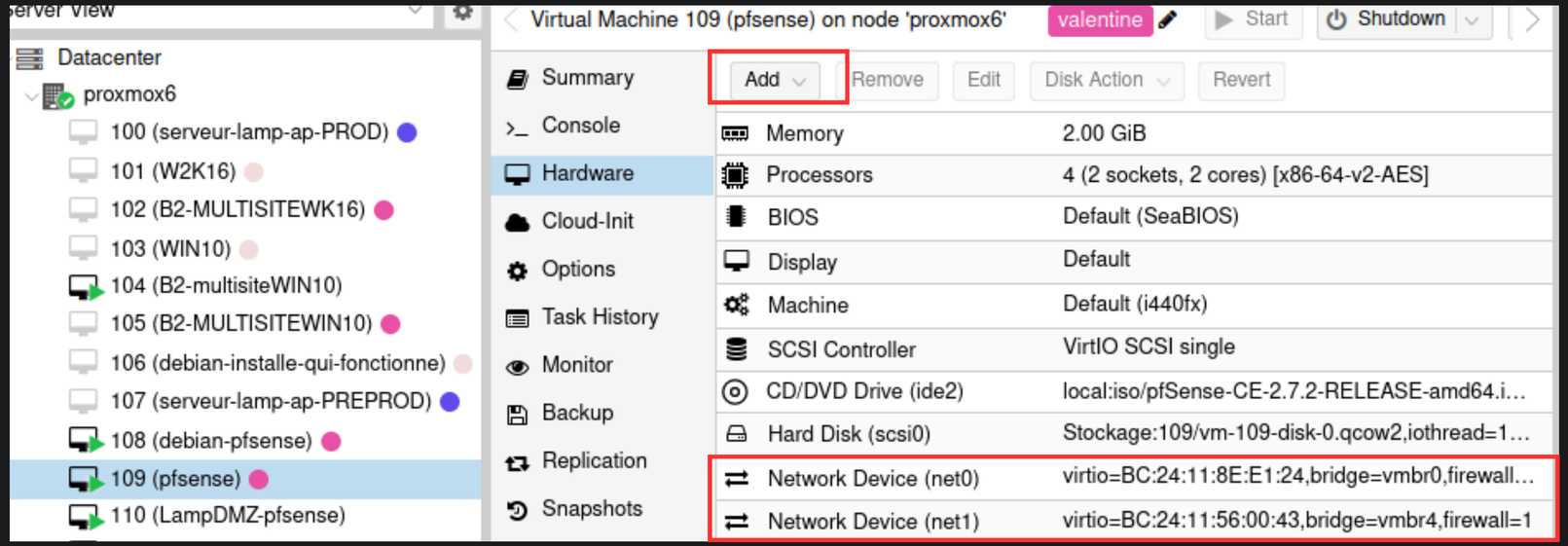
TP- PFSENSE

INSTALLATION PFSENSE

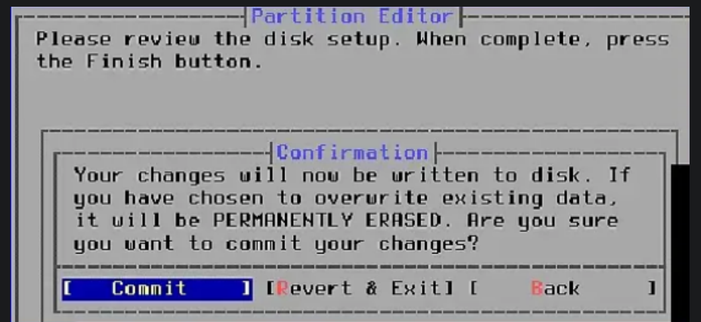
Lorsque vous installez sur proxmox, mettez 2 cartes réseaux pour votre pfsense (une pour le LAN, une pour le WAN) Pour cela, cliquez sur “Add” puis sur “Network Device”



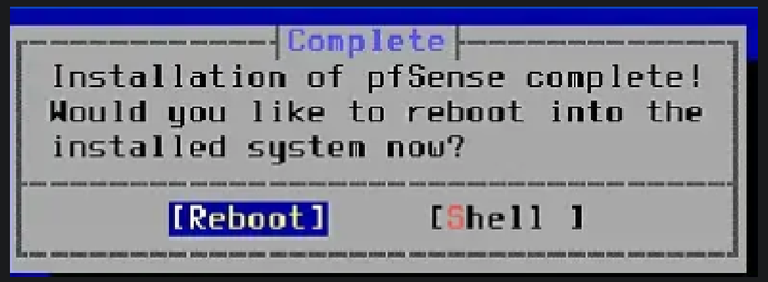
INSTALLATION PFSENSE

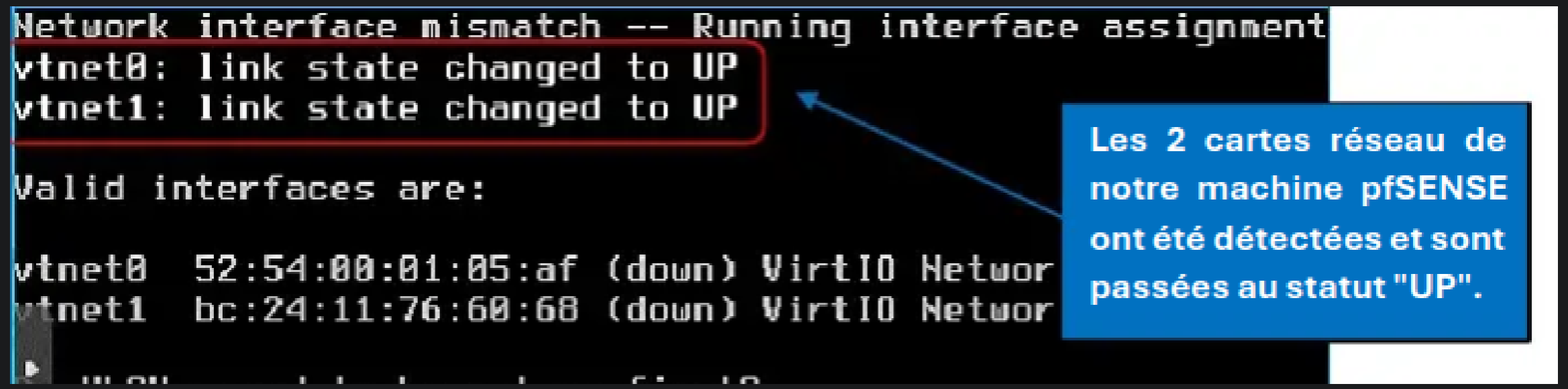
Procédons à l'installation, suivez ces étapes:

INSTALLATION PFSENSE



INSTALLATION PFSENSE

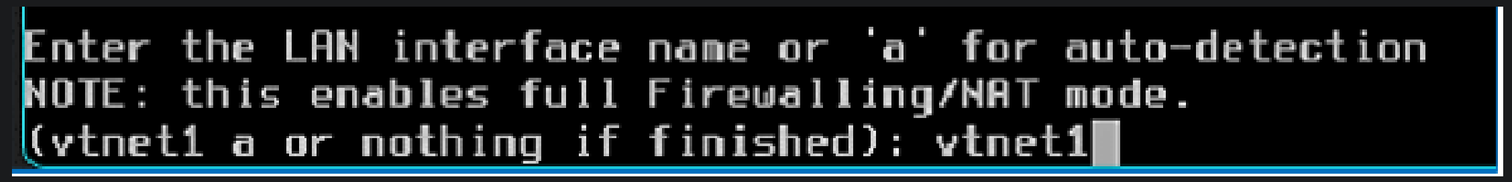




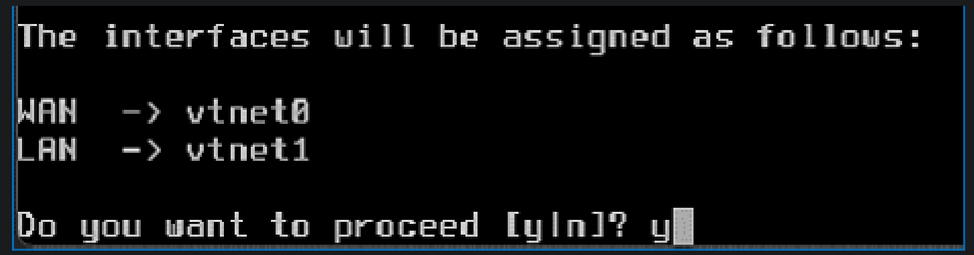
INSTALLATION PFSENSE

Assignons les cartes réseaux détectées aux interfaces WAN et LAN

Indiquez “vtnet0” et faites “Entrée” pour assigner cette carte en tant qu’interface WAN
Indiquez “vtnet1” pour l’autre carte pour l’assigner en tant qu’interface LAN



Saisissez “y” pour valider et patientez pendant que pfsense assigne les interfaces aux cartes réseaux



INSTALLATION PFSENSE

Nous allons maintenant changer l'adresse IP du LAN, pour cela, dans le menu, je choisis "2"

```
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:
```

Je re presse "2" pour sélectionner le LAN, je presse "n", je saisis mon adresse IP qui est ici "192.168.40.33", je saisis "24", je presse "entrée" car je ne dois pas modifier ceci, je presse "n" à la question, je presse "entrée", je presse "n". Votre adresse IP est modifiée.

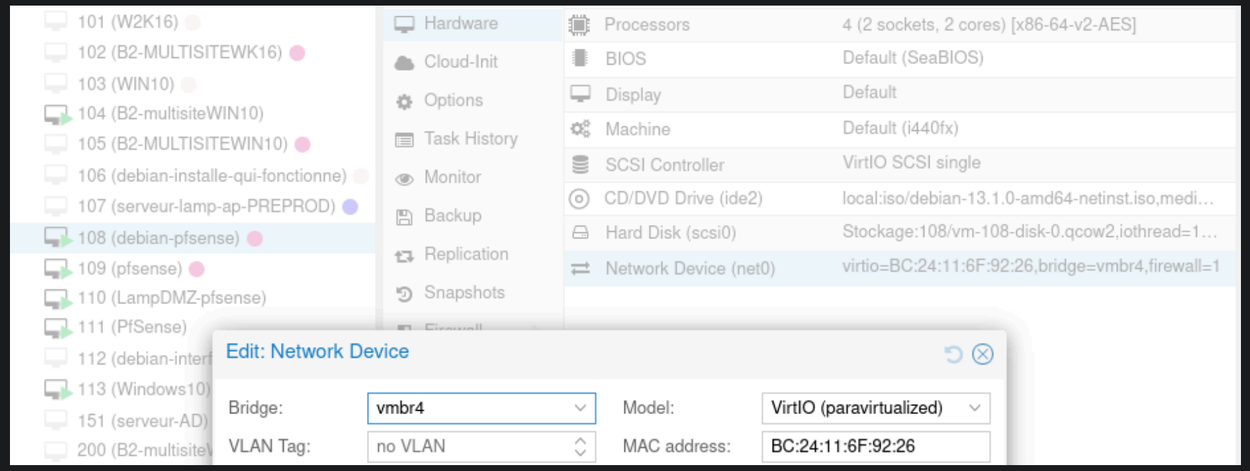
```
Enter the number of the interface you wish to configure: 2

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.40.33

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 32):
> 24

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

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...

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

The IPv4 LAN address has been set to 192.168.40.33/24
You can now access the webConfigurator by opening the following URL in your we
browser:
                    http://192.168.40.33/
```

ACCES À L'INTERFACE GRAPHIQUE

J'installe une seconde VM dotée d'une interface graphique (debian, windows…)

Il faudra attribué à cette VM la même carte réseau que le LAN (l'adresse IP de mon LAN est 192.168.40.33 et l'IP de ma carte réseau pour le LAN est 192.168.40.32)

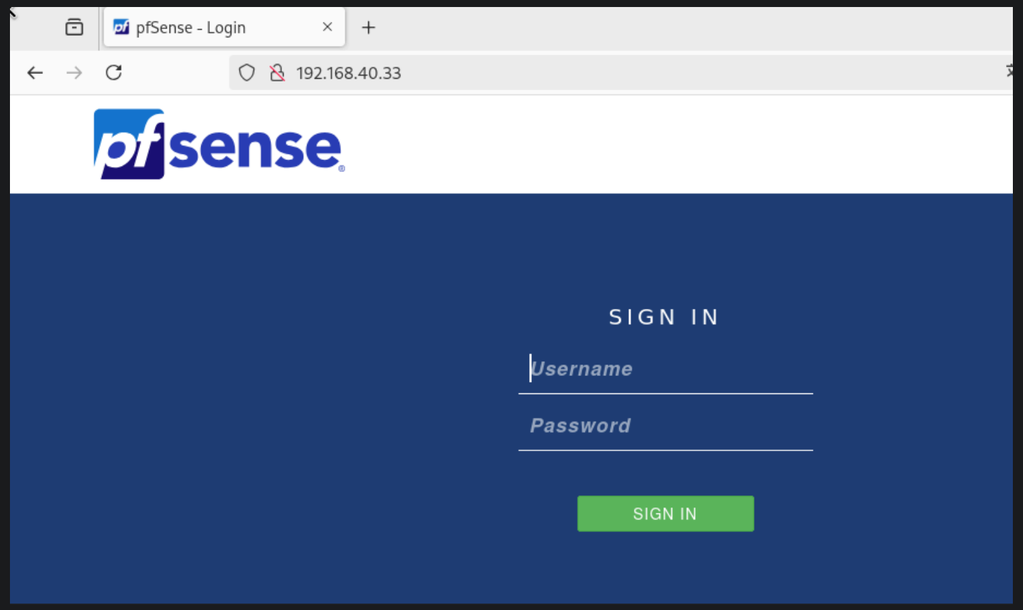


Il faudra attribué à cette VM une adresse IP en 192.168.40.x (j'ai choisi 192.168.40.34) afin qu'elle puisse afficher l'interface graphique de pfsense

```
user@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
t 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
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
up default qlen 1000
    link/ether bc:24:11:6f:92:26 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    altname enxbc24116f9226
    inet 192.168.40.34/24 brd 192.168.40.255 scope global noprefixroute ens1
       valid_lft forever preferred_lft forever
```

ACCES À L'INTERFACE GRAPHIQUE

En allant sur le moteur de recherche et en tapant l'adresse IP du LAN, je tombe sur l'interface graphique:

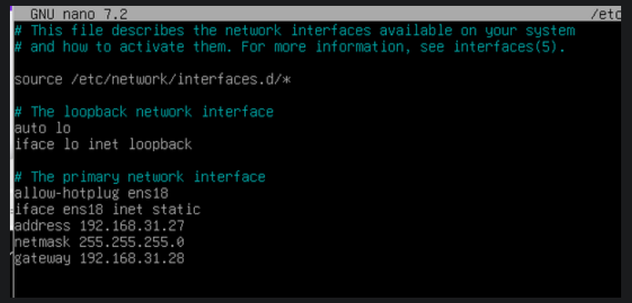


Les login sont admin en username et pfsense en password

CONNECTER UN SERVEUR LAMP

Ajoutez une nouvelle carte réseau à votre PFSENSE (comme vu au début du TP), ce sera la carte réseau pour votre DMZ.

