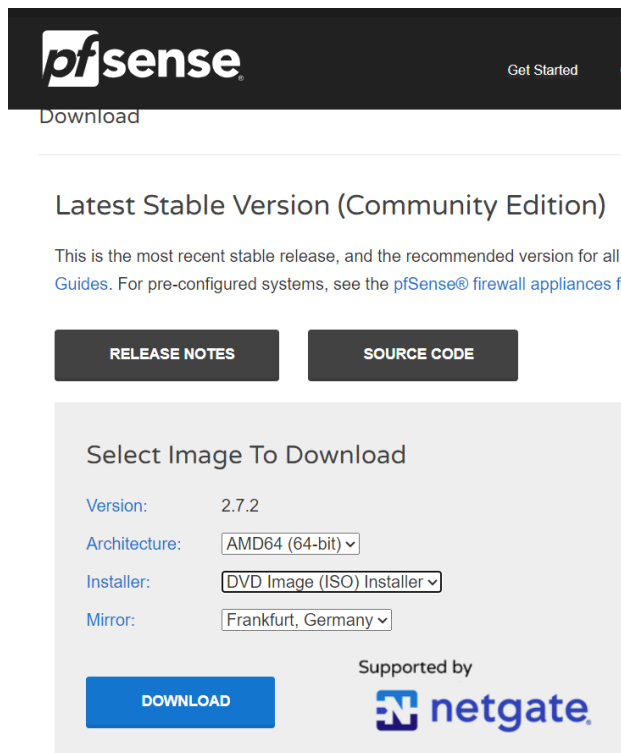


## TP pare-feu Pfsense

Intro :

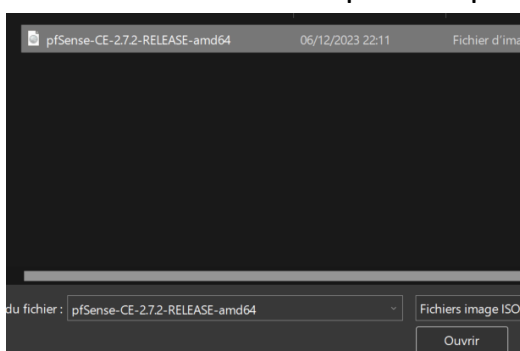
Aujourd'hui nous allons installer un pare-feu sur nos vm windows server et client pour filtrer les communications douteuses sur nos appareils et ainsi les protéger d'éventuelles attaques extérieures.

Tout d'abord nous allons télécharger l'iso de Pfsense (le firewall que nous allons utiliser)

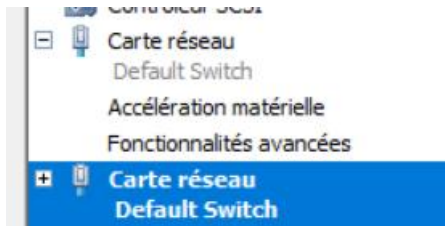


Et nous allons installer l'iso sur une nouvelle vm configuré comme dans les précédents tp à quelques exceptions près :

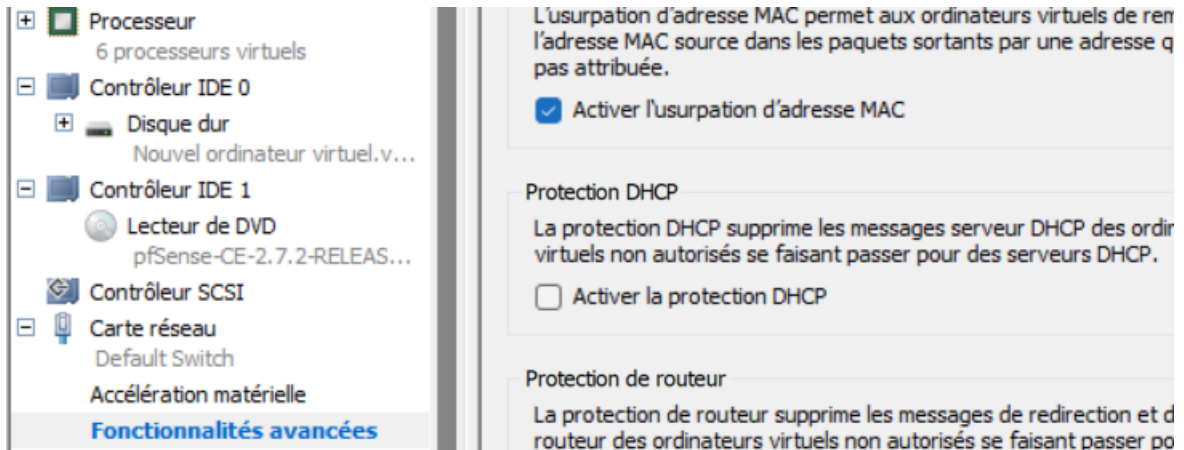
On va utiliser l'iso pfsense pour l'installer directement sur notre vm



