sûrs de notre choix car cela va écraser les données sur le disque dur :



Une fois validé, l'installation se lance :



Afin de finaliser l'installation, PfSense doit redémarrer :



PfSense est maintenant installé et il ne reste que la configuration :

4. Configuration

Une fois sur l'écran principal de PfSense, nous devons configurer l'interface LAN, pour ce faire nous allons sélectionner l'option 2, qui permet de paramétrer les interfaces :

```
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 309969253ab04587eae

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.110.201/24
LAN (lan)      -> em1      -> v4: 172.32.16.0/16

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: 
```

Une fois le LAN sélectionné, PfSense demande l'adresse IP :

```
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: 2

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - static)

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1
```

ici, nous avons mis l'adresse IP 192.168.1.1 pour notre LAN

Viens alors le choix du masque IP que nous allons mettre en 255.255.255.0 car décision du client :

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

24 correspond au masque 255.255.255.0

Une fois le masque choisi, PfSense nous demande une passerelle, mais ceci ne concerne pas le LAN, nous passons donc à l'étape suivante.

Puis vient la configuration en IPv6, que nous n'allons pas utiliser, et enfin, nous n'utiliserons pas le DHCP de PfSense, nous pouvons alors le désactiver :

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 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...
```

Une fois validé voici l'écran :

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

The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://192.168.1.1/
Press <ENTER> to continue.
```

```

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.110.201/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

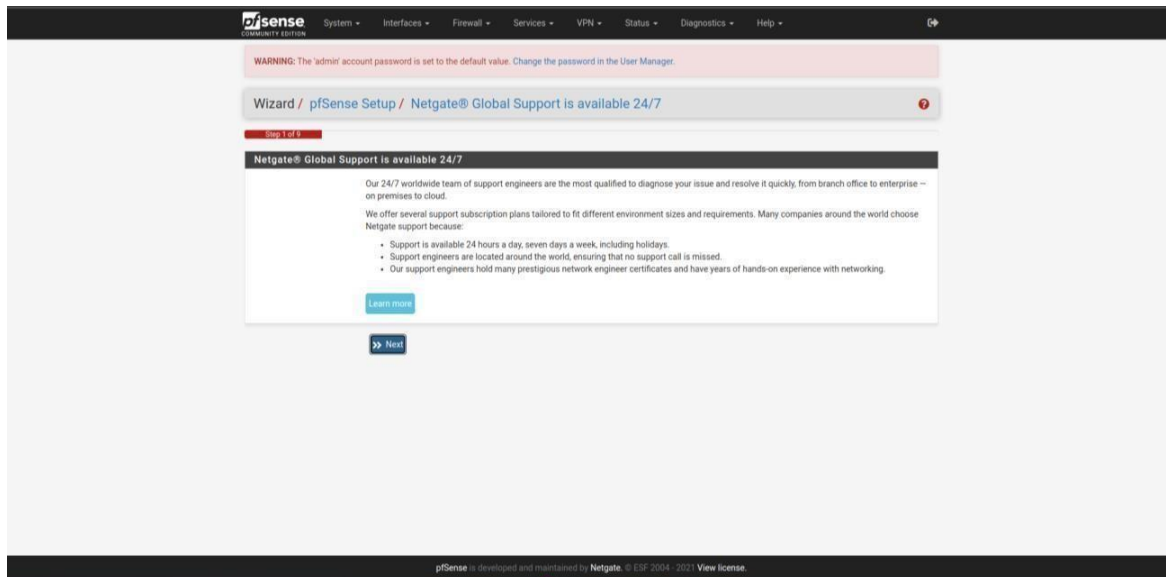
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option:

```

ici, PfSense nous montre bien la nouvelle adresse enregistré sur le LAN

Nous allons ensuite nous connecter à l'interface Web de PfSense en tapant l'adresse IP 192.168.1.1 sur un navigateur Web :



Après s'être connecté à PfSense grâce aux login et mots de par défaut que nous changerons par la suite, nous pouvons commencer les configurations.

