Guastamacchia Livio **Tp pfSense :**

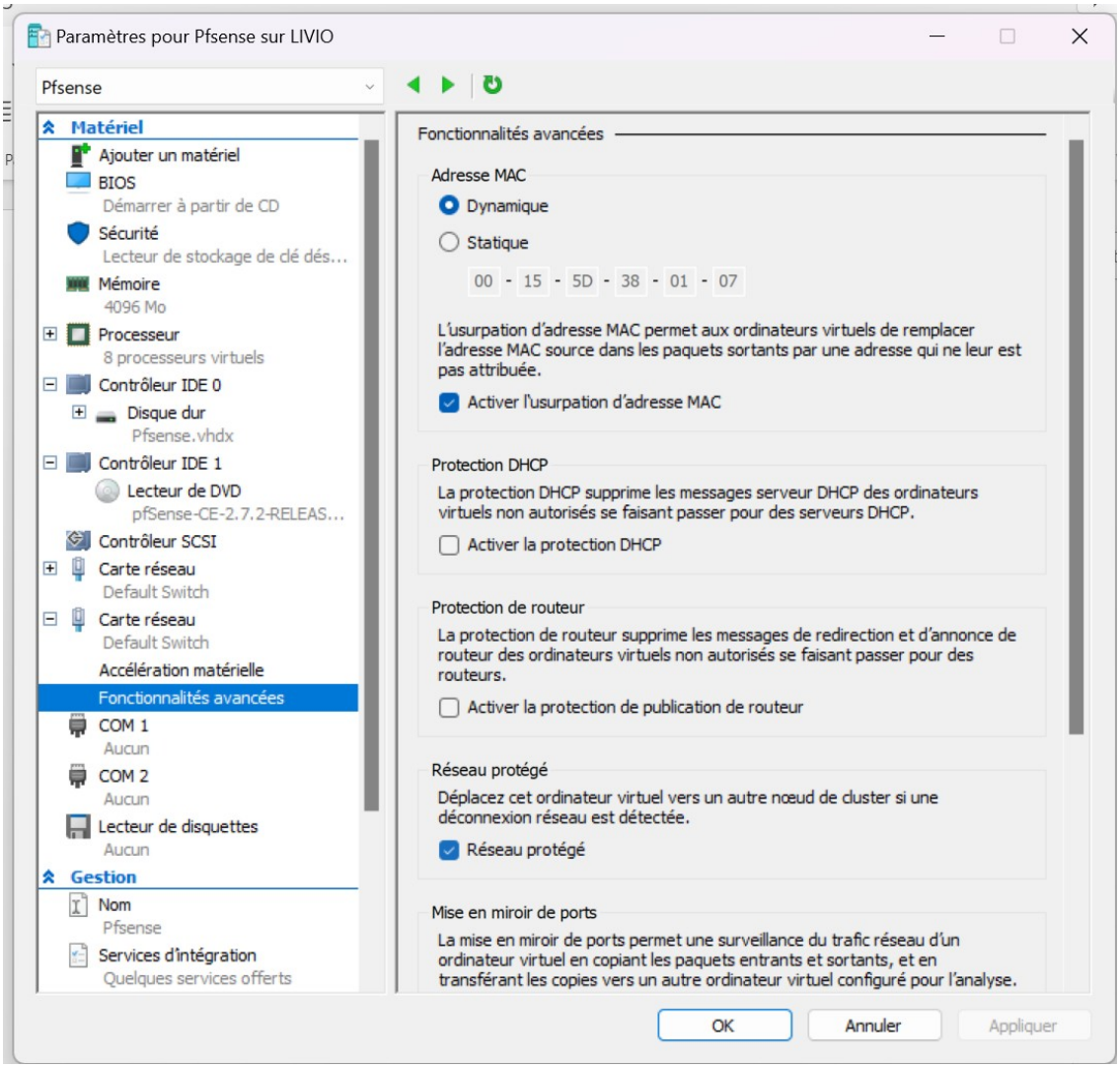
SIO1

Introduction :

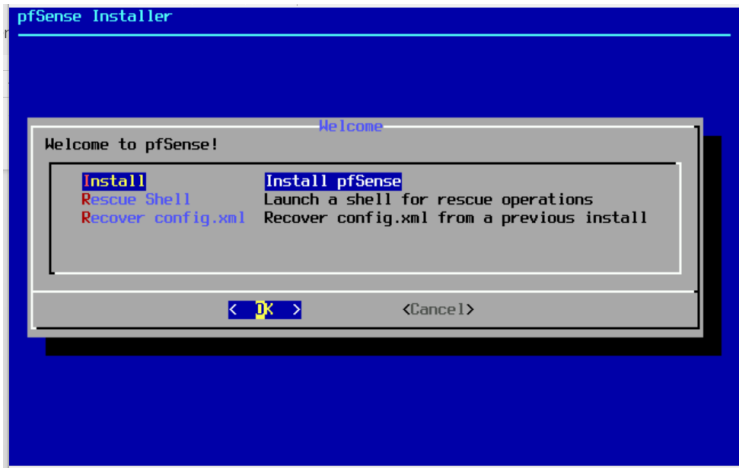
Dans ce TP nous allons procéder a l'installation et aux paramétrage de règle du parefeu Pfsense.