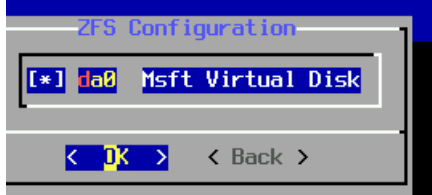
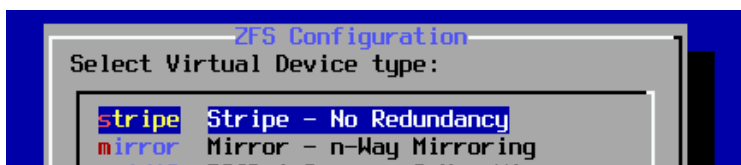
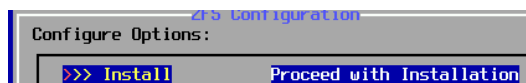
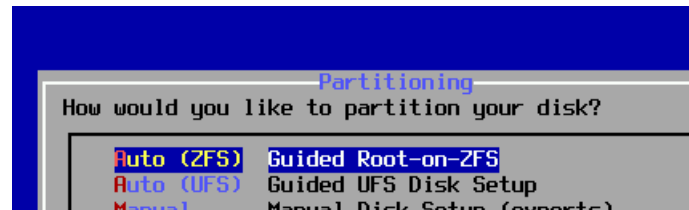
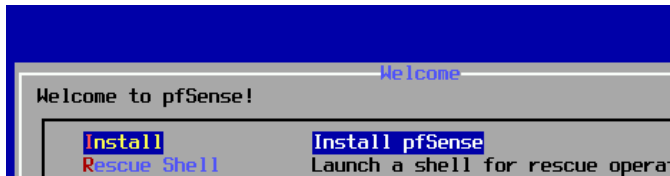
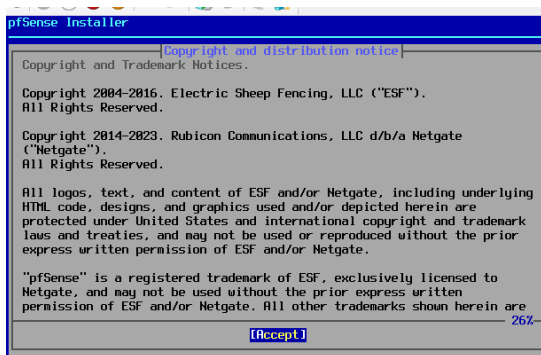
Puis dans les paramètres de notre VM on va y ajouter une deuxième carte réseau



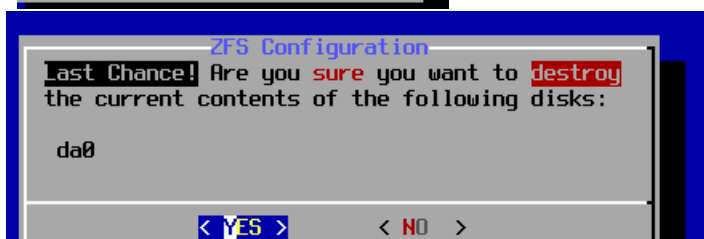
On a bien nos deux cartes et il faut juste dans les fonctionnalités avancées cocher la case d'usurpation d'adresse mac