PfSense nous propose de configurer l'IP du LAN, mais comme nous l'avons fait directement dans la configuration, nous pouvons passer cette étape :

The screenshot shows the 'Configure WAN Interface' wizard in pfSense. At the top, there is a navigation bar with links to System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: 'WARNING: The admin account password is set to the default value. Change the password in the User Manager.' Below this, the breadcrumb trail reads 'Wizard / pfSense Setup / Configure WAN Interface'. A progress bar indicates 'Step 4 of 6'. The main section is titled 'Configure WAN Interface' and contains the following fields:

- SelectedType:** A dropdown menu set to 'Static'.
- General configuration:**
 - MAC Address:** A text field with a note: '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: xx:xx:xx:xx:xx:xx or leave blank.'
 - MTU:** A text field with a note: 'Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.'
 - MSS:** A text field with a note: 'If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.'
- Static IP Configuration:**
 - IP Address:** A text field containing '192.168.1.10.201'.
 - Subnet Mask:** A dropdown menu set to '24'.
 - Upstream Gateway:** A text field.
- DHCP client configuration:**
 - DHCP Hostname:** A text field.

The screenshot shows the 'Configure LAN Interface' wizard in pfSense. At the top, there is a navigation bar with links to System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: 'WARNING: The admin account password is set to the default value. Change the password in the User Manager.' Below this, the breadcrumb trail reads 'Wizard / pfSense Setup / Configure LAN Interface'. A progress bar indicates 'Step 4 of 6'. The main section is titled 'Configure LAN Interface' and contains the following fields:

- LAN IP Address:** A text field containing '192.168.1.1' with a note: 'Type dhcp if this interface uses DHCP to obtain its IP address.'
- Subnet Mask:** A dropdown menu set to '24'.

At the bottom of the form, there is a blue button labeled 'Next'.

Viens ensuite le changement de mot de passe administrateur :

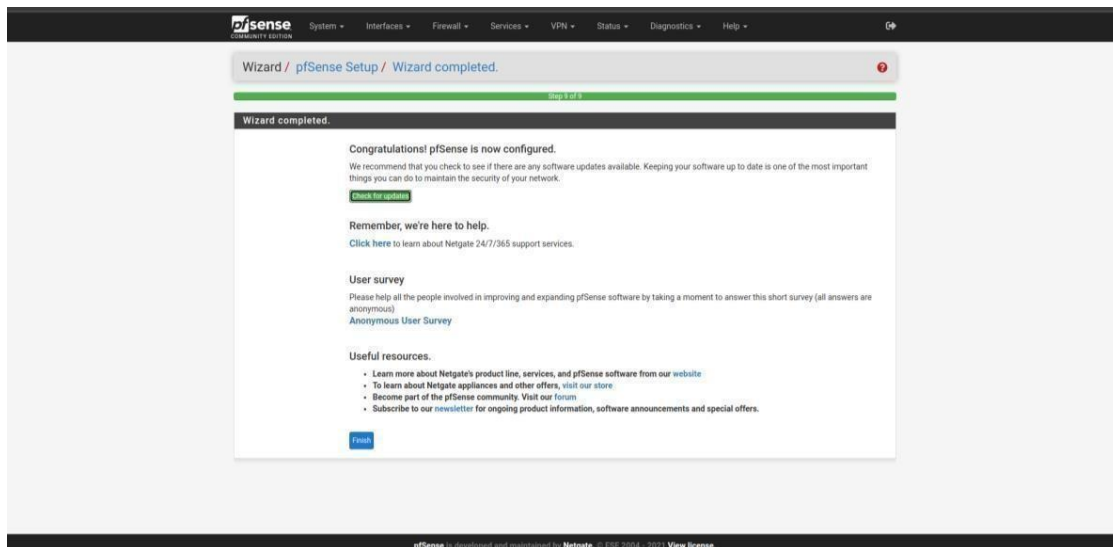
The screenshot shows the pfSense WebGUI interface. At the top, there's a navigation bar with links like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below this, a warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area is titled "Wizard / pfSense Setup / Set Admin WebGUI Password" and indicates it's "Step 6 of 8". The section is labeled "Set Admin WebGUI Password" and contains the instruction: "On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled." There are two password input fields: "Admin Password" and "Admin Password AGAIN", both with masked characters. A "Next" button is located at the bottom of the form. The footer of the page reads: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license."

Par mesure de sécurité, nous avons généré un mot de passe à 16 caractères aléatoires avec des chiffres, des caractères spéciaux et des lettres.