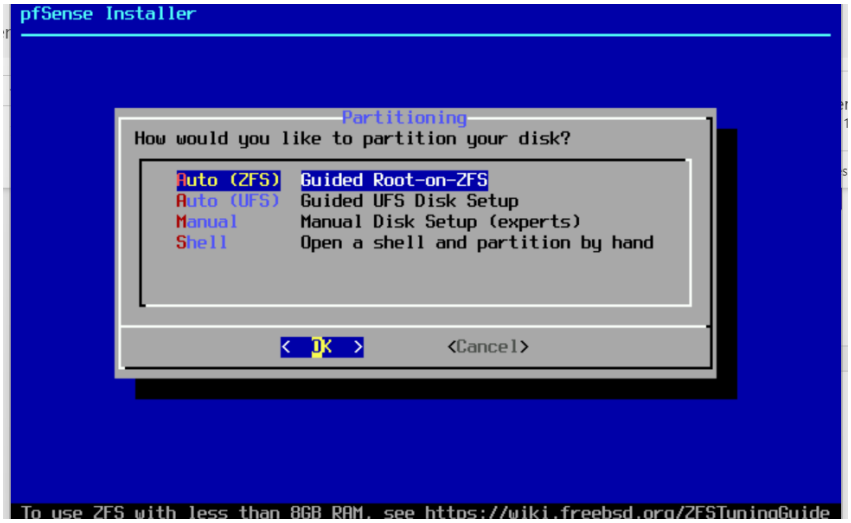
TP :

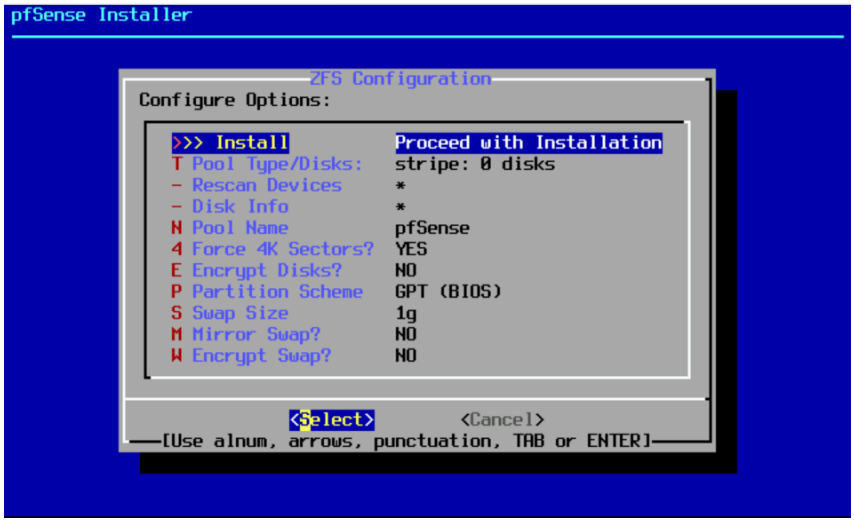
Pour commencer ce TP, nous créons une VM pfSense en activant sur les deux cartes réseaux « l'usurpation d'adresse mac » dans les fonctionnalités de la carte

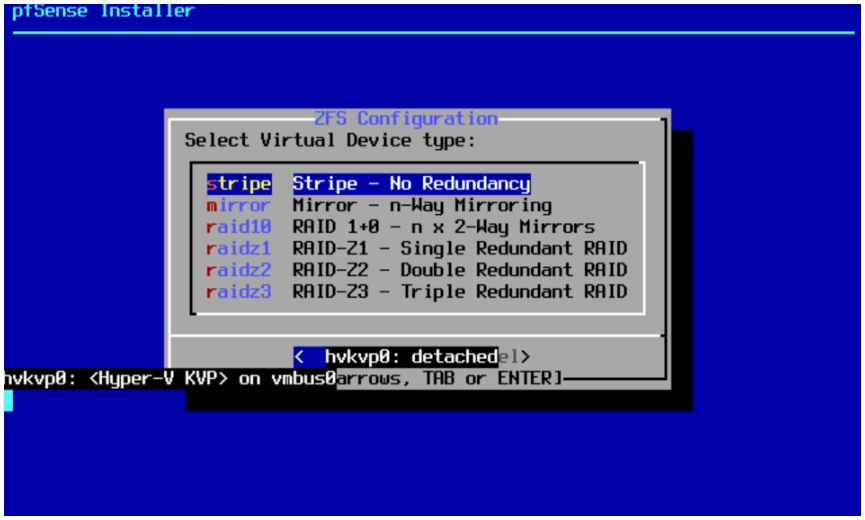


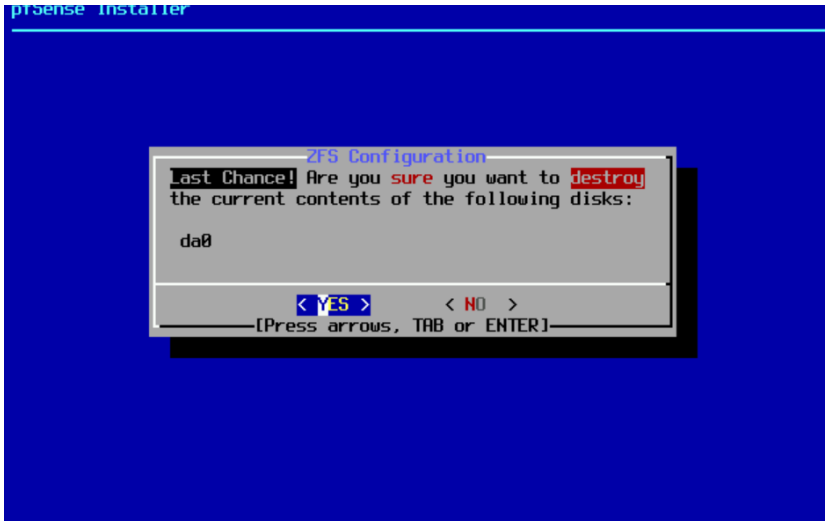
Maintenant, nous démarrons la VM et on procède à l'installation de pfSense

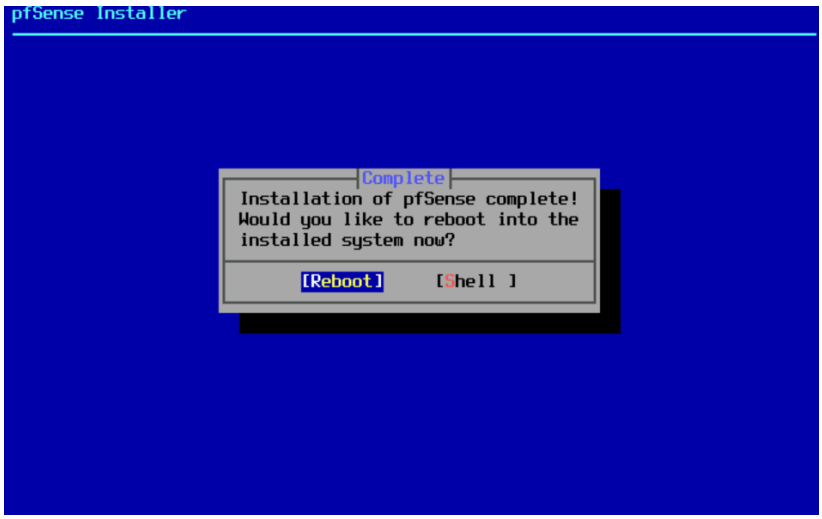

pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
< OK >
<Cancel>


pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS)
Guided Root-on-ZFS
Auto (UFS)
Guided UFS Disk Setup
Manual
Manual Disk Setup (experts)
Shell
Open a shell and partition by hand
< OK >
<Cancel>
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/ZFSTuningGuide


pfSense Installer
ZFS Configuration
Configure Options:
>>> Install
Proceed with Installation
T Pool Type/Disks:
stripe: 0 disks
- Rescan Devices
*
- Disk Info
*
N Pool Name
pfSense
4 Force 4K Sectors?
YES
E Encrypt Disks?
NO
P Partition Scheme
GPT (BIOS)
S Swap Size
1g
M Mirror Swap?
NO
W Encrypt Swap?
NO
<Select>
<Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]







Après l'installation de faite, nous allons attribuer si il y a des cartes VLAN, dans notre cas nous n'en avons pas donc on va juste mettre "n"

```
Should VLANs be set up now [y|n]? 2024-03-01T08:22:56.725872+00:00 - php-fpm 395
 - - /rc.linkup: Ignoring link event during boot sequence.
2024-03-01T08:22:56.725872+00:00 - php-fpm 394 - - /rc.linkup: Ignoring link eve
nt during boot sequence.
n
```

Puis nous allons paramétrer qui est notre carte LAN et WAN, notre LAN sera hn0 et notre WAN sera hn1.

```
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
```

Nous validons avec “y”

```
Do you want to proceed [y|n]? y
```

Nous allons maintenant changer l’adresse IP du LAN

```
WAN (wan)       -> hn1        -> v4/DHCP4: 192.168.227.124/20
LAN (lan)       -> hn0        -> 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
```

Nous choisirons bien l’interface LAN (2)

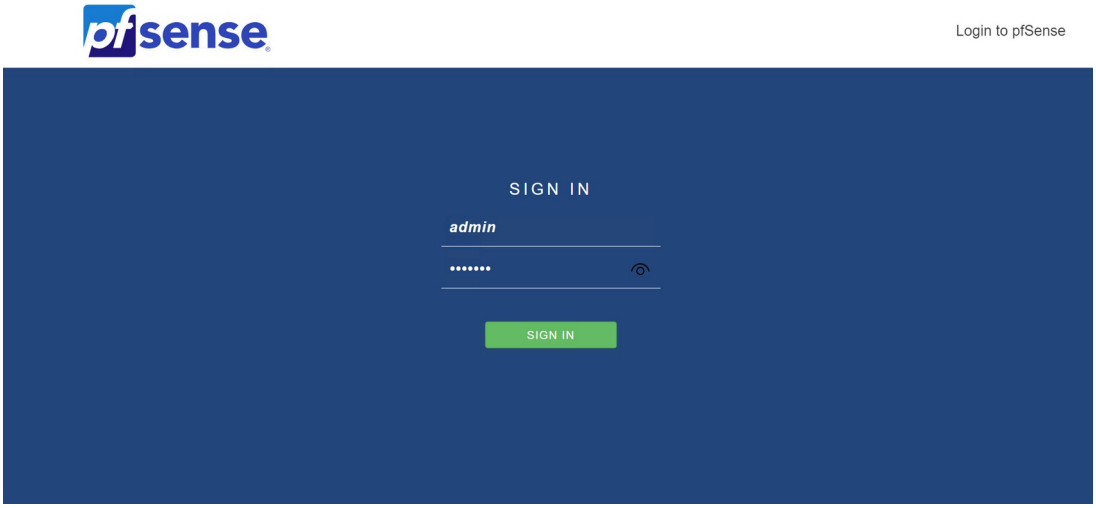
```
Available interfaces:

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

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

On modifie l’adresse IP 192.168.1.1/24 par 192.168.20.1/24

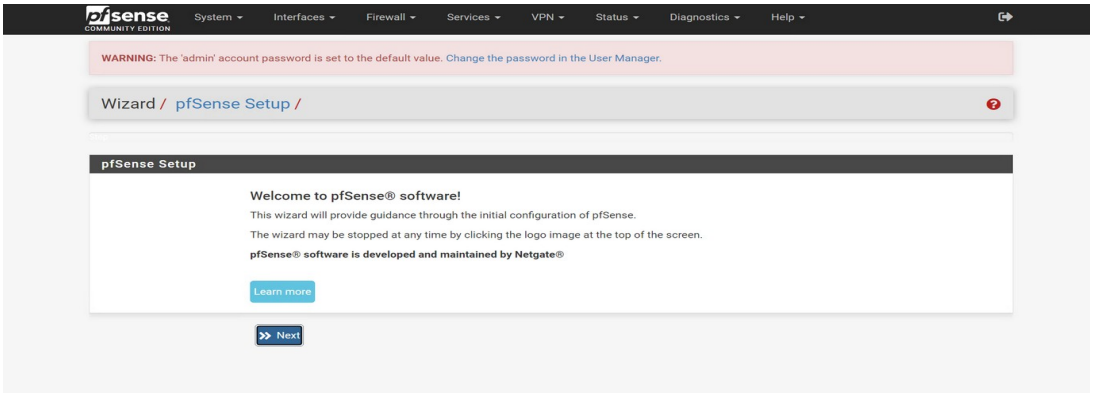
```
Configure IPv6 address LAN interface via DHCP6? (y/n) n