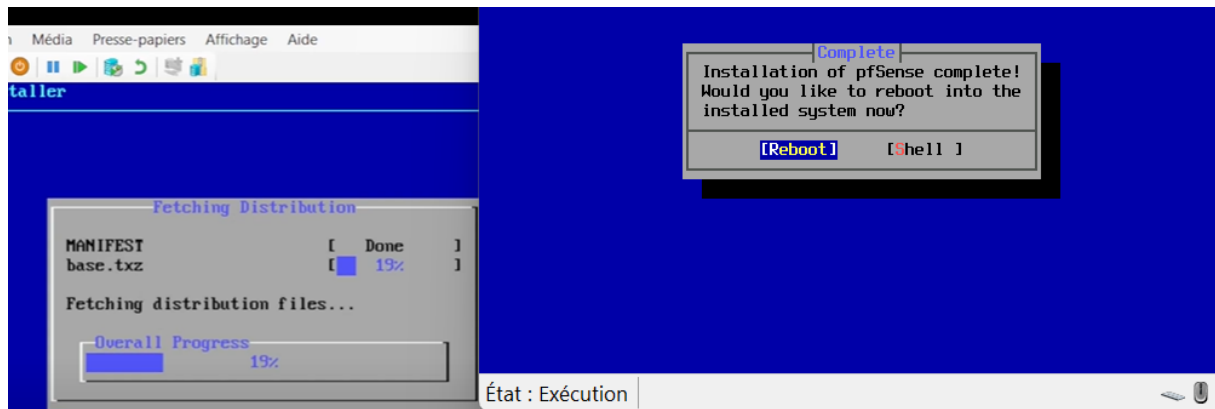
Une fois la vm lancée on va suivre les étapes suivantes :



Appuyez sur espace pour sélectionner



Une fois le téléchargement fait il suffira de reboot le système en sortant l'iso du cycle de démarrage car il est déjà installé.



UN fois relancée une première question nous est posé on répondra simplement non car nous avons une carte réseau physique avec un petit n pour non

```
hn0 00:15:5d:90:09:0c (down) Hyper-V Network Interface
hn1 00:15:5d:90:09:0d (down) Hyper-V Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [yn]? 2024-02-16T08:25:37.458608+00:00 - php-fpm 394
- - /rc.linkup: Ignoring link event during boot sequence.
2024-02-16T08:25:37.458608+00:00 - php-fpm 395 - - /rc.linkup: Ignoring link event
during boot sequence.
```

Pour la prochaine question on va attribuer le lan et wan a chaque carte réseau installé hn0 pour le lan et hn1 pour le wan dans notre cas

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a): hn1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn0 a or nothing if finished): hn0

The interfaces will be assigned as follows:

WAN -> hn1
LAN -> hn0

Do you want to proceed [yn]? y
```

Une fois fini on pourra voir les ip de nos carte réseaux pour pouvoir y accéder via l'interface web

```
Trimming the zpool... done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

Microsoft Azure - Netgate Device ID: 4aa3234c3231f3b21c2b

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

WAN (wan)      -> hn0      -> v4/DHCP4: 172.18.212.128/20
LAN (lan)      -> hn1      -> 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: 2
```

Puis on va choisir de changer l'adresse ipv4 nous même

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

WAN (wan)      -> hn0      -> v4/DHCP4: 172.18.212.128/20
LAN (lan)      -> hn1      -> 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: 2

Available interfaces:
1 - WAN (hn0 - dhcp, dhcp6)
2 - LAN (hn1 - static)

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

Configure IPv4 address LAN interface via DHCP? (y/n) n
```