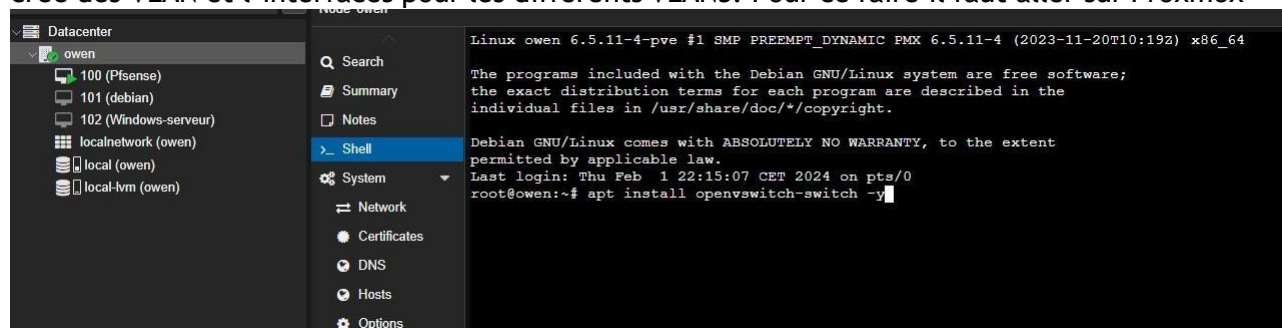
Ne reste alors qu'à valider les paramètres entrés :

The screenshot shows the pfSense WebGUI interface at the "Reload configuration" step of the wizard. The navigation bar is the same as in the previous screenshot. The main content area is titled "Wizard / pfSense Setup / Reload configuration" and indicates it's "Step 7 of 8". The section is labeled "Reload configuration" and contains the instruction: "Click 'Reload' to reload pfSense with new changes." There is a single "Reload" button at the bottom of the form. The footer of the page reads: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license."

PfSense nous montre avec cet écran qu'il a bien enregistré la configuration et est opérationnel :

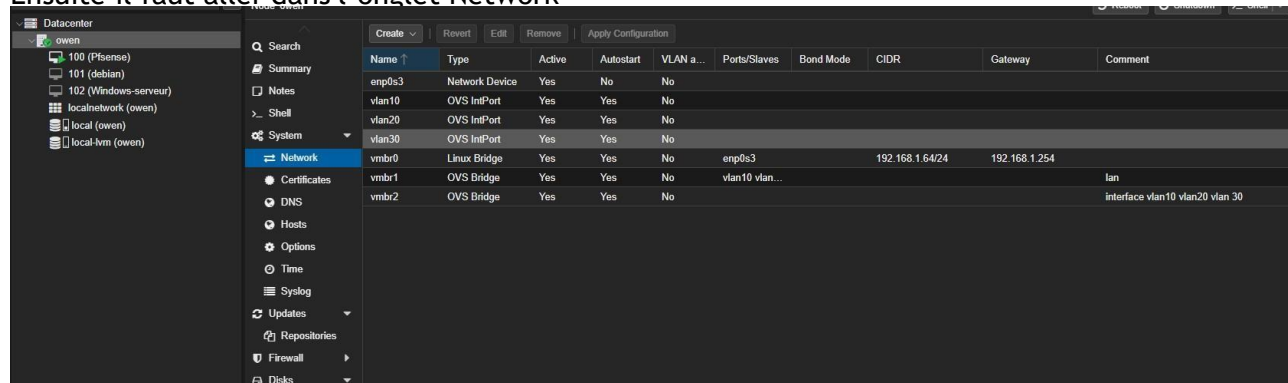


Ensuite nous allons maintenant passer à la configuration et au bon fonctionnement du LAN et crée des VLAN et l'interfaces pour les différents VLANs. Pour ce faire il faut aller sur Proxmox



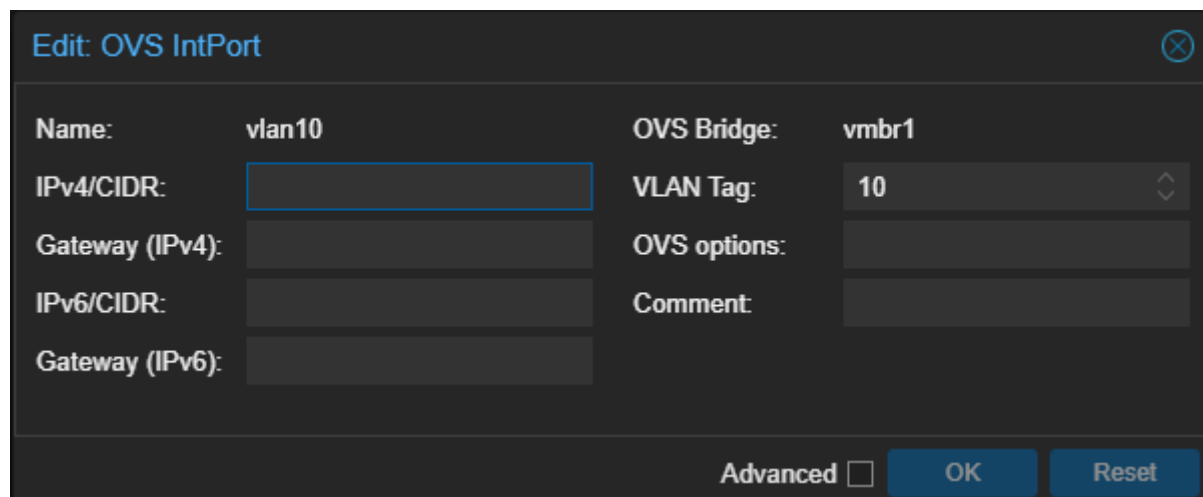
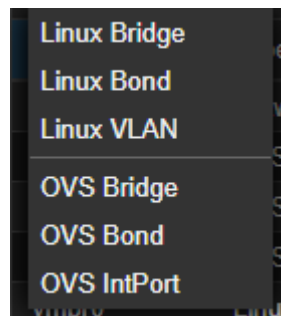
Installer openvswitch-switch