Installez un serveur LAMP, une fois dessus, vous allez devoir changer l'adresse IP de votre serveur et ajouter la gateway, faites nano /etc/network/interfaces:



Pour la gateway, vous mettrez l'adresse IP de la carte réseau que vous venez d'ajouter "192.168.31.28", c'est la carte réseau dédié à votre DMZ
Vous devrez forcément mettre une adresse ip similaire à 192.168.31.x (ici on mettra 192.168.31.27)

```
root@debian:~# ip a
1: 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
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:22:a6:c2 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.31.27/24 brd 192.168.31.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe22:a6c2/64 scope link
       valid_lft forever preferred_lft forever
root@debian:~# ip route
default via 192.168.31.28 dev ens18 onlink
192.168.31.0/24 dev ens18 proto kernel scope link src 192.168.31.27
```

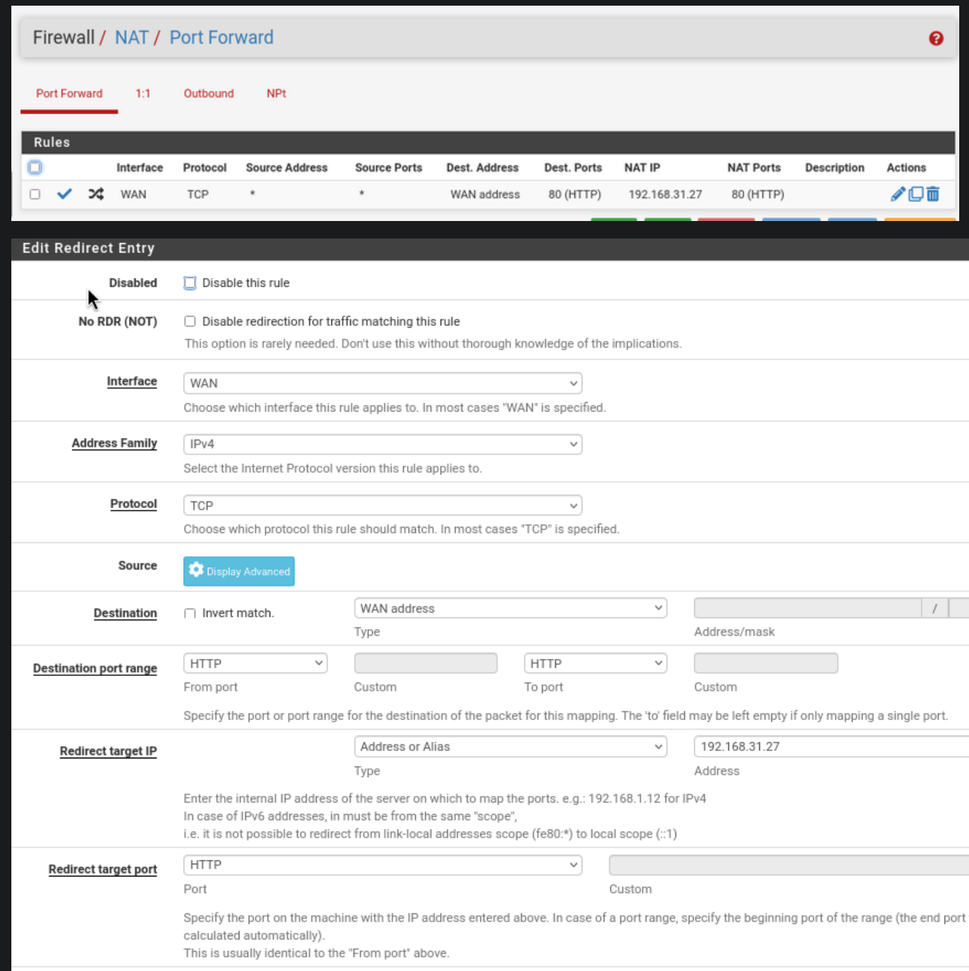
CONNECTER UN SERVEUR LAMP

Pour la gateway, vous mettrez l'adresse IP de la carte réseau que vous venez d'ajouter "192.168.31.28", c'est la carte réseau dédié à votre DMZ
Vous devrez forcément mettre une adresse ip similaire à 192.168.31.x (ici on mettra 192.168.31.27)

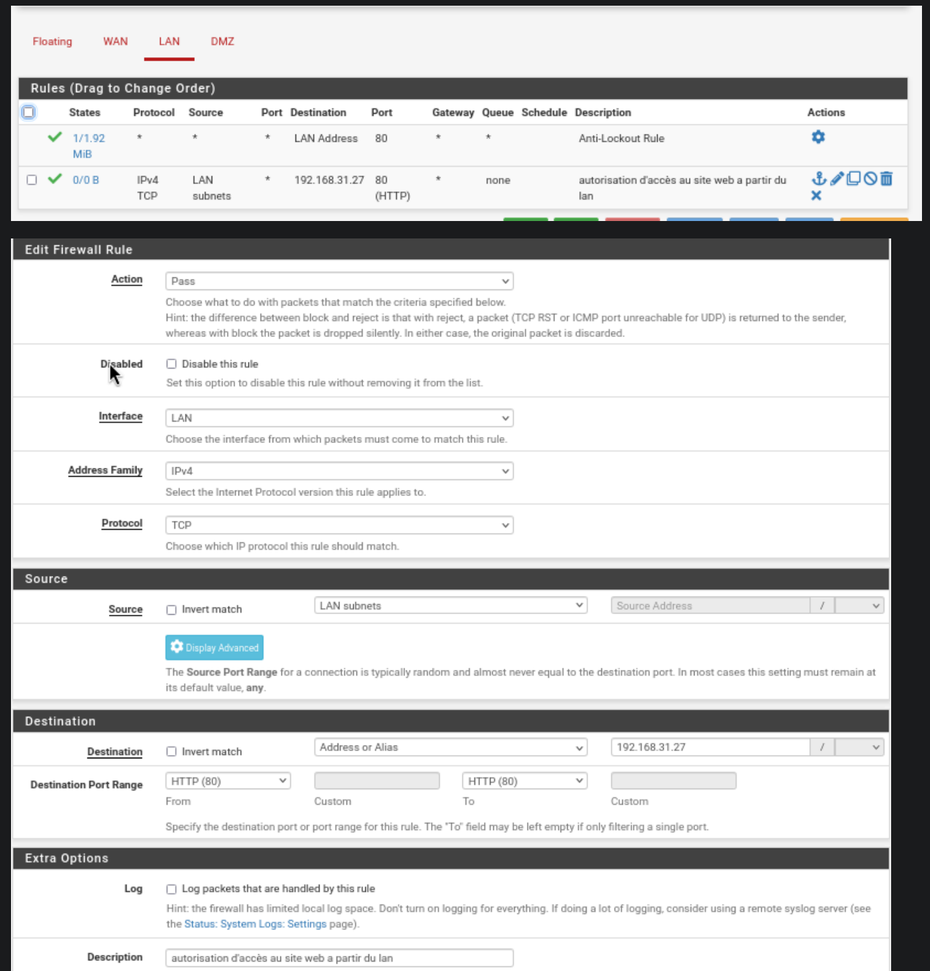
```
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:22:a6:c2 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.31.27/24 brd 192.168.31.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe22:a6c2/64 scope link
       valid_lft forever preferred_lft forever
root@debian:~# ip route
default via 192.168.31.28 dev ens18 onlink
192.168.31.0/24 dev ens18 proto kernel scope link src 192.168.31.27
```

ACCÈS DU LAN VERS LA DMZ

Pour le NAT cela permet d'envoyer la page WEB vers le LAN en faisant une rediraction de ce port :