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

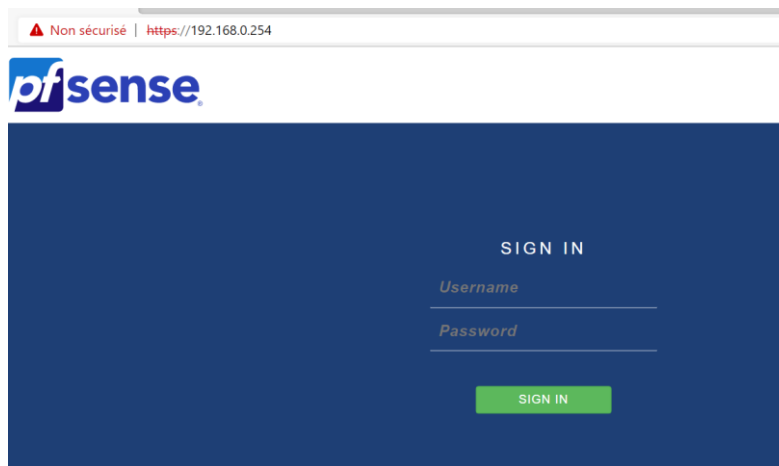
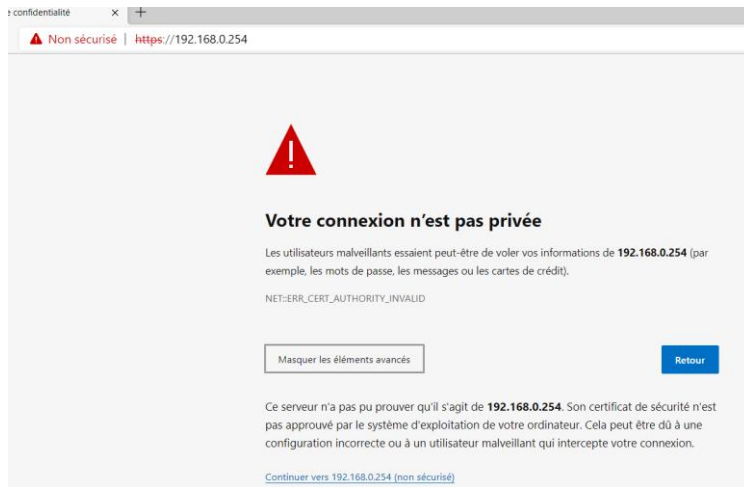
Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.0.254
```

192.168.0.254/24 sera notre ip

Ensuite on dira non aux autres paramètres. Et en faisant entrer on va revenir aux options de bases on peut maintenant se rendre sur une vm connectée à se même réseau pour ce faire on utilisera la vm Windows 10 pro créer dans un tp précédent.

Une fois sur la vm on va ouvrir un navigateur et se rendre sur l'ip correspondante et faire continuer si on est bloqué.



Puis on arrive sur une interface pour se login avec les identifiants par défaut admin et pfsens (changeable si besoin).

Une fois sur la plateforme on va faire suivant et commencer le paramétrage des différentes chose demandé.

On this screen the general pfSense parameters will be set.

Hostname	<input type="text" value="pfsense"/>	Name of the firewall host, without domain part. Examples: pfsense, firewall, edgfw
Domain	<input type="text" value="sio.local"/>	Domain name for the firewall. Examples: home.arpa, example.com  Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
Primary DNS Server	<input type="text" value="192.168.0.1"/>	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.
Secondary DNS Server	<input type="text"/>	
Override DNS	<input checked="" type="checkbox"/>	Allow DNS servers to be overridden by DHCP/PPP on WAN

[Next](#)