Ensuite il faut aller dans l'onglet Network



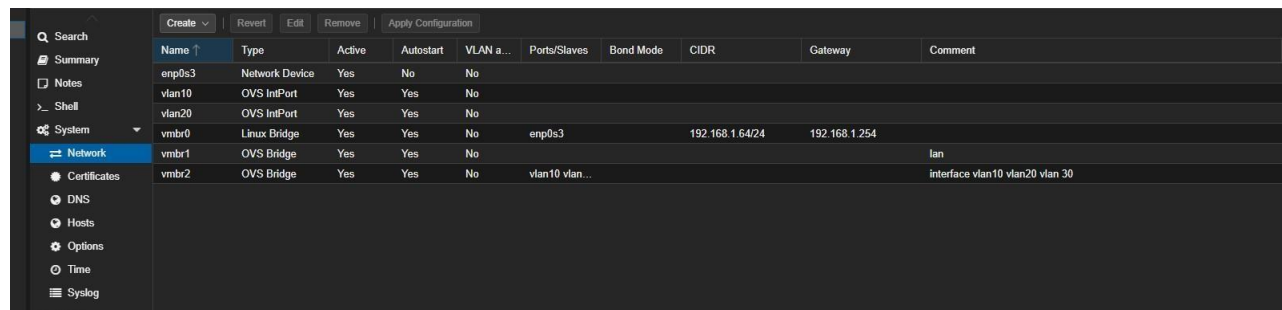
Il faut cliquer sur Create et OVS bridge pour crée des interfaces réseau supplémentaires il faut en crée deux une pour le LAN et une pour les VLAN .

Il faut ensuite crée les vlan pour cela il faut cliquer sur OVS INPORT



Il faut crée le Vlan en le nommant et en le taguant avec le bon numéro correspondant au VLAN

Répéter cela pour les autres VLAN en les mettant sur la bonne interfaces réseau en mettant le tag 20 et 30.