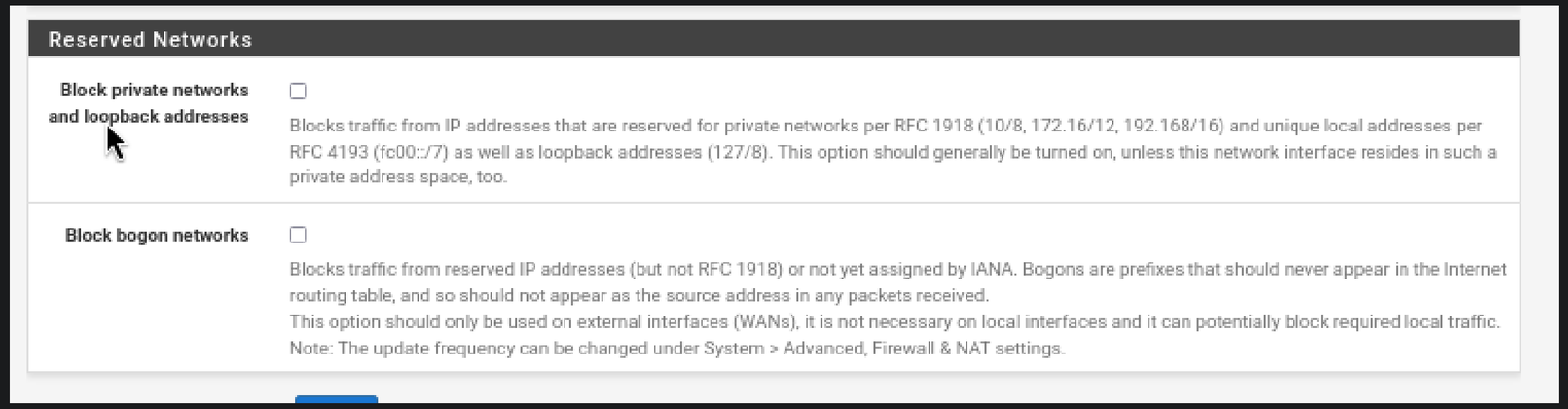


Pour le LAN nous autorisons l'accès au site web à partir du LAN



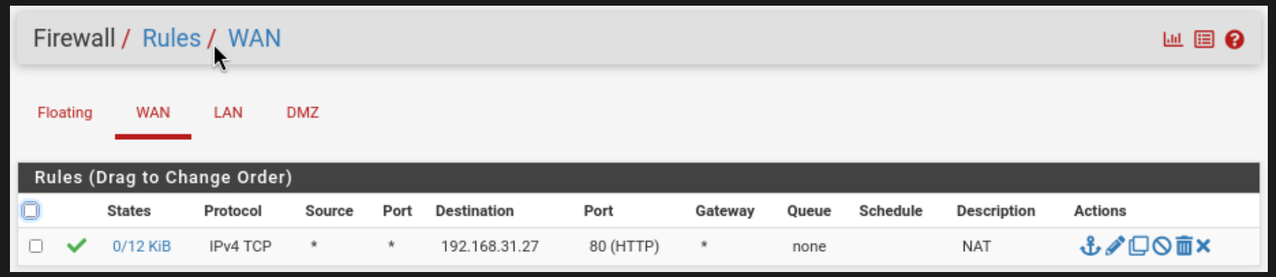
ACCÈS DU WAN VERS LA DMZ

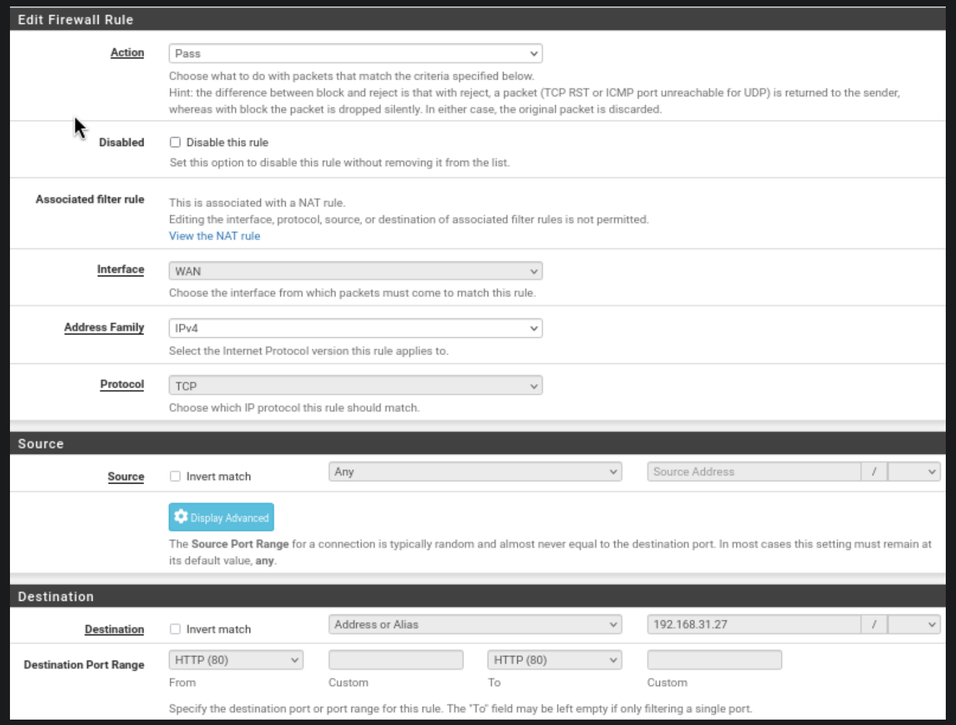
Il va falloir retirer les deux premières règles car elles sont gênantes, pour cela, allez dans “Firewall” → “WAN”, allez tout en bas et décochez les deux cases, enregistrez les changements



ACCÈS DU WAN VERS LA DMZ

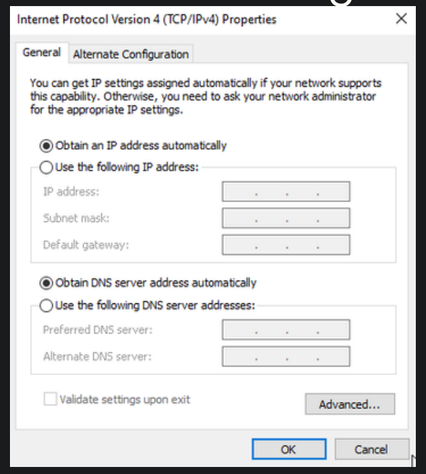
Pour le WAN direction vers le site web sur le port 80