Il a donc fallu remplir le nom du server donc de la vm le nom du domaine active directory et l'adresse de notre dns toutes ces infos qui ont été utilisés les tp précédents.

Ensuite on règle l'heure

**Time Server Information**

Please enter the time, date and time zone.

**Time server hostname**   
Enter the hostname (FQDN) of the time server.

**Timezone**

[» Next](#)

Puis lors de la prochaine étape on ne touchera à rien et on laissera tout en dhcp.

**Configure WAN Interface**

On this screen the Wide Area Network information will be configured.

**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 c in the following format: xx:xx:xx:xx:xx:xx or leave blank.

**MTU**   
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 ot assumed.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/I this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumec MTU value in most all cases.

**Static IP Configuration**

De même pour l'adresse ip lan changée plus tôt.

**Configure LAN Interface**

On this screen the Local Area Network information will be configured.

**LAN IP Address**   
Type dhcp if this interface uses DHCP to obtain its IP address.

**Subnet Mask**

[» Next](#)

Ensuite on va créer un mot de passe : ici Azerty123 fera l'affaire pour nos test

### Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI

**Admin Password**

**Admin Password AGAIN**

Puis on pourra mettre l'interface à jour

**Step 7 of 9**

## Reload configuration

Click 'Reload' to reload pfSense with new changes.