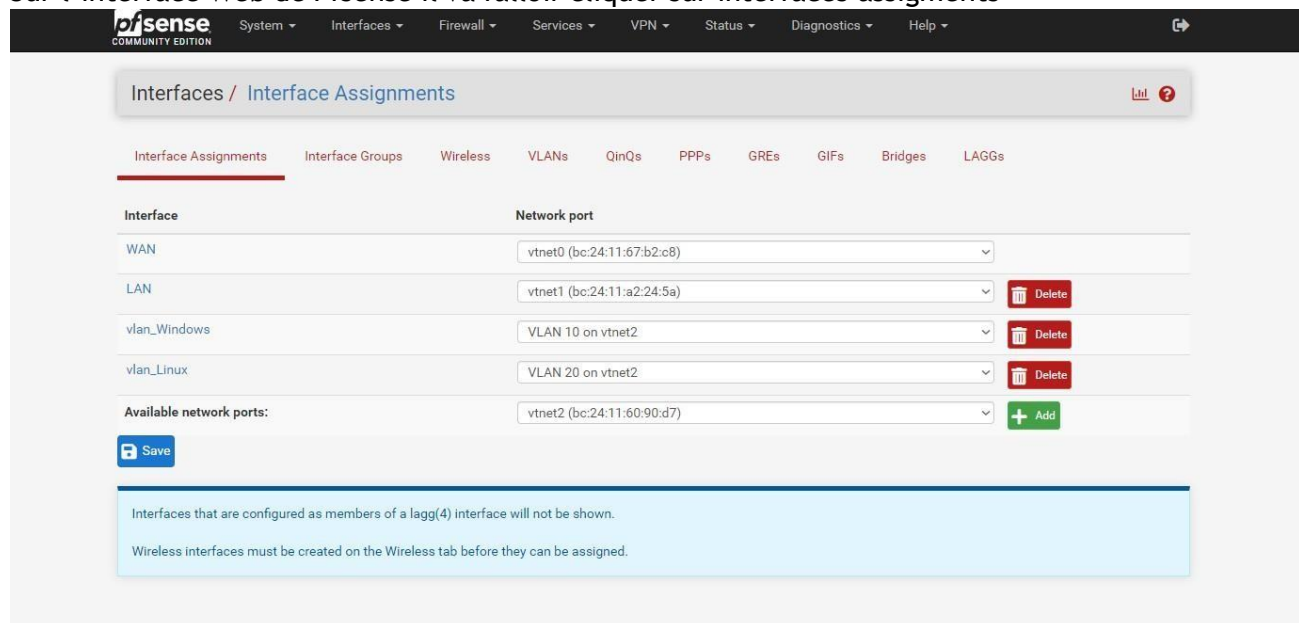


Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
enp0s3	Network Device	Yes	No	No					
vlan10	OVS IntPort	Yes	Yes	No					
vlan20	OVS IntPort	Yes	Yes	No					
vmbr0	Linux Bridge	Yes	Yes	No	enp0s3		192.168.1.64/24	192.168.1.254	
vmbr1	OVS Bridge	Yes	Yes	No					lan
vmbr2	OVS Bridge	Yes	Yes	No	vlan10 vlan...				interface vlan10 vlan20 vlan 30

Une fois tout cela crée il faut cliquer sur la machine Pfsense pour lui attribuer les interfaces réseau.

Cliquer sur ADD network device et choisir premièrement le Vmbr1 pour l'interfaces LAN et refaire la manipulation avec le Vmbr2 pour les interfaces Vlan.

Sur l'interface Web de Pfsense il va falloir cliquer sur interfaces assignments



Interfaces / Interface Assignments

Interface Assignments | Interface Groups | Wireless | VLANs | QinQs | PPPs | GREs | GIFs | Bridges | LAGGs

Interface	Network port	
WAN	vtnet0 (bc:24:11:67:b2:c8)	
LAN	vtnet1 (bc:24:11:a2:24:5a)	Delete
vlan_Windows	VLAN 10 on vtnet2	Delete
vlan_Linux	VLAN 20 on vtnet2	Delete
Available network ports:	vtnet2 (bc:24:11:60:90:d7)	+ Add

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

Ensuite il va falloir cliquer sur LAN

General Configuration

Enable ☒ Enable interface

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

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
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
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 /

IPv4 Upstream gateway [+ Add a new gateway](#)

Il faut activer l'interface LAN mettre la configuration IPV4 en Static et mettant l'adresse ip de la passerelle en /24 ici nous aurons 192.168.5.1/24 nous cliquons sur Save et on applique les changements.

Interfaces			
	WAN	↑ 10Gbase-T <full-duplex>	192.168.1.105 2001:861:3248:3ab0:be24:11ff:fe67:b2c8
	LAN	↑ 10Gbase-T <full-duplex>	192.168.5.1

Nous avons l'interface Lan fonctionnel maintenant nous allons créer les VLANs pour cela nous allons dans interfaces assignments et nous cliquons sur VLANs

Interfaces / [Interface Assignments](#)

[Interface Assignments](#) [Interface Groups](#) [Wireless](#) [VLANs](#) [QinQs](#) [PPPs](#) [GREs](#) [GIFs](#) [Bridges](#) [LAGGs](#)

Nous cliquons sur Add on sélectionne vtnet2, nous mettons le tag ici le 10 nous pouvons mettre une priorité si nous en avons plusieurs et en dessous ajouter une description du vlan si nous souhaitons.

VLAN Configuration

Parent Interface

vtnet2 (bc:24:11:60:90:d7)

Only VLAN capable interfaces will be shown.

VLAN Tag

10

802.1Q VLAN tag (between 1 and 4094).

VLAN Priority

0

802.1Q VLAN Priority (between 0 and 7).

Description

Description

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

Nous avons donc crée un vlan nous en créons un deuxième pour ce faire pareil que pour la premier nous sélectionnons le vtnet2, on tag le vlan ici 20, pas de priorité ici et pas de descriptions.

Interfaces / VLANs

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
vtnet2	10			
vtnet2	20			

+ Add

Nous avons bien deux VLANs.