ACCES AU WEB VIA LE WAN

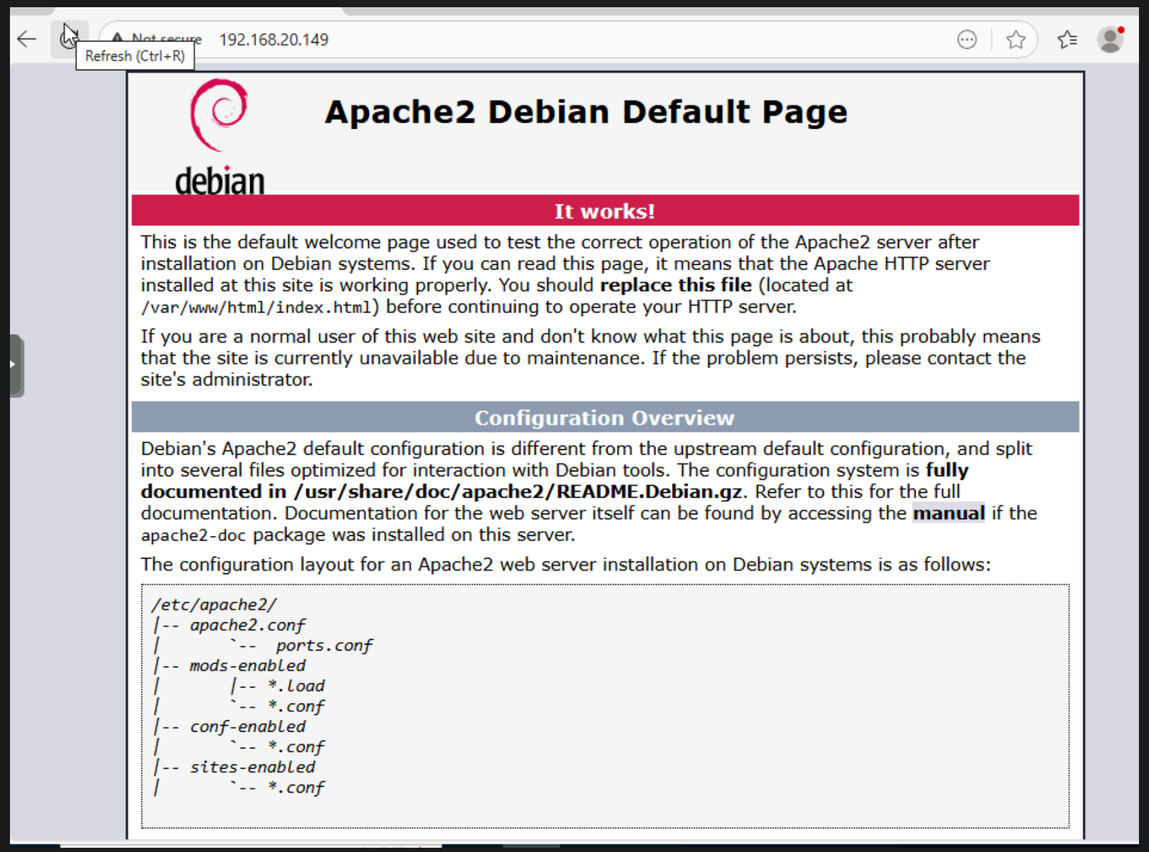
Sur une machine virtuelle Windows 10, sur proxmox, dans Network, je mets la carte réseau de mon WAN.
Dans mes configurations d'adresse ip:



Les données vont être récupérées automatiquement grâce à la carte réseau et ainsi, vous aurez internet:

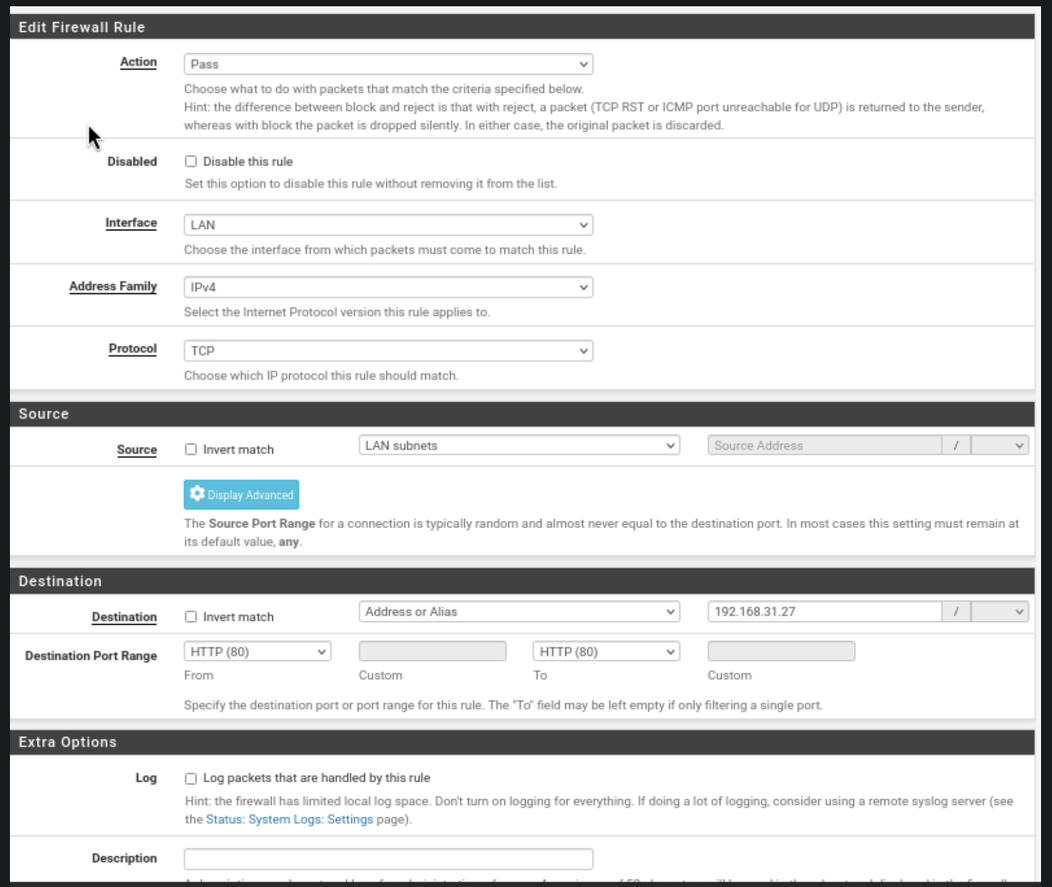
ACCES AU WEB VIA LE WAN

Je me rends sur Edge, je rentre l'adresse ip de mon WAN et je peux bien accéder à l'interface Apache: tout fonctionne bien.



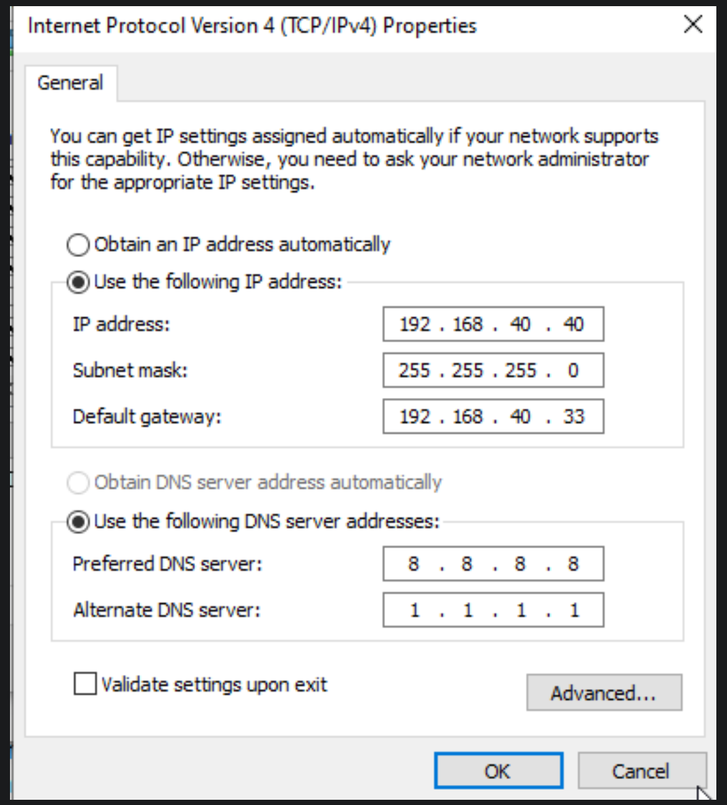
ACCES AU WEB VIA LE LAN

Je me rends dans Firewall → Rules → LAN,
j'ajoute une règle:



ACCES AU WEB VIA LE LAN

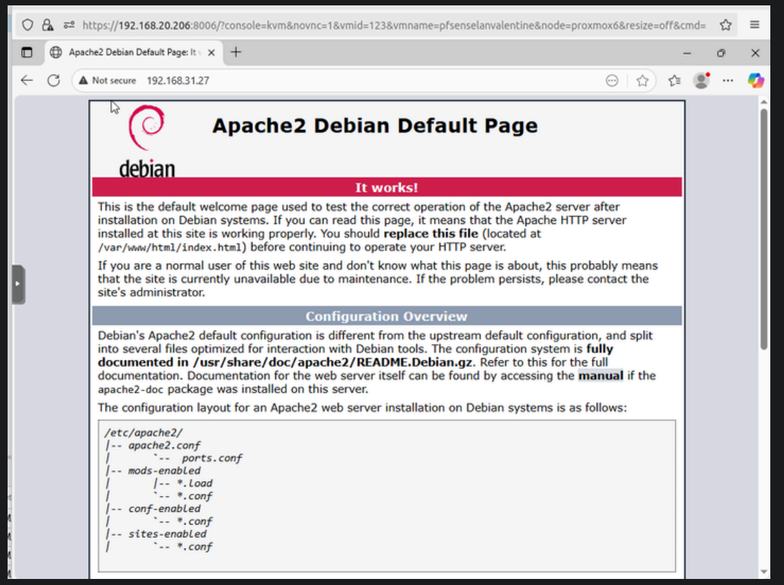
Sur une machine cliente avec la carte réseau du LAN:
J'accède aux paramètres IP:



IP sur la même plage que mon LAN

Gateway = IP du LAN

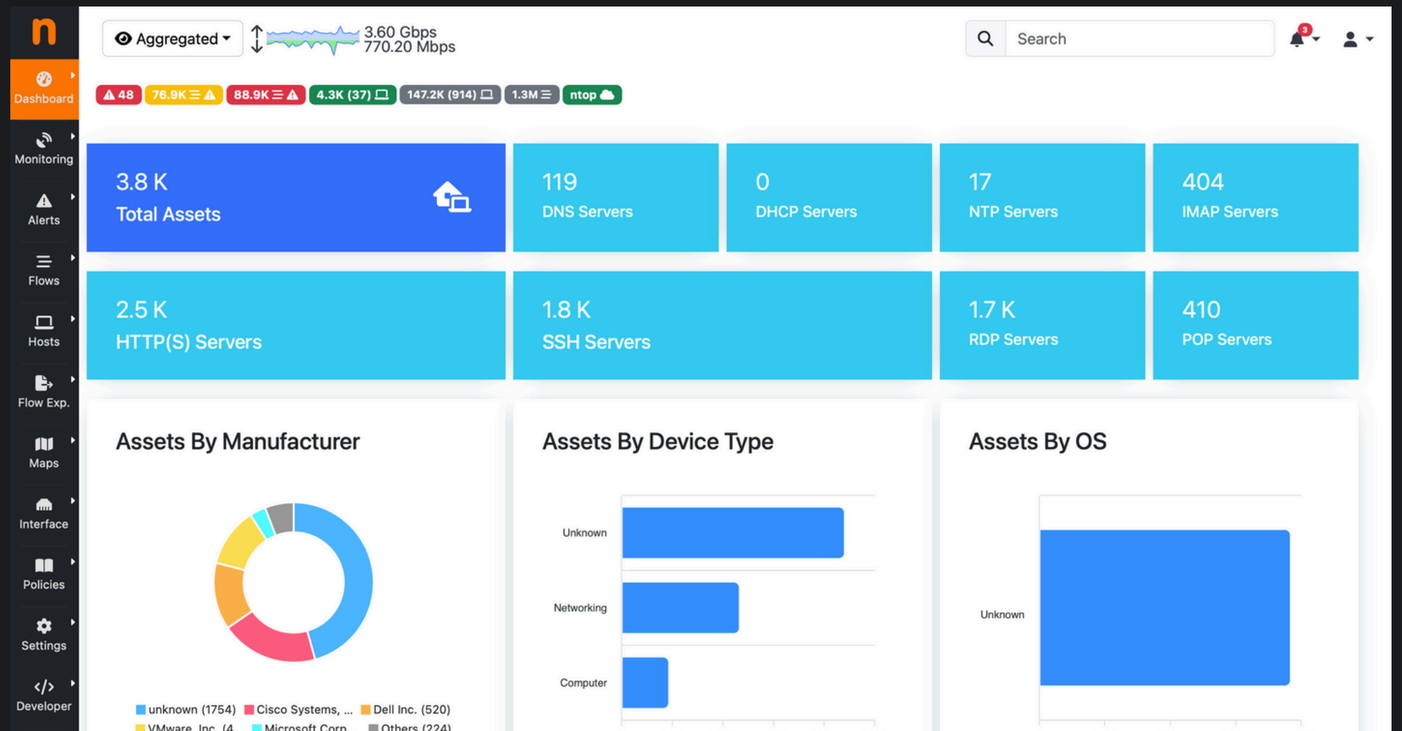
Je peux accéder au site:
le LAN redirige le client vers la DMZ