[➔ Reload](#)

Une fois notre page rechargé on peut voir en bas à droite que nos lan et wan sont bien présent et fonctionnels

The screenshot shows the pfSense web interface. On the left, the 'System' tab is active, displaying system details:

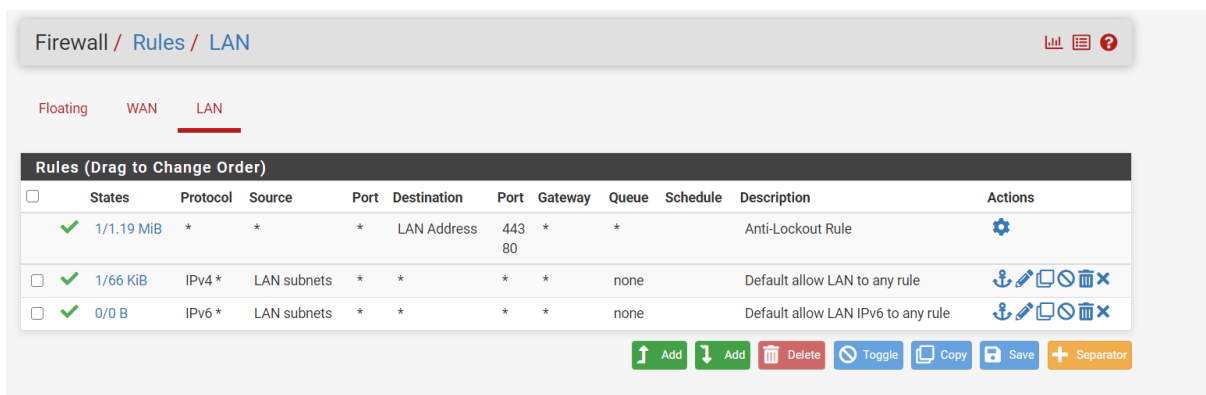
- System:** Microsoft Azure, Netgate Device ID: 4aa3234c3231f3b21c2b
- BIOS:** Release Date: Wed Dec 31 1969
- Version:** 2.7.2-RELEASE (amd64), built on Wed Dec 6 19:10:00 -01 2023, FreeBSD 14.0-CURRENT. A message states: "The system is on the latest version. Version information updated at Fri Feb 16 7:32:37 -01 2024".
- CPU Type:** 13th Gen Intel(R) Core(TM) i7-1355U, 6 CPUs: 1 package(s) x 3 core(s) x 2 hardware threads, AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No
- Hardware crypto:** Inactive
- Kernel PTI:** Disabled
- MDS Mitigation:** Inactive
- Uptime:** 01 Hour 14 Minutes 21 Seconds
- Current date/time:** Fri Feb 16 9:17:36 -01 2024
- DNS server(s):** 127.0.0.1, 172.18.208.1, 192.168.0.1
- Last config change:** Fri Feb 16 9:16:53 -01 2024
- State table size:** 0% (336/403000) Show states
- MBUF Usage:** 0% (2032/1000000)

On the right, the 'Interfaces' tab is active, showing the status of network interfaces:

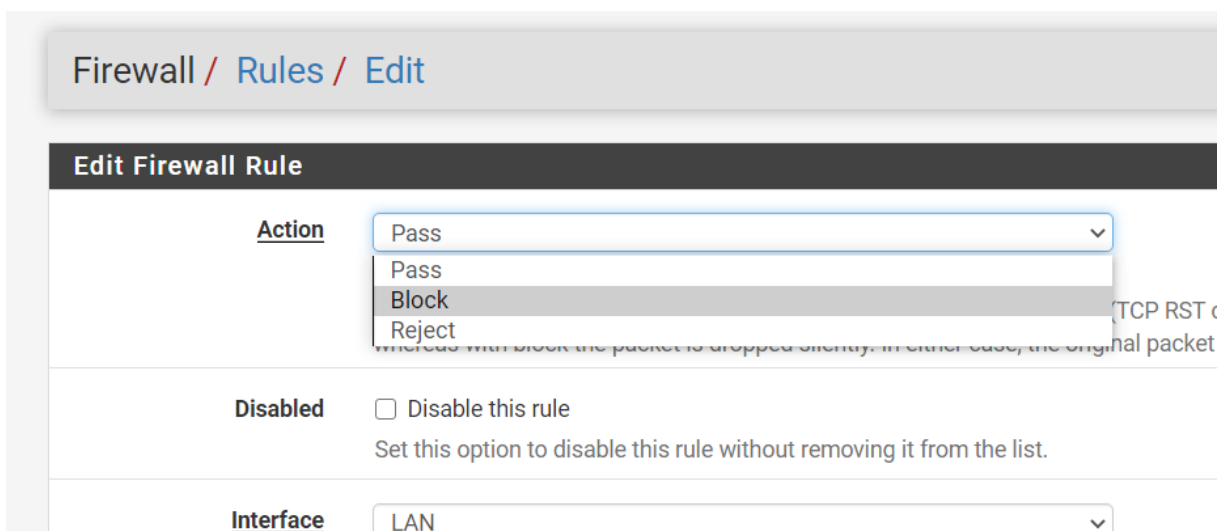
Interface	Status	Speed	MAC
WAN	↑	10Gbase-T <full-duplex>	172.18.212.128
LAN	↑	10Gbase-T <full-duplex>	192.168.0.254