Maintenant il faut retourner sur interfaces assignment

Nous ajoutons nos VLans que nous venons de crée

Available network ports: vtnet2 (bc:24:11:60:90:d7) + Add

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface	Network port
WAN	vtnet0 (bc:24:11:67:b2:c8)
LAN	vtnet1 (bc:24:11:a2:24:5a)
vlan_Windows	VLAN 10 on vtnet2
vlan_Linux	VLAN 20 on vtnet2

Available network ports: vtnet2 (bc:24:11:60:90:d7) + Add

Save

Ensuite nous activons l'interfaces VLANs, nous la mettons en static IPv4 nous mettons la passerelle ici nous avons mis 192.168.10.1/24

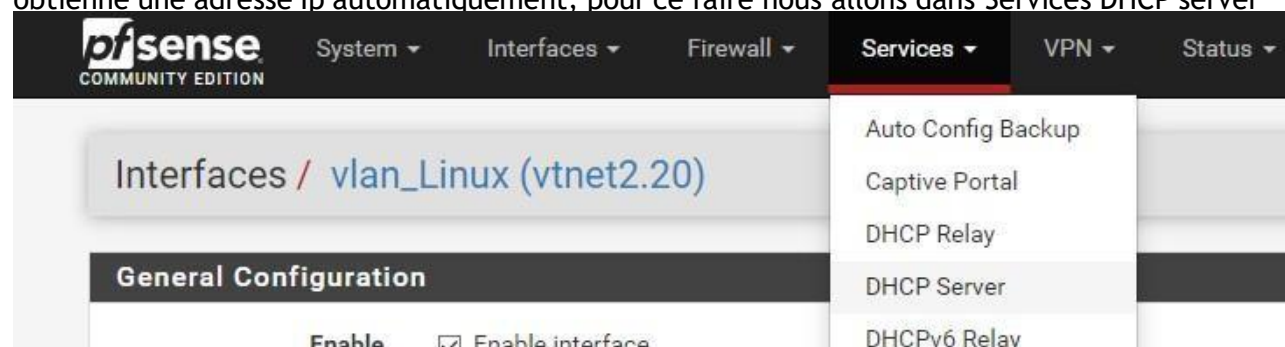
General Configuration	
Enable	☒ Enable interface
Description	vlan_Windows Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx The MAC address of a VLAN interface must be set on its parent interface
MTU	 If this field 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	192.168.10.1 / 24
IPv4 Upstream gateway	None + Add a new gateway 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 .

Ensuite nous faisons la même chose pour le vlan suivant celui-ci

General Configuration	
Enable	☒ Enable interface
Description	vlan_Linux Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx The MAC address of a VLAN interface must be set on its parent interface
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.

Maintenant nous allons aller activé le DHCP pour que toutes les machine étant dans un Vlan obtienne une adresse Ip automatiquement, pour ce faire nous allons dans Services DHCP server



Nous sélectionnons l'interface sur laquelle nous voulons nous mettre le DHCP ici nous nous mettons sur le VLAN 20 (vlan_linux)

Il faut activé le DHCP en mettre une range d'Ip sur laquelle qui correspond aux IP disponible sur le VLAN ici nous avons 192.168.20.100 à 192.168.20.200 nous pouvons mettre n'importe quelle range de 192.168.20.2 à 192.168.20.253.