DMZ ADDON

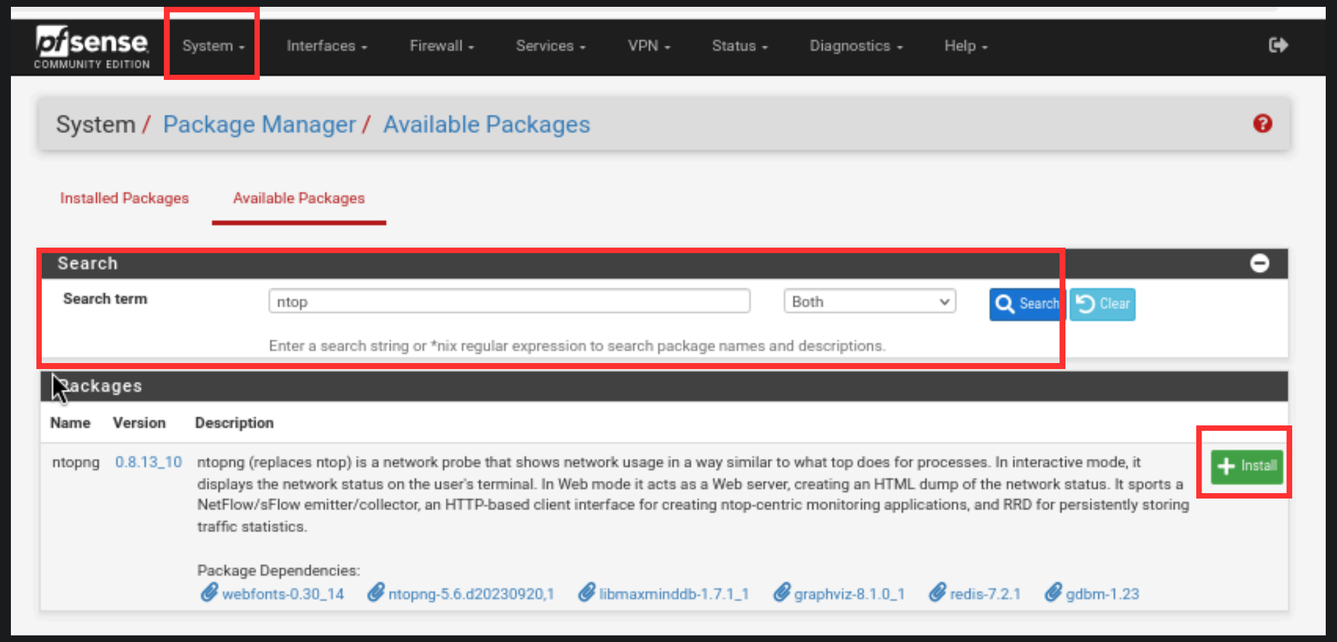
NTOP

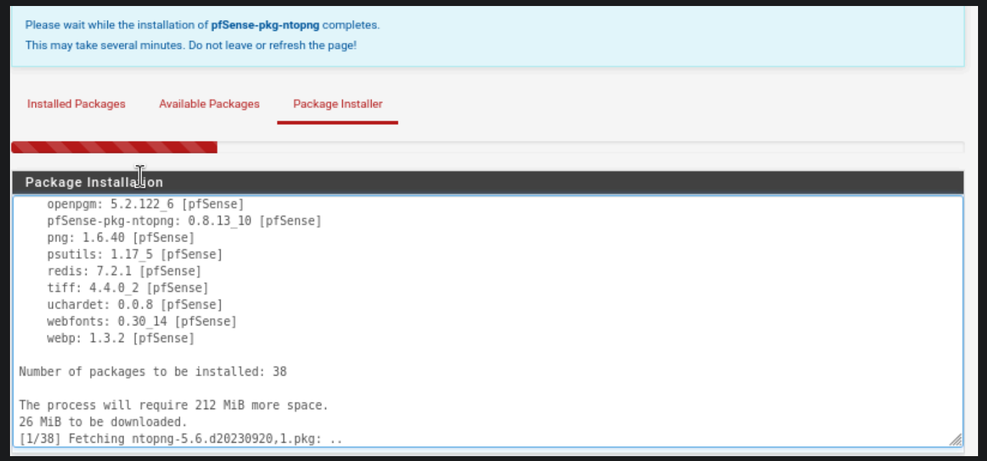
- Il analyse le trafic réseau en temps réel.
- Il détaille les protocoles et adresses IP.
- Son interface web est simple et intuitive.
- Il s'intègre facilement avec pfSense.
- Il aide à détecter rapidement les anomalies.



INSTALLATION DE NTOP

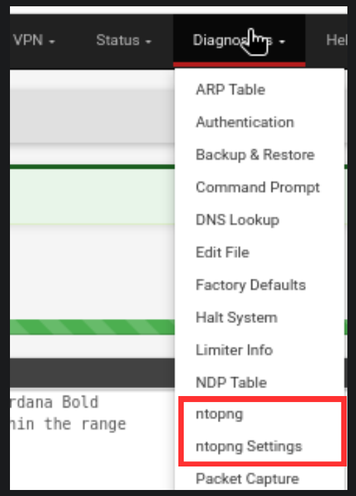
Allez sur votre interface graphique pfsense
Déroulez System → Package Manager → Available Packages
Recherchez ntop et installez le



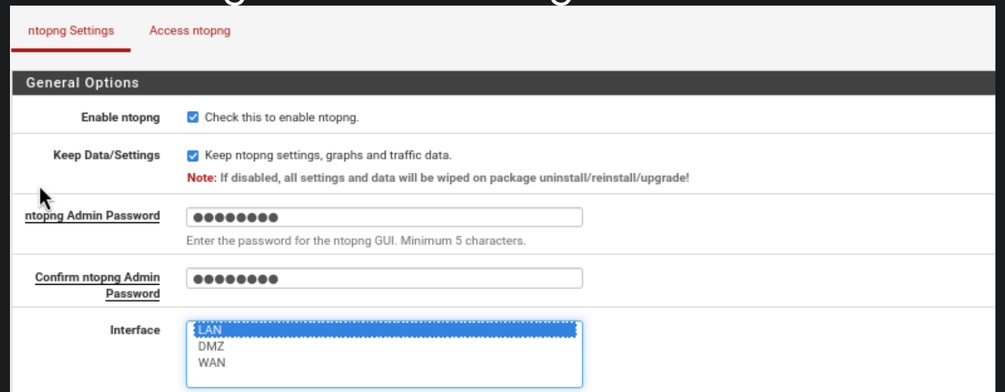


INSTALLATION DE NTOP

L’installation a fait apparaître deux nouvelles options dans “Diagnostics”:

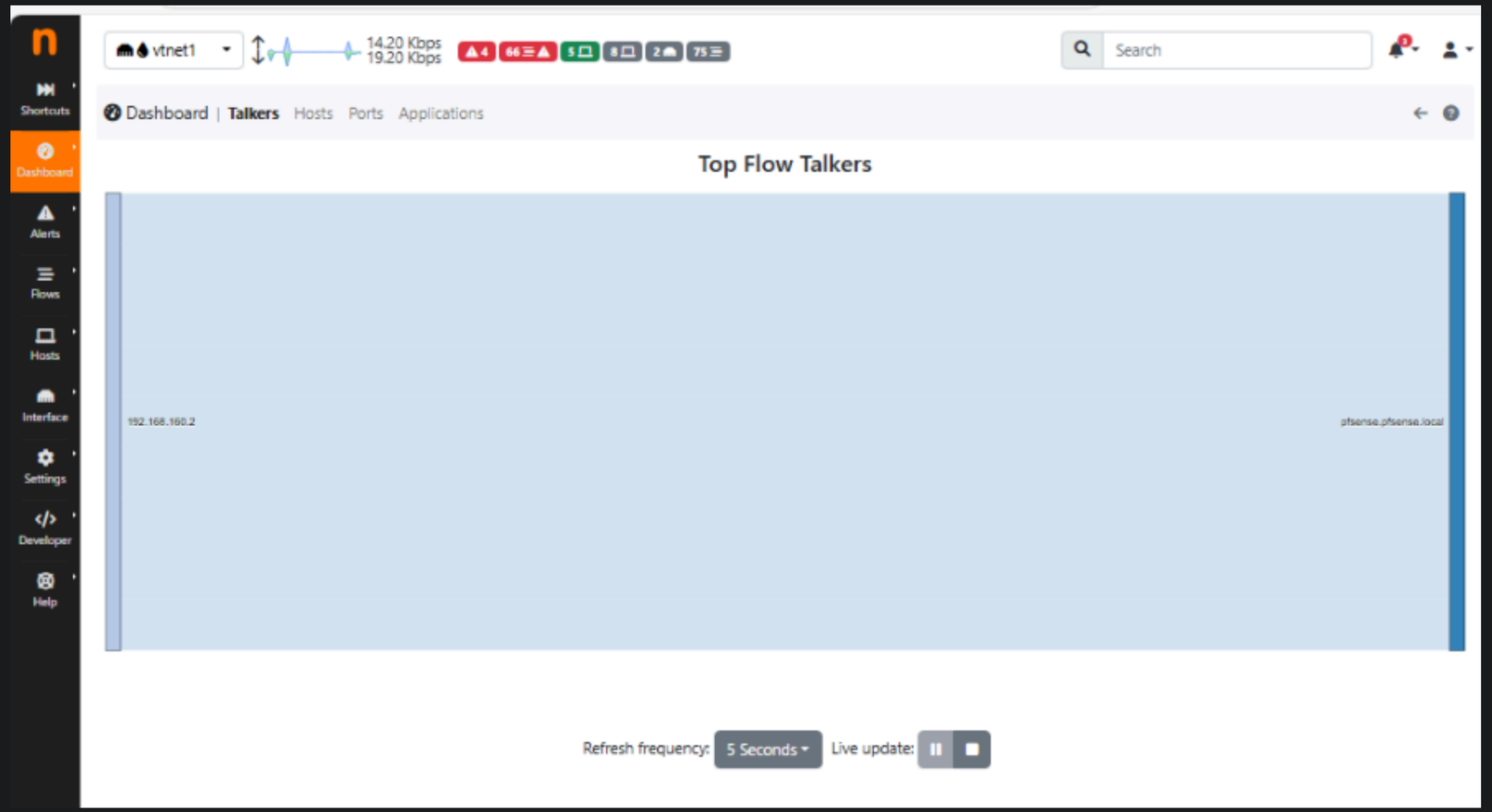


Cliquez sur “ntoppng settings”, cochez “Enable ntopng” puis configurez un mot de passe et choisissez l’interface LAN. Sauvegardez vos changements