Below the interfaces, there is a section for 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' with links to support resources and a note about Netgate TAC support subscriptions.

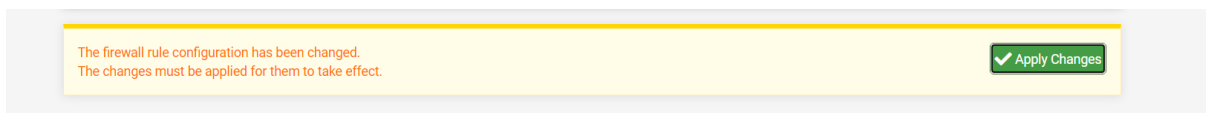
Ensuite on va apporter quelques modifications. On va pour cela modifier les règles par défaut du firewall.



On va déjà bloquer.

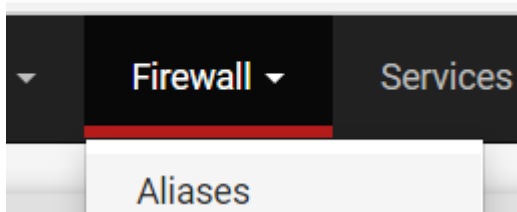


En ipv4 ou 6 puis ne pas oublier d'appliquer les modifications.



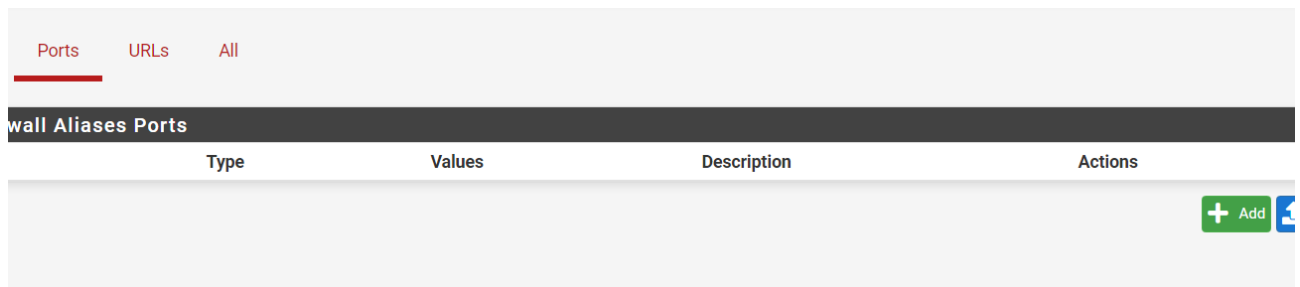
Puis dans firewall aliases on va accepter ce qui nous intéresse.

/all\_rules.php?if=lan

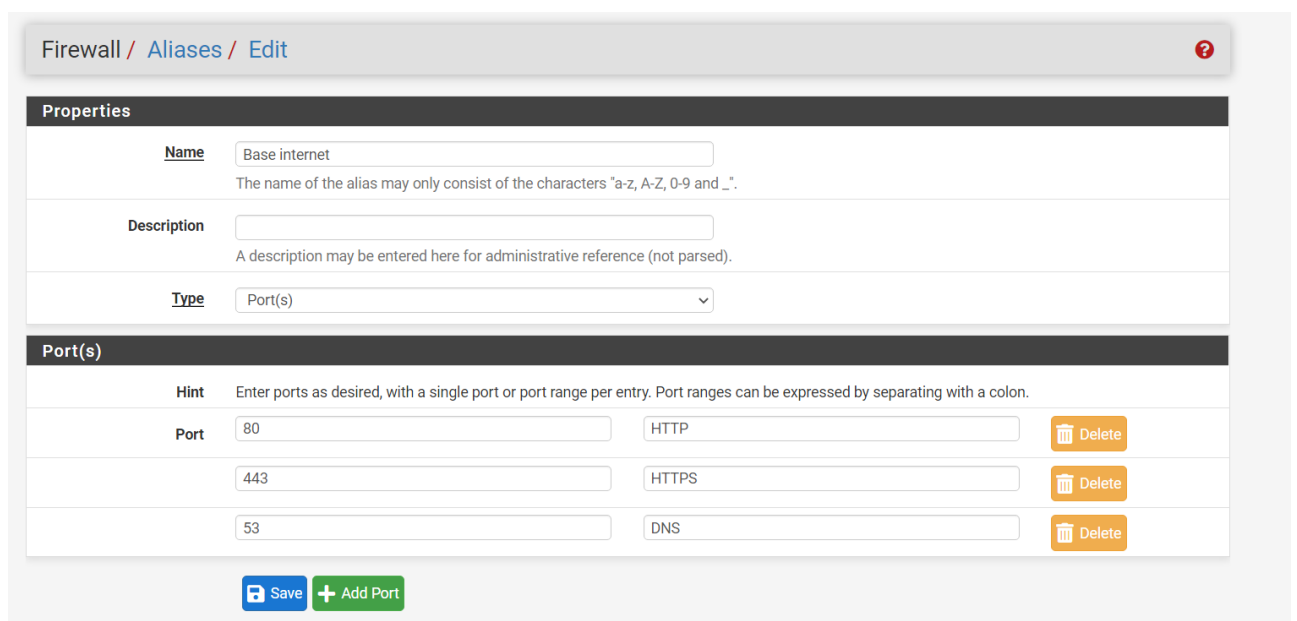




Dans ports on pourra ajouter ces règles.

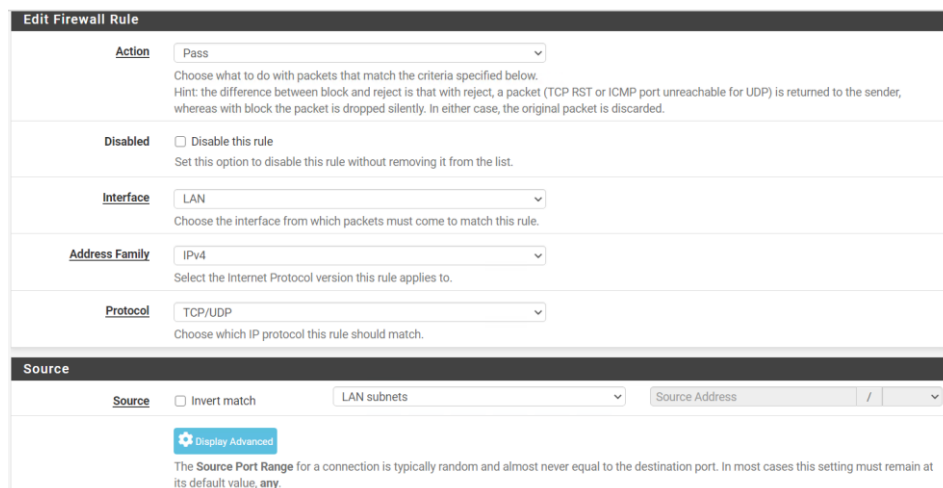


Une fois nos ports ajouté on peut sauvegarder.



Et on va maintenant retourner dans les règle pour en ajouter une qui utilise cet alias.

Et il faudra veiller à bien rentrer les bon paramètres suivant :



**Destination**

**Destination**  Invert match Any Destination Address

**Destination Port Range** (other) BaselInternet (other) Destination Address

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.

**Extra Options**

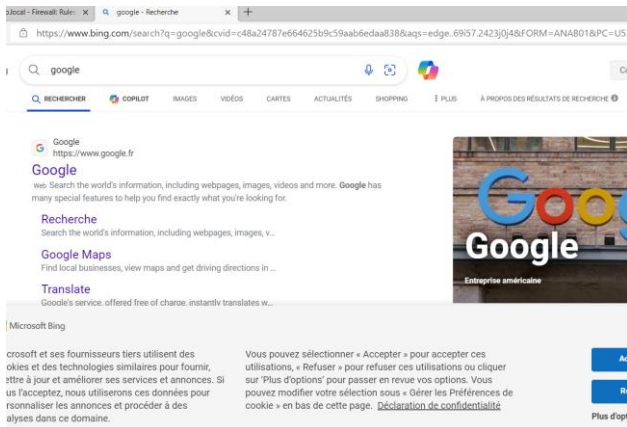
**Log**  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**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**

On a donc bien utilisé BaselInternet qui acceptera les bon ports et on applique avant de sauvegarder les changements.

Pour vérifier on fait simplement une recherche google :



Notre par feu est donc bien

fonctionnel