LAN VLAN_WINDOWS **VLAN_LINUX**

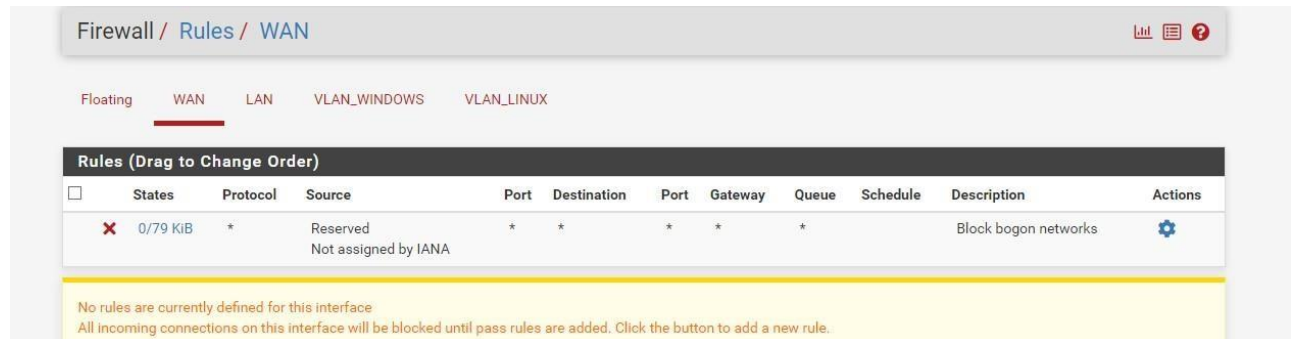
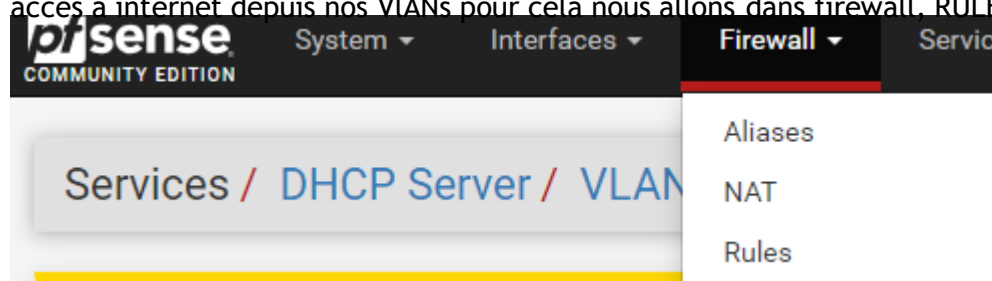
General DHCP Options

DHCP Backend	ISC DHCP
Enable	☒ Enable DHCP server on VLAN_LINUX interface
BOOTP	☐ Ignore BOOTP queries
Deny Unknown Clients	Allow all 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 in a static mapping 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 in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients	☐ Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet	192.168.20.0/24	
Subnet Range	192.168.20.1 - 192.168.20.254	
Address Pool Range	192.168.20.100 From	192.168.20.200 To
The specified range for this pool must not be within the range configured on any other address pool for this interface.		
Additional Pools	+ Add Address Pool If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	

Le DHCP est bien activé maintenant nous pouvons mettre en place les règle de trafic pour avoir accès à internet depuis nos VLANs pour cela nous allons dans firewall. RULES



Il faut trois règle en tout une sur la LAN, une sur le VLAN10 (windows) et une sur le VLAN20 (Linux) Aucune règle sur le WAN.

Pour faire une règle il faut cliquer sur Add :

Il faut faire cette règle là pour les trois :

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: Any
Choose which IP protocol this rule should match.

Source:
Source: ☐ Invert match LAN subnets Source Address: /

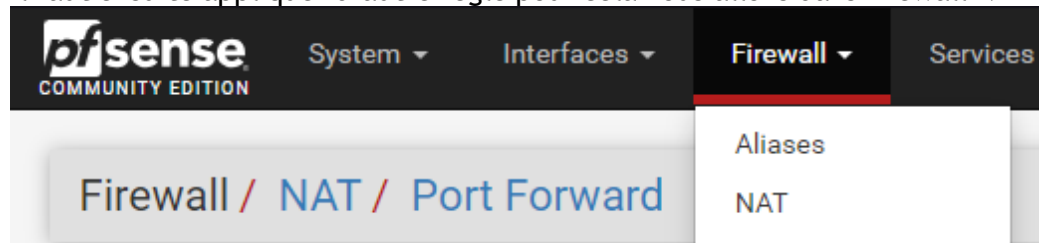
Destination:
Destination: ☐ Invert match Any Destination Address: /

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).

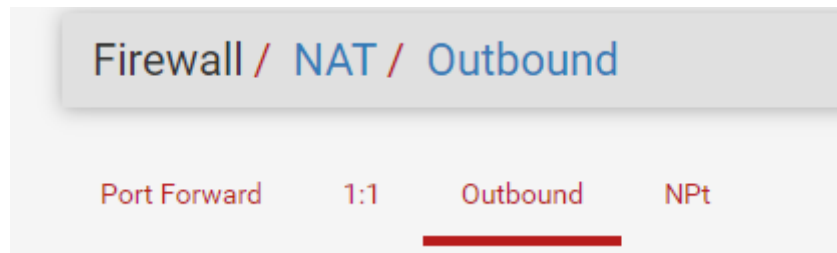
Description: Default allow LAN to any rule
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: [Display Advanced](#)