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...

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

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

The IPv4 LAN address has been set to 192.168.10.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.10.1/
```

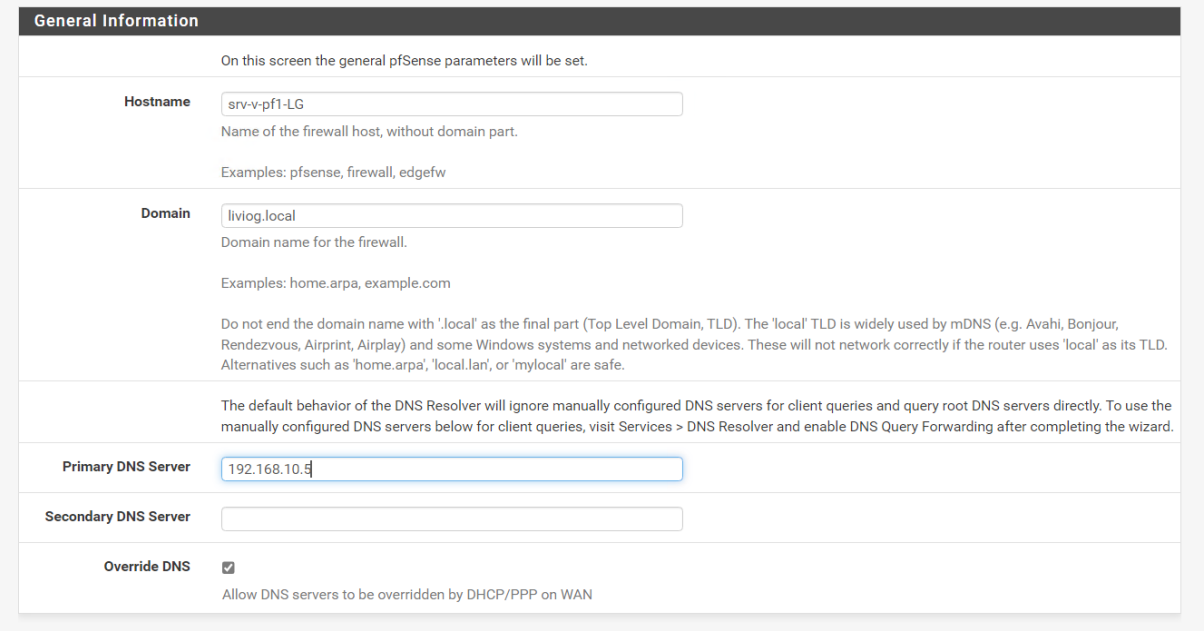
après avoir modifier l'adresse IP de notre LAN il nous reste plus qu'à aller sur le site ci-dessus sur une machine connecter au réseaux (de préférence client) pour pouvoir paramétrer notre parefeu

nous arrivons sur ce site, nous devrons se connecter avec l 'identifiants « admin » et le mdp « pfsense » (il est conseiller de changer mdp de suite après la connexion)



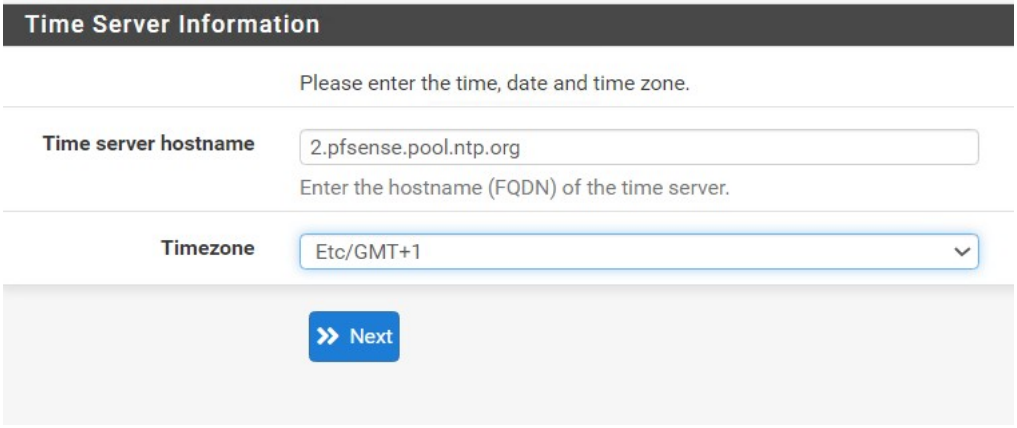
Nous arrivons sur cette page qui est l'assistant de paramétrage pfsense.





Nous allons continuer jusque cette page ou l'on va noté : le nom du parefeu, le nom du domaine ainsi que l'adresse IP de notre serveur DNS

il nous est maintenant demander de paramétrer l'heure pour nous on est en GMT+1



après cela on nous demandera de paramétrer le WAN que l'on ne changera pas car il est bien paramétrer par défaut et on nous demandera aussi si l'on veut modifier l'adresse IP du parefeu que l'on a déjà changer au préalable donc qui n'est pas nécessaire.

Après avoir passer les deux page de configuration, Nous arrivons a la modification du mdp du parefeu après il nous resteras plus qu'a accepter la demande de redémarrage

(j'ai oublier de prendre un screen et je ne peux plus aller en arrière)

On voit bien que le parefeu a bien été paramétrer

Status / Dashboard

System Information

Name	srv-v-pf1-LG.liviog.local
User	admin@192.168.10.100 (Local Database)
System	Microsoft Azure Netgate Device ID: **67d5d5ffc235d87ebbe8**
BIOS	Vendor: □□□□□□□□□□None Version: □□□
Version	**2.7.2-RELEASE** (amd64) built on Wed Dec 6 19:10:00 -01 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Fri Mar 15 7:47:07 -01 2024
CPU Type	13th Gen Intel(R) Core(TM) i7-13620H 8 CPUs: 1 package(s) x 4 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	00 Hour 29 Minutes 54 Seconds
Current date/time	Fri Mar 15 8:16:01 -01 2024
DNS server(s)	• 127.0.0.1 • 172.25.0.1 • 192.168.10.5
Last config change	Fri Mar 15 8:12:56 -01 2024
State table size	0% (31/403000) Show states

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- **Upgrade Your Support**
- Netgate Global Support FAQ
- Netgate Professional Services
- **Community Support Resources**
- Official pfSense Training by Netgate
- Visit Netgate.com

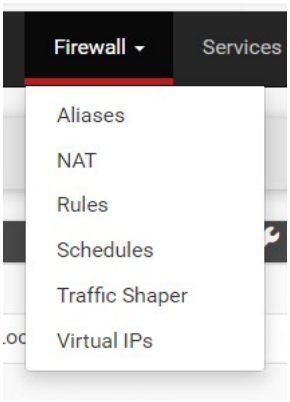
If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.

Interfaces

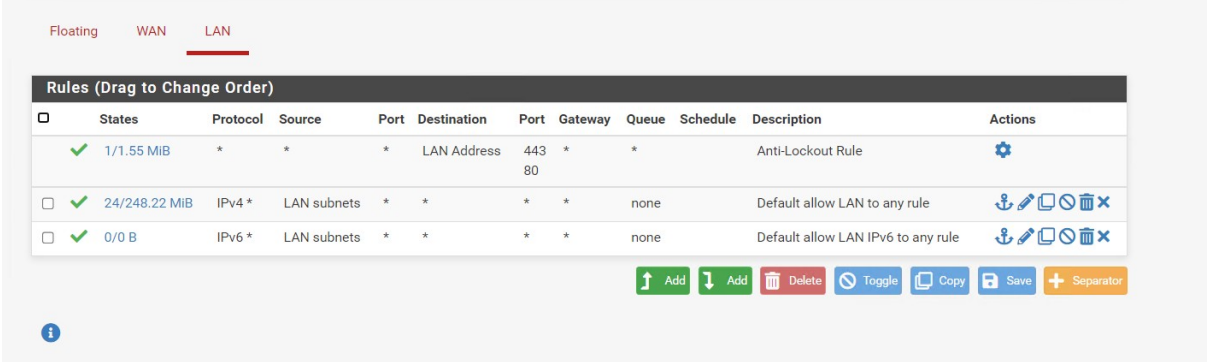
WAN	↑	10Gbase-T <full-duplex>	172.25.11.36
LAN	↑	10Gbase-T <full-duplex>	192.168.10.1

maintenant nous allons passé aux règles de parefeu

Nous irons dans l'onglet firewall puis sur rules



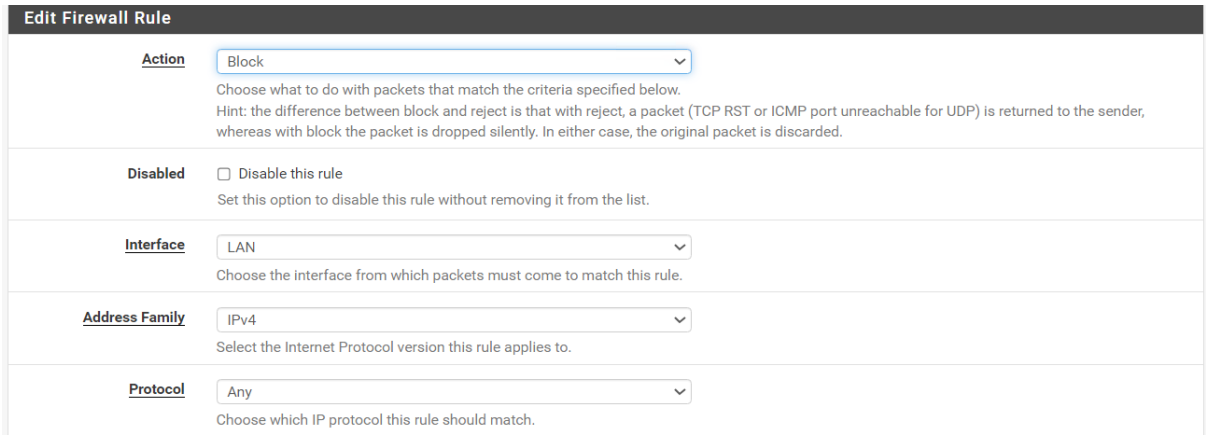
on voit que tous est autorisé pour le LAN



on va premièrement modifier les paramètre IPV4 et IPV6 pour bloquer le passage

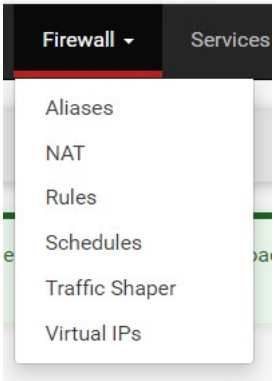
on clique sur le petit crayon

puis on bloque les actions

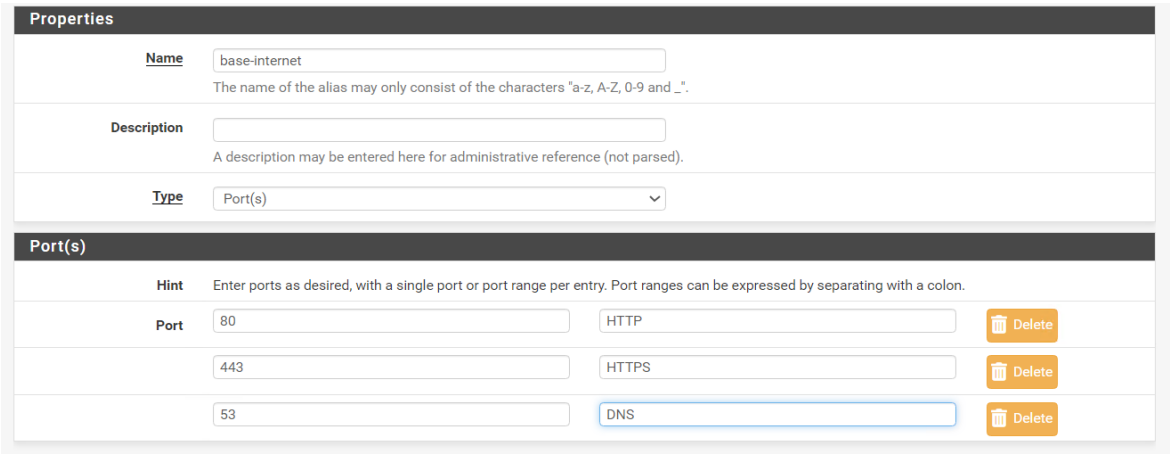


deuxièmement nous créons un alias pour les port qui nous intéresse

pour cela nous allons sur firewall > aliases > port



et on add les port qui nous intéresse notamment les port internet donc le port 80 pour HTTP, le port 443 pour HTTPS et le port 53 pour DNS



Nous allons maintenant créer une règle de parefeu pour les alias créer

on ajoute une règle puis comme paramètre nous allons mettre

- Action : pass (autoriser les passages)

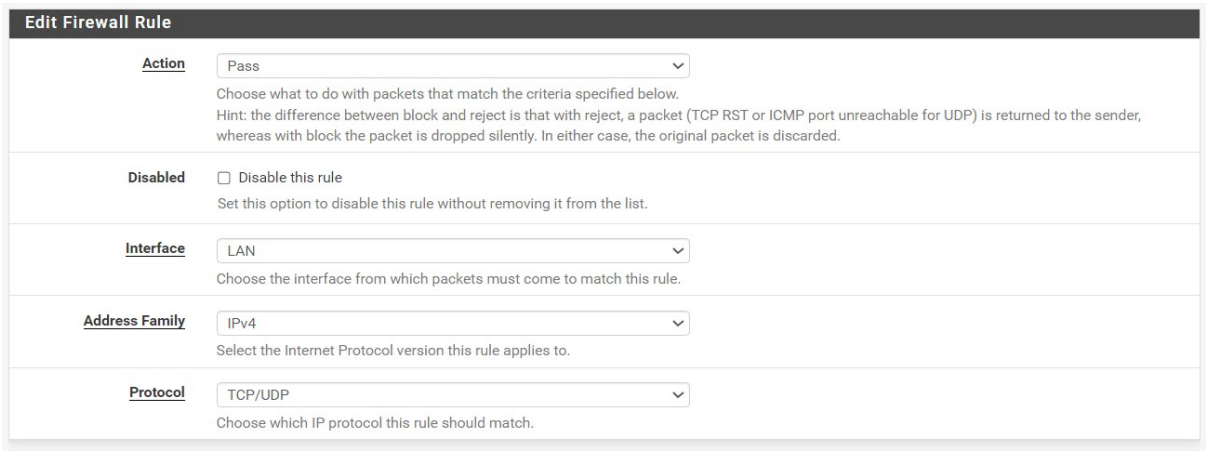
- Protocol : TCP/UDP

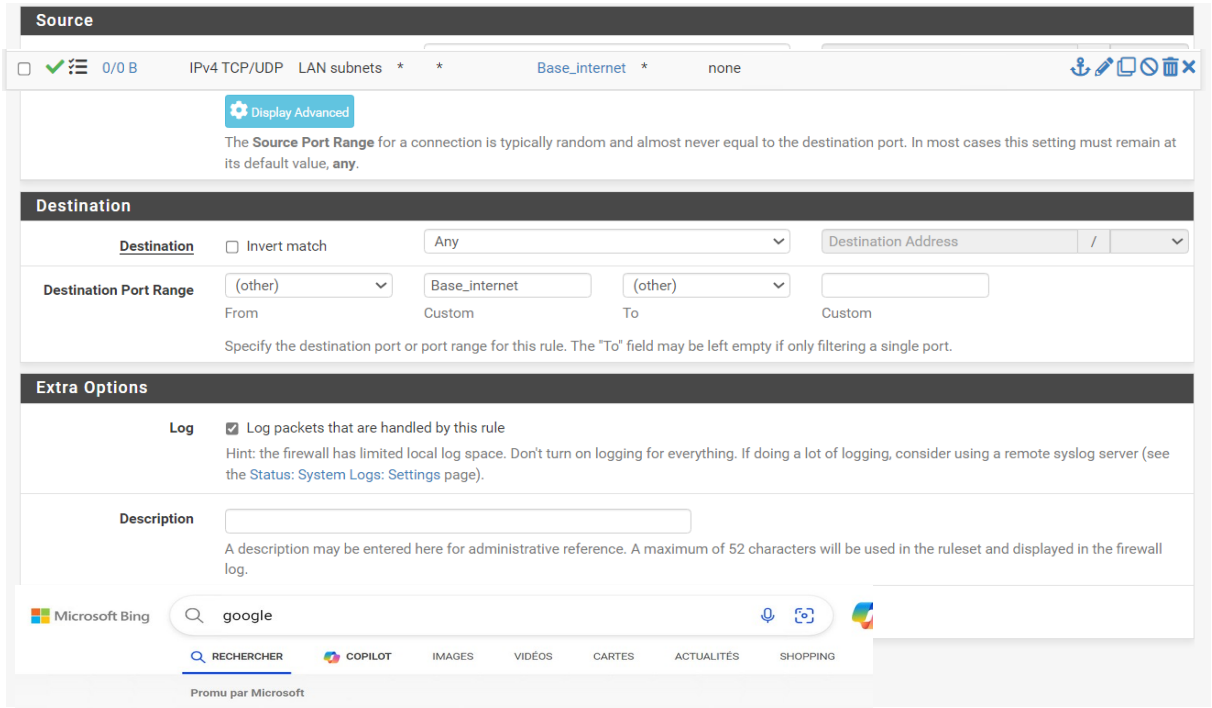
- Source : LAN subnets (autoriser tout ce qui vien du réseaux LAN)

- destination : ANY (pour n'importe quel destination)

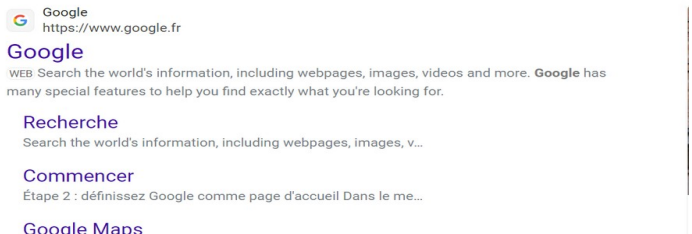
- destination Port Range : base_internet (alias créer au préalable)

et on coche les logs pour nous permettre d'avoir un historique des passages



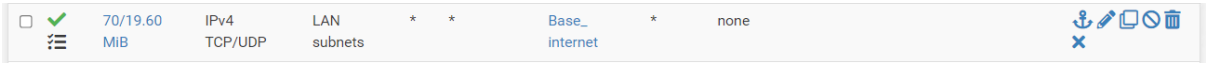


N ur un navigateur internet

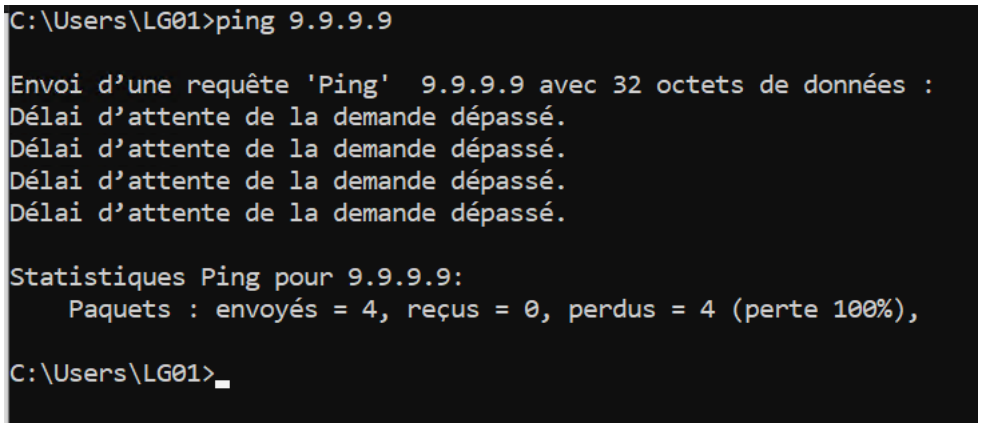


La recherche a bien fonctionné ce qui nous montre que nous avons réussis a avoir un accès internet

Sur pfsense nous pouvons bien voir qu'il y a eu du trafic qui est passer via cette règle



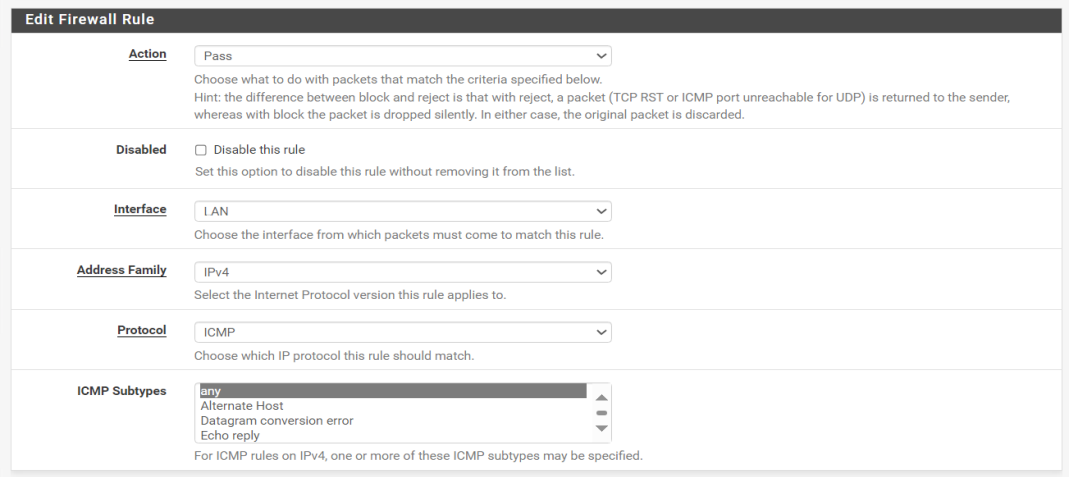
pour finir on vas rajouter une règle pour les pings vers internet car il est impossible de faire un ping via internet

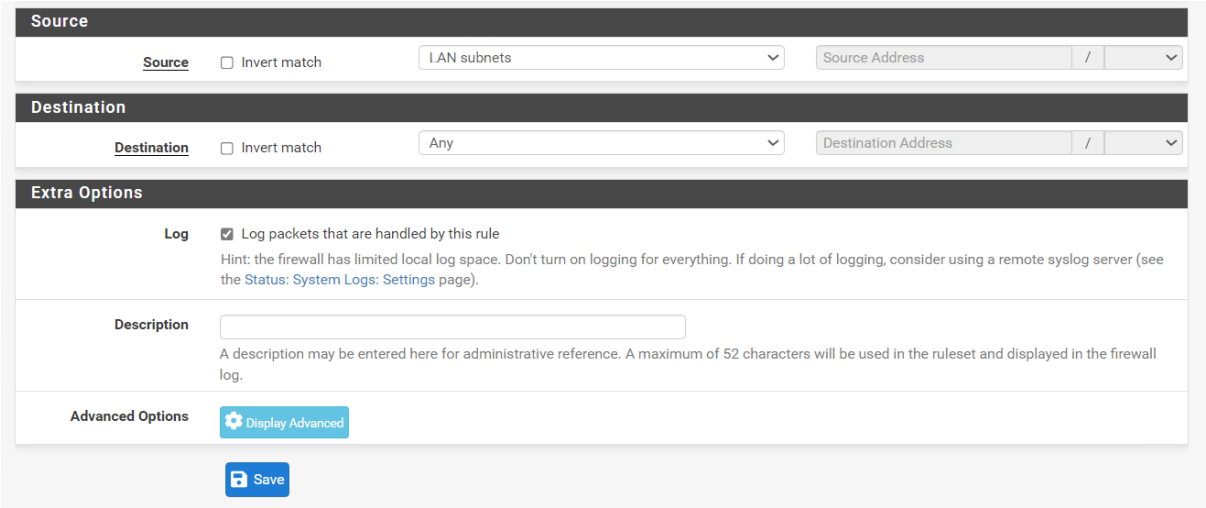


- action : pass

- protocole : IMCP (protocole pour les pings)

- source : LAN subnets





maintenant on voit bien que les ping sont possible vers internet

```
C:\Users\LG01>ping 9.9.9.9

Envoi d'une requête 'Ping'  9.9.9.9 avec 32 octets de données :
Réponse de 9.9.9.9 : octets=32 temps=175 ms TTL=49
Réponse de 9.9.9.9 : octets=32 temps=172 ms TTL=49
Réponse de 9.9.9.9 : octets=32 temps=300 ms TTL=49
Réponse de 9.9.9.9 : octets=32 temps=132 ms TTL=49

Statistiques Ping pour 9.9.9.9:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 132ms, Maximum = 300ms, Moyenne = 194ms
```

conclusion :

SIO 1 : TP court et pas très compliquer a effectuer mis a part les problème d'accordement d IP qui reste un petit problème mais qui est réglable sans trop de soucis ou bien le fait d oublier de lancer la VM pfsense pour le paramétrer sur le site.

SIO 2 : TP rapide a effectué, problème de récupération d'ip pour le WAN du a des paramètres d'hyper V mal configuré mis a part ça aucun soucis.