Et on peut voir que il y a eu du trafic

	Status	Bytes	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
<input checked="" type="checkbox"/>	<span style="color: green;">✓</span>	2/1.59 MiB	*	*	*	LAN Address	443			
<input type="checkbox"/>	<span style="color: green;">✓</span>	66/8.70 MiB	IPv4 TCP/UDP	LAN subnets	*	*	BaselInternet			
<input type="checkbox"/>	<span style="color: red;">✗</span>	0/15 KiB	IPv4 *	LAN	*	*	*			

Alias details

Value	Description
80	HTTP
443	HTTPS
53	DNS

Enfin si on veut autoriser le ping on refait une règle avec le protocole icmp

**Disabled**  Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface**   
Choose the interface from which packets must come to match this rule.

**Address Family**   
Select the Internet Protocol version this rule applies to.

**Protocol**   
Choose which IP protocol this rule should match.

**ICMP Subtypes**   
Alternate Host  
Datagram conversion error  
Echo reply  
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

**Source**  Invert match

**Destination**  Invert match

et nos ping vont à nouveau fonctionner via le pare feu

### Conclusion :

Nous avons donc dans ce tp installé un firewall sous forme de vm et configuré les paramètres de bases sur les deux cartes réseaux lan et wan puis on lui a attribué une adresse ip pour se connecter à son interface web et y ajouter le filtrage en fonction des protocoles lors de la navigations sur le web pour sécuriser le tout. Mon premier pare-feu est installé !