Il faut ensuite appliquer d'autre règle pour cela nous allons dans firewall NAT

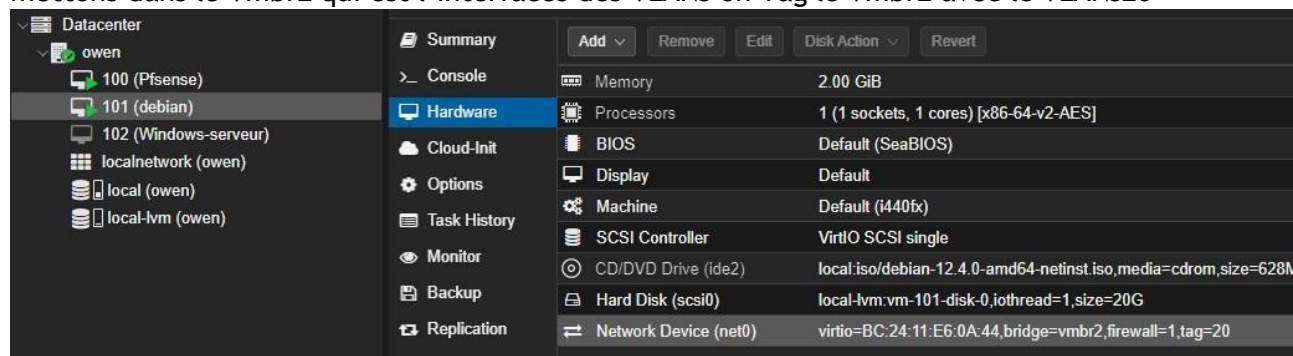


Et sur Outbound



Nous sélectionnons le premier mode Automatic outbound NAT nous sauvegardons et appliquons les changements.

Une fois cela fait il ne nous reste plus qu'à tester en mettant une machine virtuelle dans un Vlan. Pour cela nous prenons une machine debian et nous le mettons dans le bon Vmbr ici nous la mettons dans le Vmbr2 qui est l'interface des VLANs on Tag le Vmbr2 avec le VLANs20



Nous allumons la machine et nous faisons trois commande un ip a pour voir si le DHCP donne bien une adresse ip :

```
root@deb-test:~# ip a
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether bc:24:11:e6:0a:44 brd ff:ff:ff:ff:ff:ff
  altname enp0s18
  inet 192.168.20.100/24 brd 192.168.20.255 scope global dynamic ens18
    valid_lft 4565sec preferred_lft 4565sec
  inet6 fe80::be24:11ff:fee6:a44/64 scope link
```

Il sors bien avec une Ip compris dans le DHCP

Un ping vers la passerelle pour voir si cela fonctionne bien.

```
root@deb-test:~# ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=0.935 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=0.895 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=64 time=0.803 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=64 time=0.741 ms
64 bytes from 192.168.20.1: icmp_seq=5 ttl=64 time=0.886 ms
64 bytes from 192.168.20.1: icmp_seq=6 ttl=64 time=0.816 ms
64 bytes from 192.168.20.1: icmp_seq=7 ttl=64 time=0.901 ms
^C
--- 192.168.20.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6025ms
rtt min/avg/max/mdev = 0.741/0.853/0.935/0.063 ms
```

Nous faisons ensuite une commande pour savoir si la machine sors bien sur internet ici :

```
root@deb-test:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
4 bytes from 1.1.1.1: icmp_seq=22 ttl=56 time=8.15 ms
4 bytes from 1.1.1.1: icmp_seq=23 ttl=56 time=6.91 ms
4 bytes from 1.1.1.1: icmp_seq=24 ttl=56 time=6.13 ms
4 bytes from 1.1.1.1: icmp_seq=25 ttl=56 time=6.35 ms
4 bytes from 1.1.1.1: icmp_seq=26 ttl=56 time=7.12 ms
4 bytes from 1.1.1.1: icmp_seq=27 ttl=56 time=6.36 ms
4 bytes from 1.1.1.1: icmp_seq=28 ttl=56 time=7.21 ms
4 bytes from 1.1.1.1: icmp_seq=29 ttl=56 time=6.26 ms
4 bytes from 1.1.1.1: icmp_seq=30 ttl=56 time=7.74 ms
4 bytes from 1.1.1.1: icmp_seq=31 ttl=56 time=7.51 ms
4 bytes from 1.1.1.1: icmp_seq=32 ttl=56 time=5.46 ms
4 bytes from 1.1.1.1: icmp_seq=33 ttl=56 time=4.60 ms
^C
-- 1.1.1.1 ping statistics --
3 packets transmitted, 12 received, 63.6364% packet loss, time 32795ms
rtt min/avg/max/mdev = 4.595/6.649/8.152/0.957 ms
root@deb-test:~# _
```

Nous sortons bien sur internet la commande est donc fonctionnel

Nous avons donc bien installé et configuré Pfsense