INSTALLATION DE NTOP

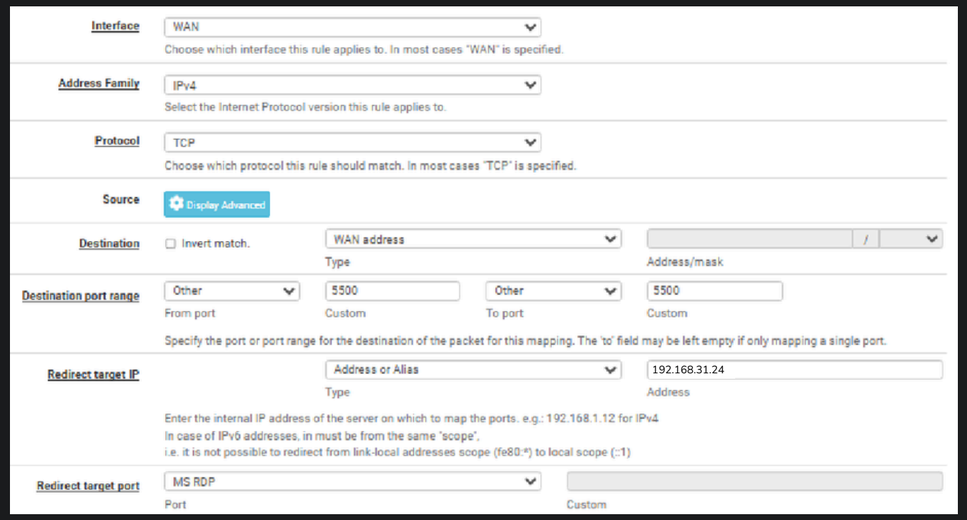
Une fois ceci fait, allez sur Access ntopng et cliquez sur le lien
Avec l'adresse IP de votre machine LAN, vous pourrez accéder à l'interface ntop
Ainsi, vous pourrez monitorer votre réseau



ACCÈS BUREAU À DISTANCE

Ajoutez une machine Windows Server et modifiez sa carte réseau pour y mettre la carte réseau de notre DMZ
Sur cette machine: une adresse IP 192.168.x.2, L'adresse IP DMZ du pare-feu, DNS préféré 8.8.8.8, DNS secondaire 1.1.1.1

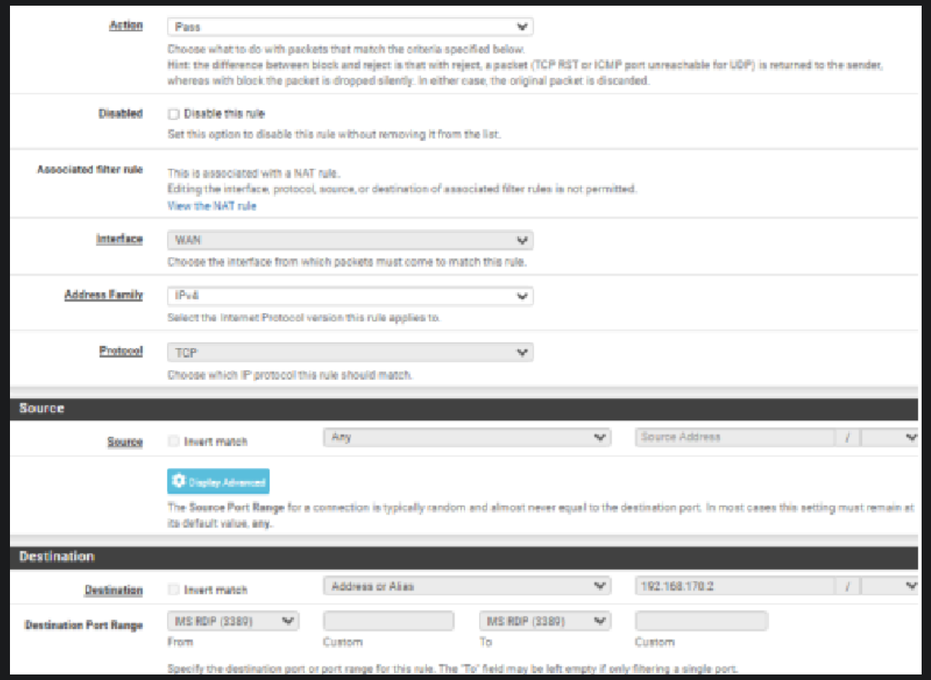
Ajoutons une redirection de port:
Pour cela, allons sur Firewall → NAT → Port Forward → Edit
Ajoutez une règle:
On va faire en sorte que l'interface WAN en Protocol TCP à destination de l'adresse WAN sur le port 5500 (redirection de port pour des raisons de sécurité) redirige vers notre Windows Serveur.



ACCÈS BUREAU À DISTANCE

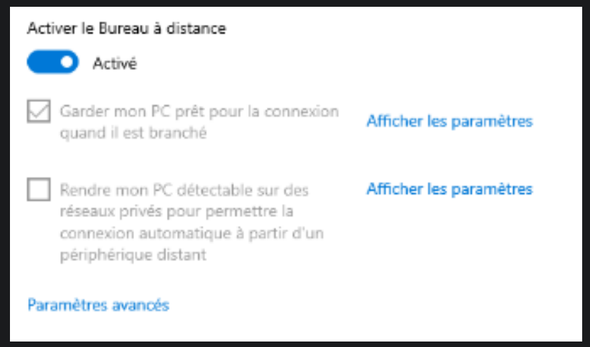
Vérifions dans les règles du WAN si nous avons une règle qui confirme bien la redirection RDP vers Windows serveur:

☐	✔	0/1.19 MiB	IPv4 TCP	*	*	192.168.170.2	3389 (MS RDP)	*	none	NAT Redirection RDP vers Windows Serveur



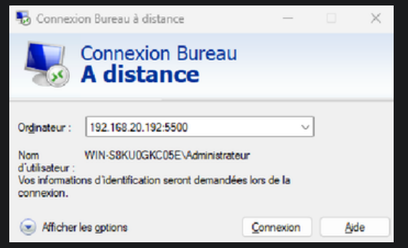
ACCÈS BUREAU À DISTANCE

Il faut maintenant sur votre Windows Serveur autoriser le bureau à distance



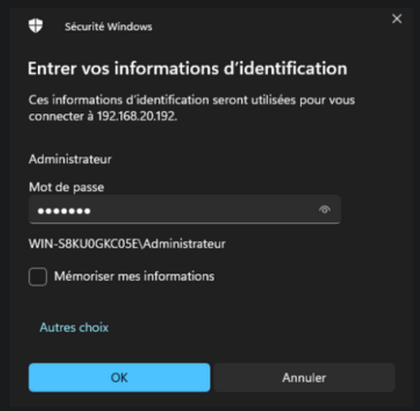
On va ensuite dans la gestion de l'ordinateur et on y ajoute un user s'il n'y a pas de Active Directory (Utilisation de l'administrateur perso)
Nous allons ensuite dans "groupes", on clique sur « Serveurs Accès Distant RDS » et on ajoute notre user.
Ensuite on va dans le panneau de configuration de l'ordinateur-> Système et sécurité -> Système
-> Paramètres d'utilisation à distance et on choisit notre utilisateur: 

Sur notre machine connectée au réseau WAN, allez dans le bureau à distance et connectez vous à votre Windows Server avec l'IP Windows server et son port:



ACCÈS BUREAU À DISTANCE

Entrez les logs:



Vous avez maintenant accès au serveur: