2024-2025

BTS SIO2

TP-PFSENSE /NTOP/RDP

Nicolas Debut

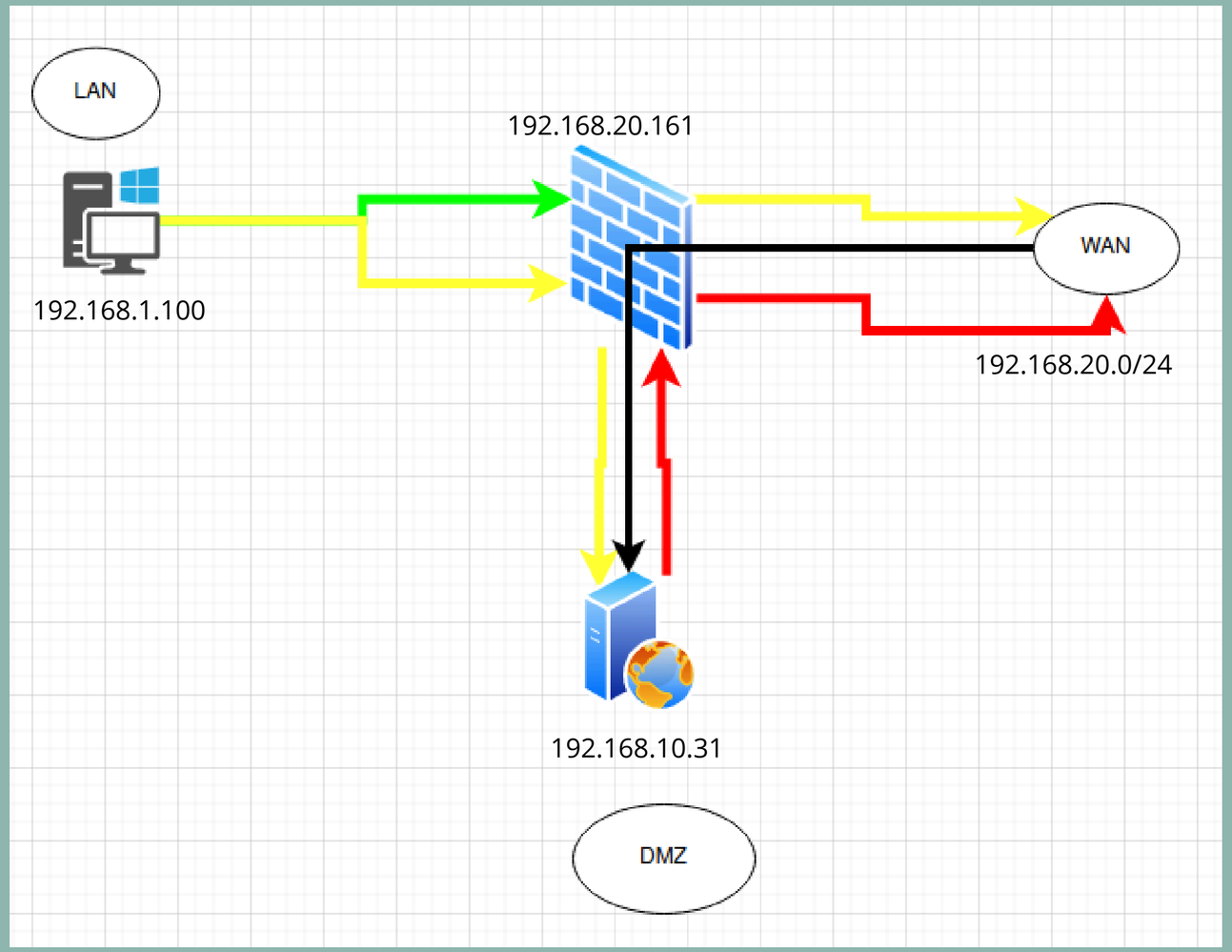
SHÉMA RÉSEAU

→ Redirection WAN vers le site Web

→ Accès du LAN vers WAN et DMZ

→ Accès à la configuration du pfsense

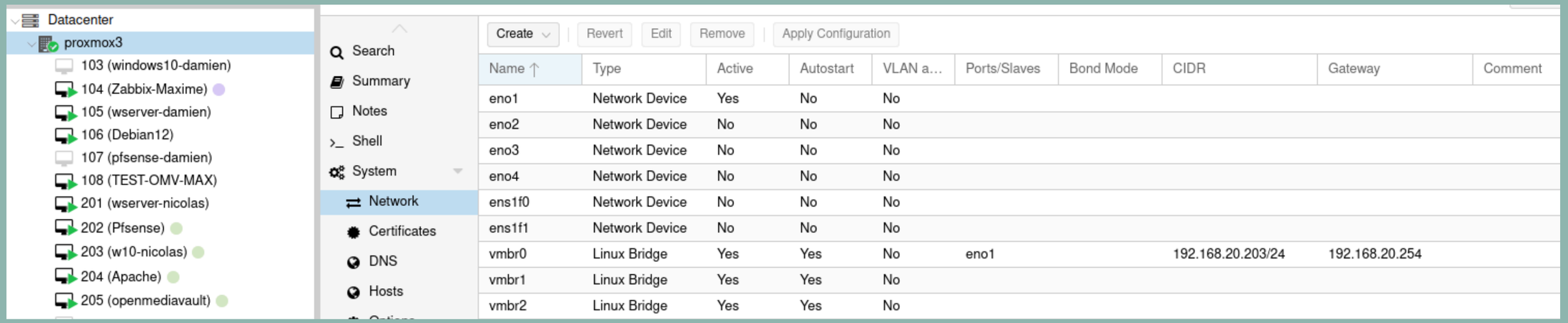
→ Accès de la DMZ vers Internet



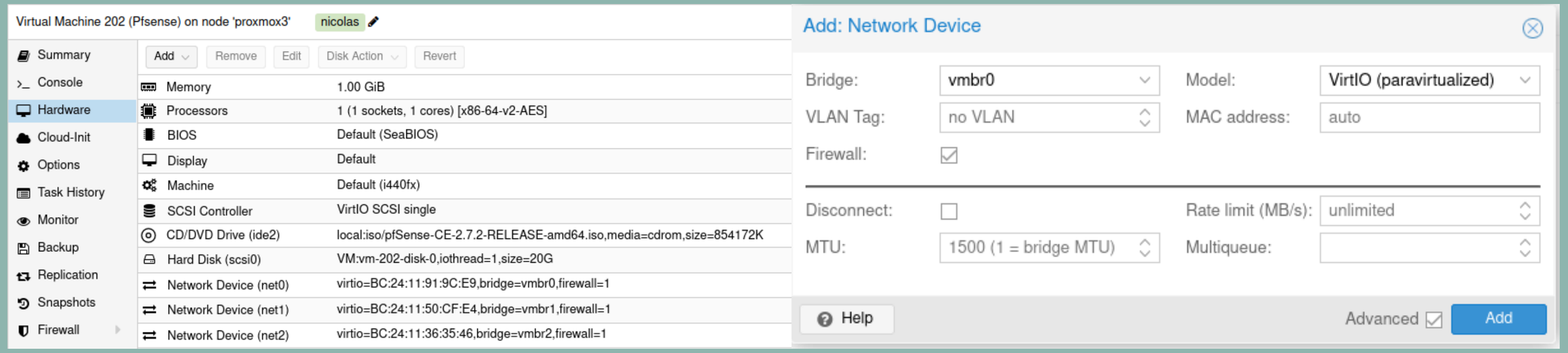
AVANT INSTALLATION

Avant de démarrer votre pfSense pour la première fois, veillez à attribuer 3 interfaces réseau à votre machine.
Pour une VM située sur Proxmox, voici comment procéder :

- **Allez sur Proxmox, puis dans l'onglet Network.**
- **Cliquez ensuite sur Create puis sélectionnez Linux Bridge.**



Name	Type	Active	Autostart	VLAN a…	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
eno1	Network Device	Yes	No	No					
eno2	Network Device	No	No	No					
eno3	Network Device	No	No	No					
eno4	Network Device	No	No	No					
ens1f0	Network Device	No	No	No					
ens1f1	Network Device	No	No	No					
vmbr0	Linux Bridge	Yes	Yes	No	eno1		192.168.20.203/24	192.168.20.254	
vmbr1	Linux Bridge	Yes	Yes	No					
vmbr2	Linux Bridge	Yes	Yes	No					



- **Rendez-vous dans l'onglet de votre pfSense, puis dans la catégorie Hardware.**
- **Cliquez sur Add, puis sur Network Device.**
- **Sélectionnez l'interface réseau que vous souhaitez, puis cliquez sur Add.**
- **Vous devriez ensuite voir l'interface que vous avez ajoutée.**

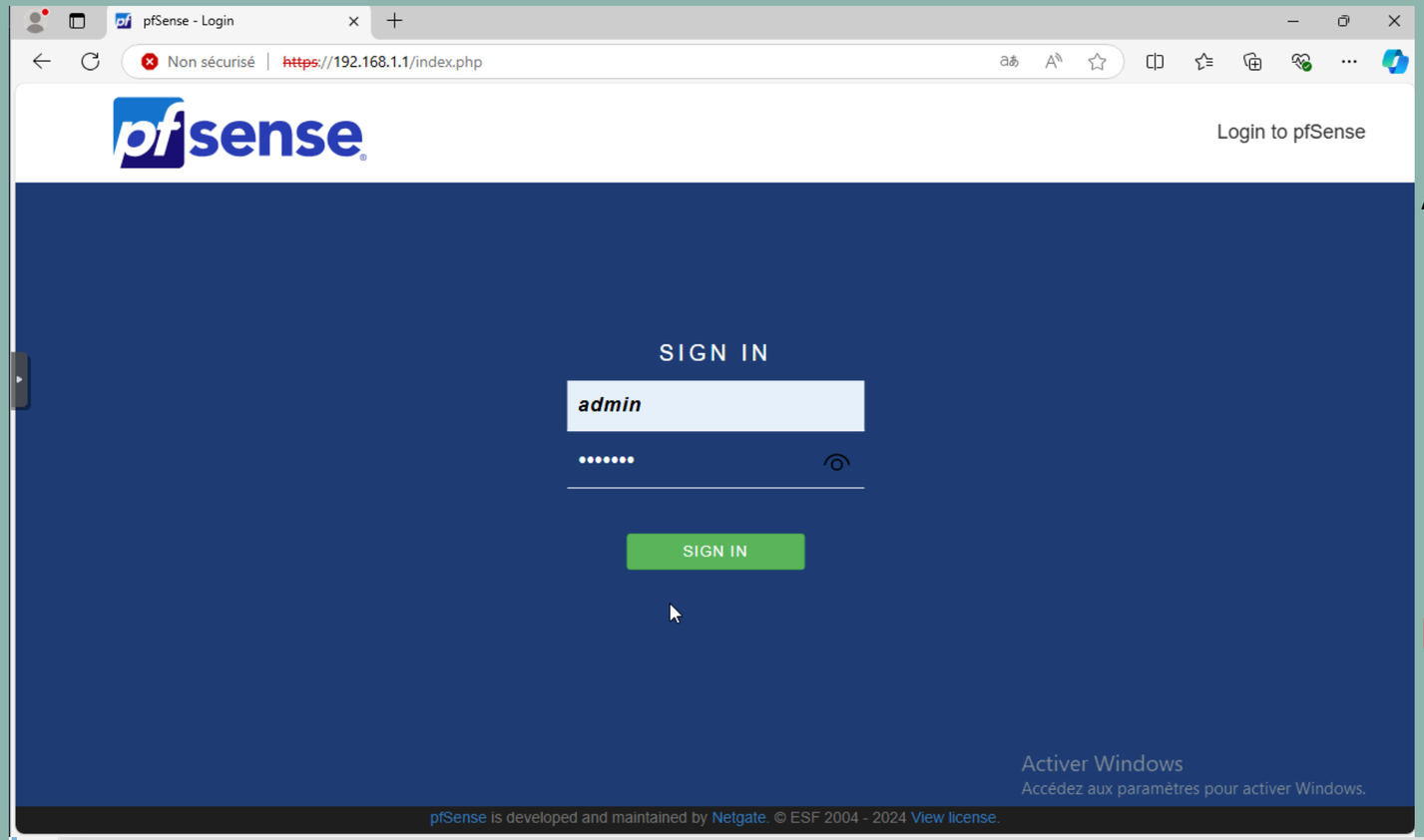
```
Should VLANs be set up now [y|n]? n

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
(vtnet0 vtnet1 vtnet2 or a): vtnet0
```

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 vtnet2 a or nothing if finished): vtnet1

Optional interface 1 description found: DMZ
Enter the Optional 1 interface name or 'a' for auto-detection
(vtnet2 a or nothing if finished): vtnet2
```

```
The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1
OPT1 -> vtnet2

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

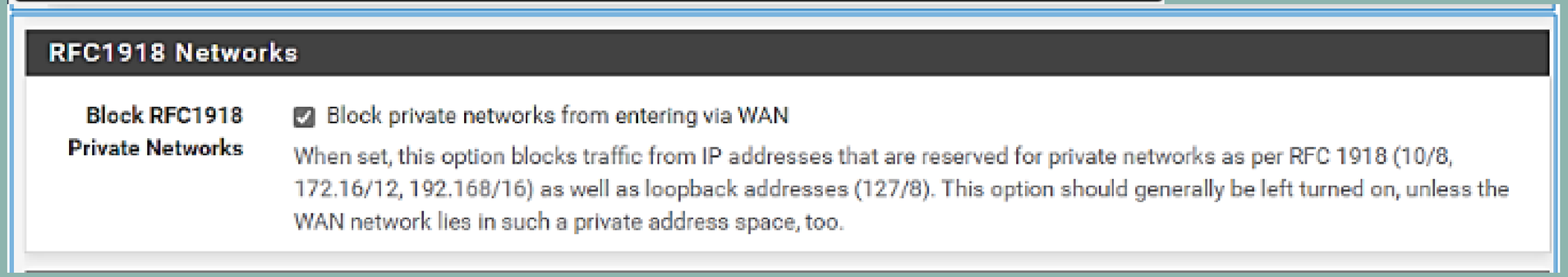
Démarrez ensuite votre VM afin de procéder à l'installation. Une fois celle-ci terminée, associez la bonne interface réseau au bon réseau.

```
(Local Database)



FreeBSD/amd64 (pfSense.nicolasdebut.com) (ttyv0)

KVM Guest - Netgate Device ID: 5f117e33bf87bcffc63e

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

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.20.161/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.1.1/24
 DMZ (opt1)      -> vtnet2     -> v4: 192.168.10.1/24

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

Enter an option:
```

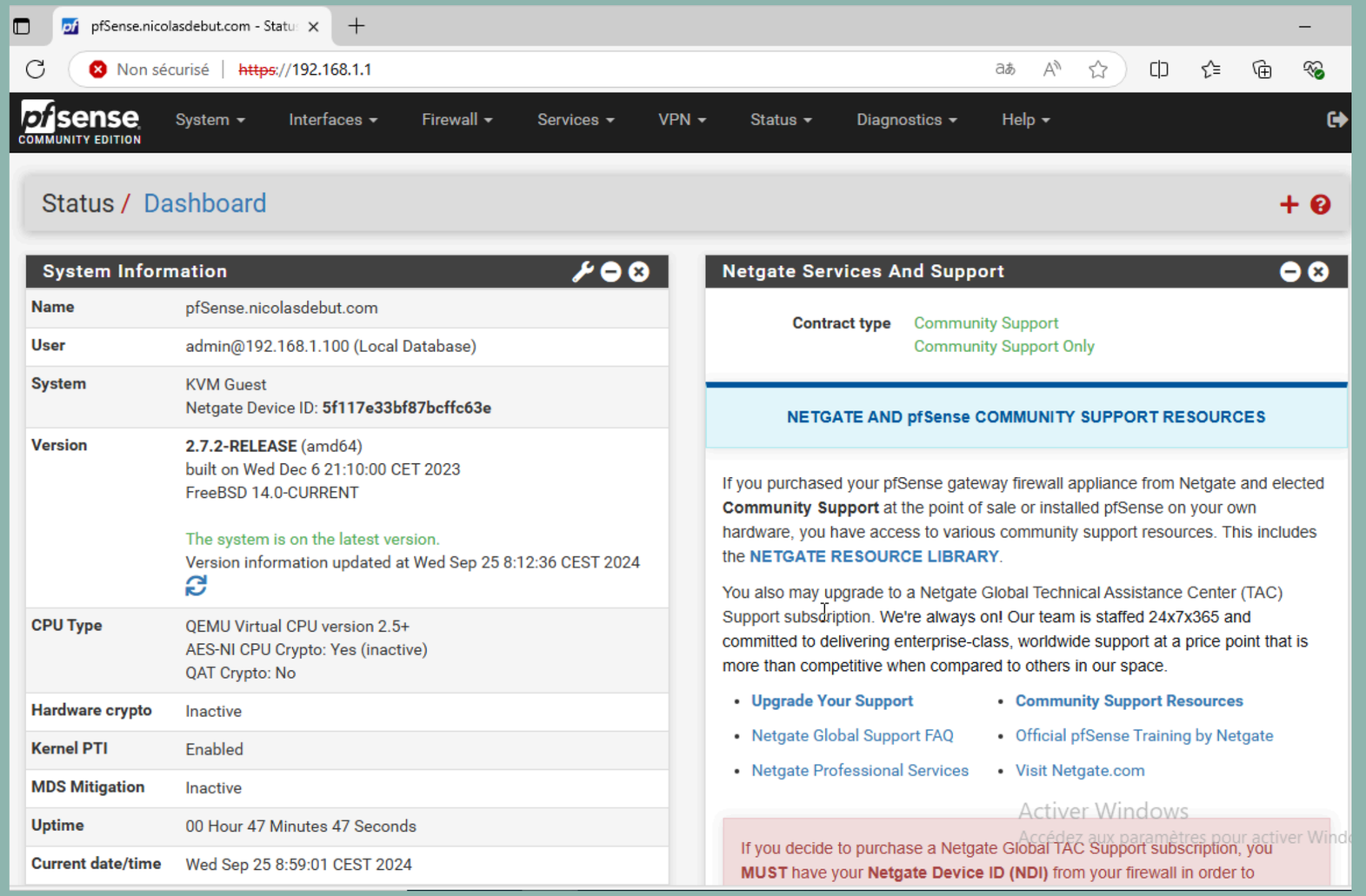


Une fois cela fait, créez une VM en veillant à la connecter à l'interface réseau de votre LAN.
Accédez ensuite à votre pfSense en entrant l'IP de votre LAN dans votre navigateur.
Identifiant par défaut : admin
Mot de passe par défaut : pfsense

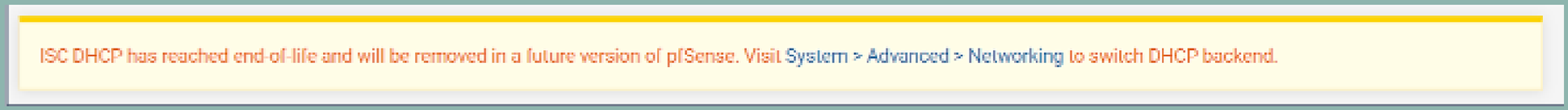
N'oubliez pas de vérifier votre configuration.
!!! Ne pas oublier de désactiver l'option en bas de la page 4/9 pour permettre d'utiliser un réseau privé comme WAN si nécessaire.

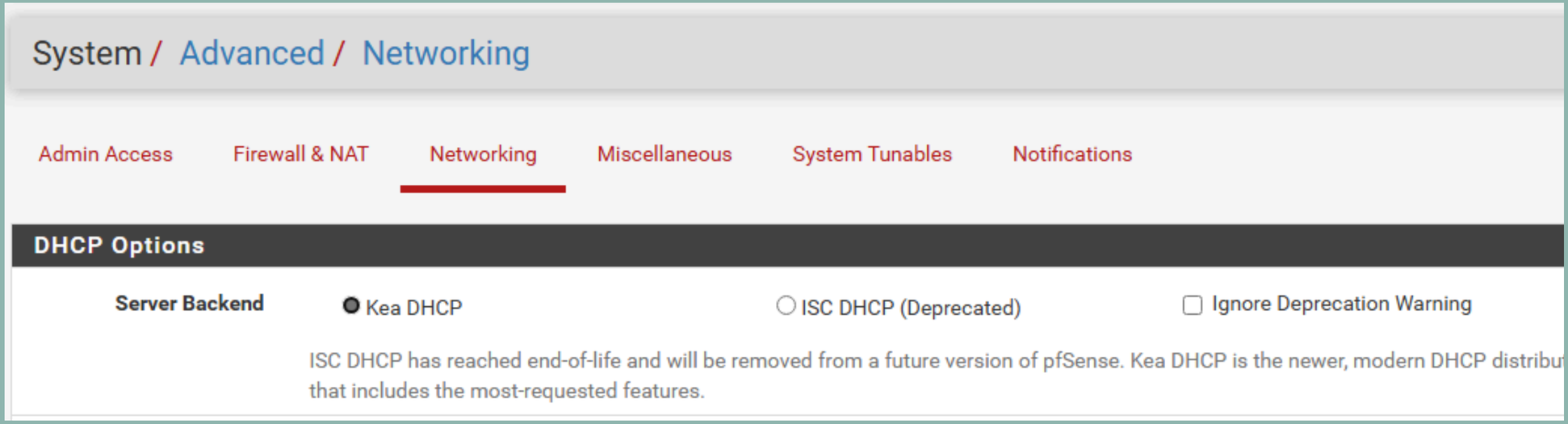


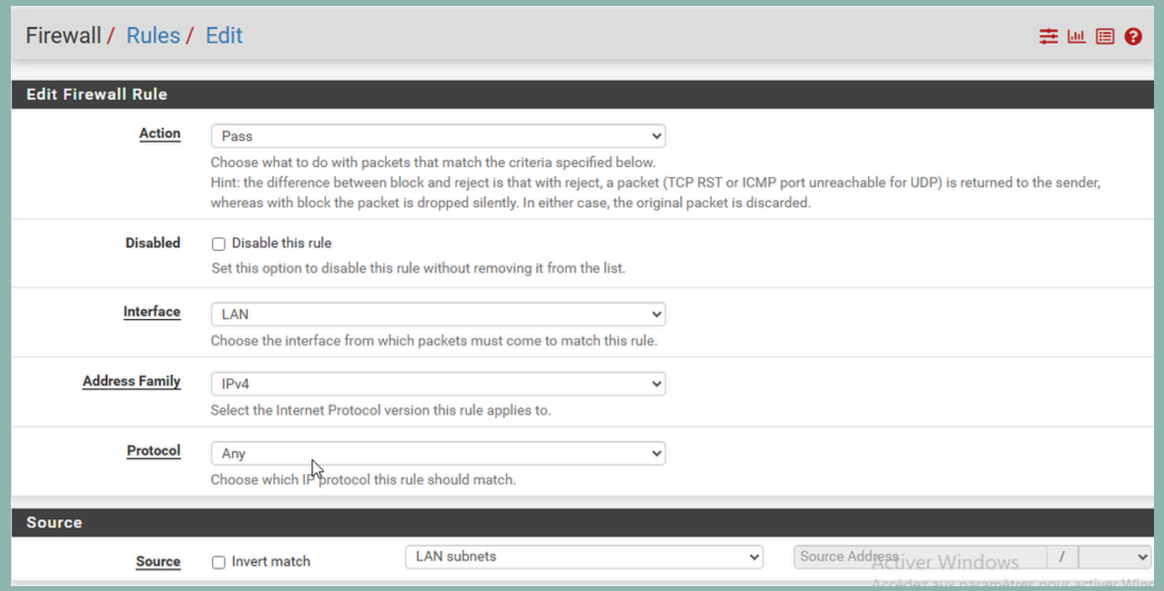
Vous arriverez ensuite sur la page d'accueil de votre pfSense.



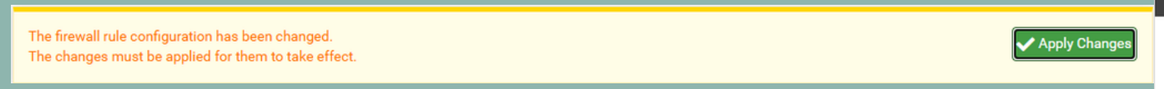
Un message s'affichera pour vous proposer de changer l'option DHCP.
Il est conseillé de passer à la version Kea DHCP, car ISC DHCP n'est plus d'actualité.



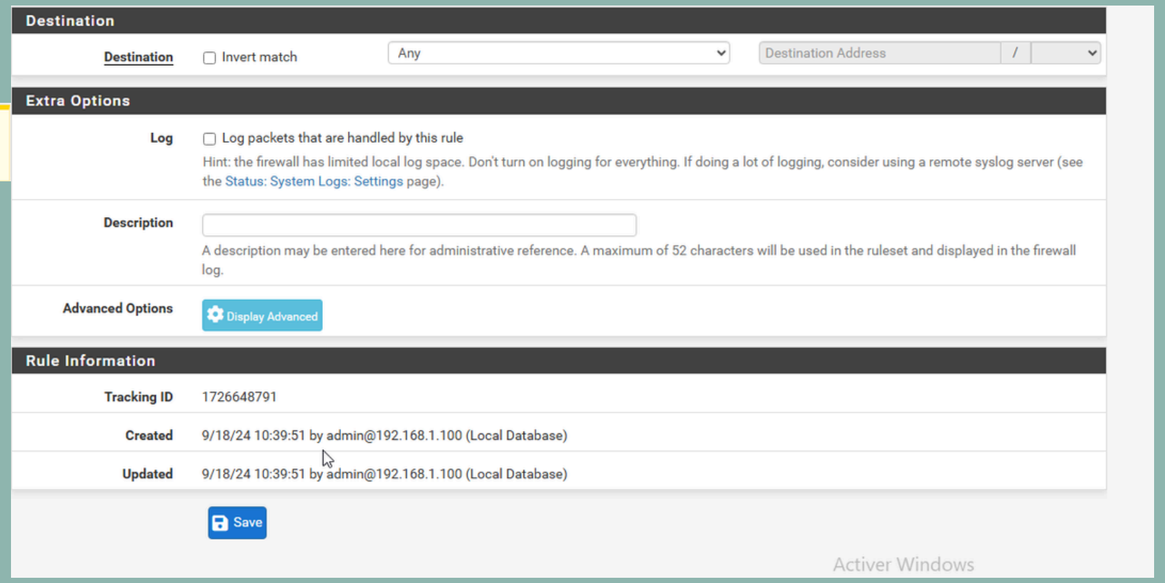


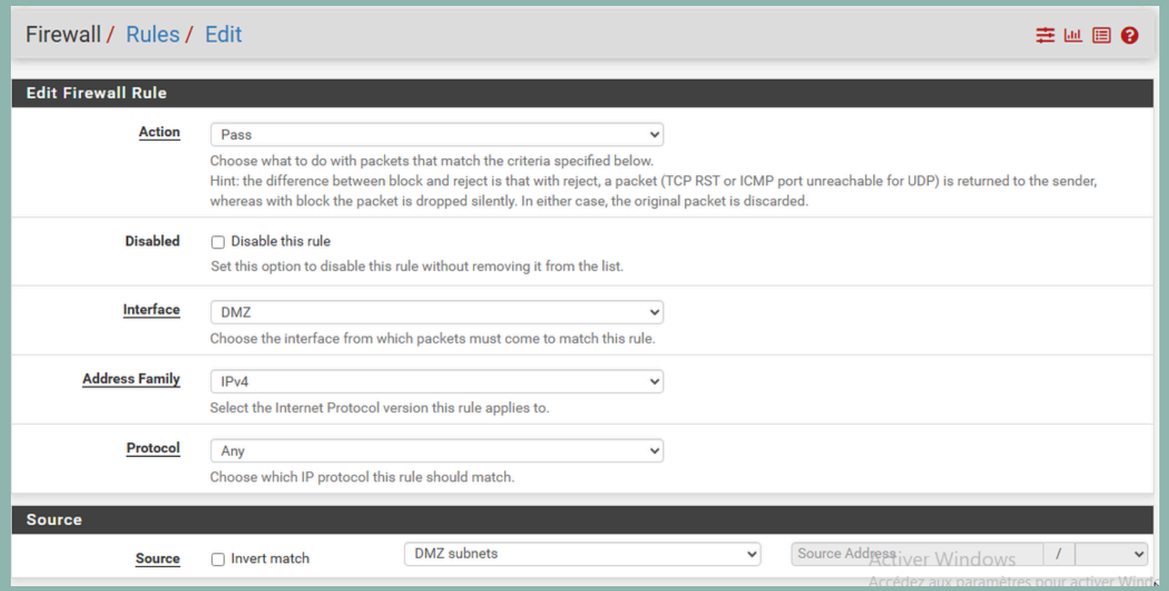


Il est maintenant temps de configurer les règles dans pfSense.
Pour les créer, allez dans Firewall, puis Rules, et cliquez sur Add.
La première règle permettra au LAN d'accéder au web via le WAN (ici, notre réseau de la salle).

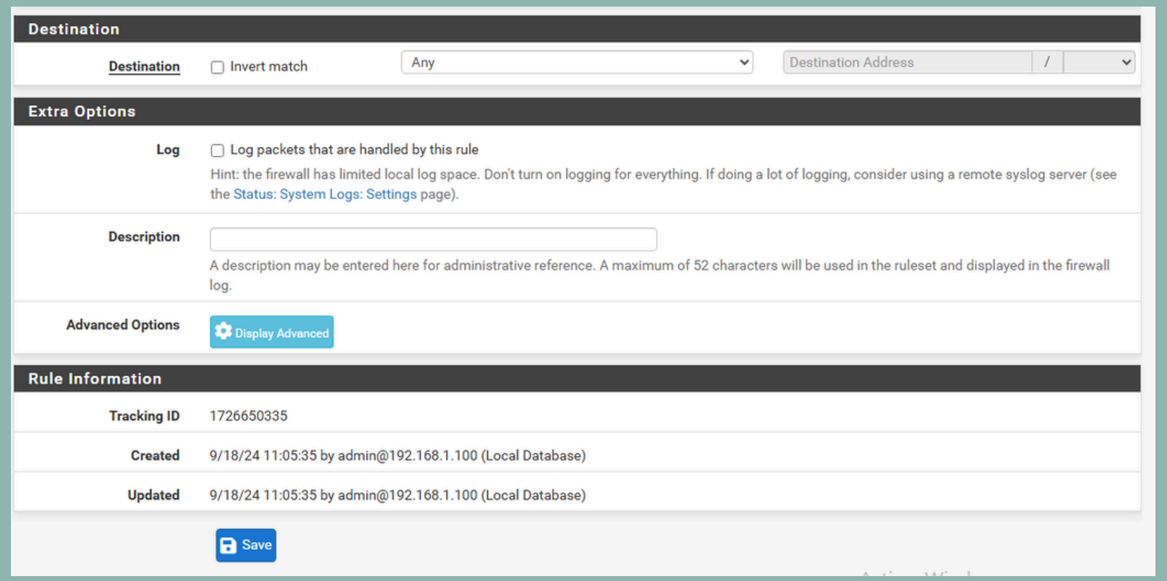


!!! Après chaque règle sauvegardée, cliquez sur Apply Changes, sinon les règles que vous avez mises en place ne fonctionneront pas.

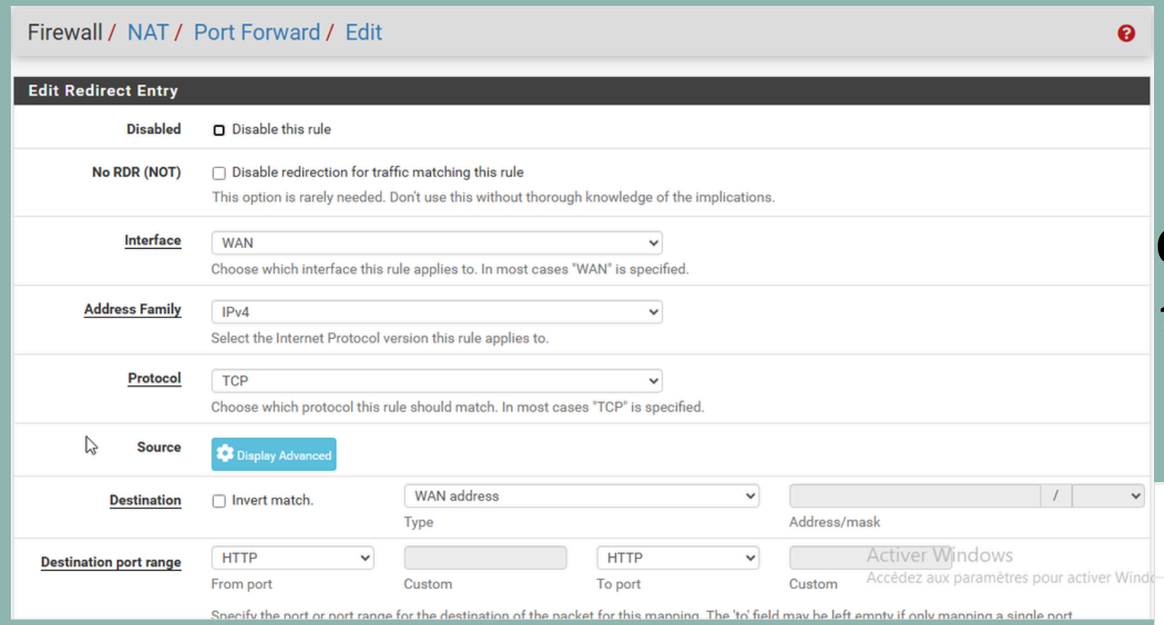


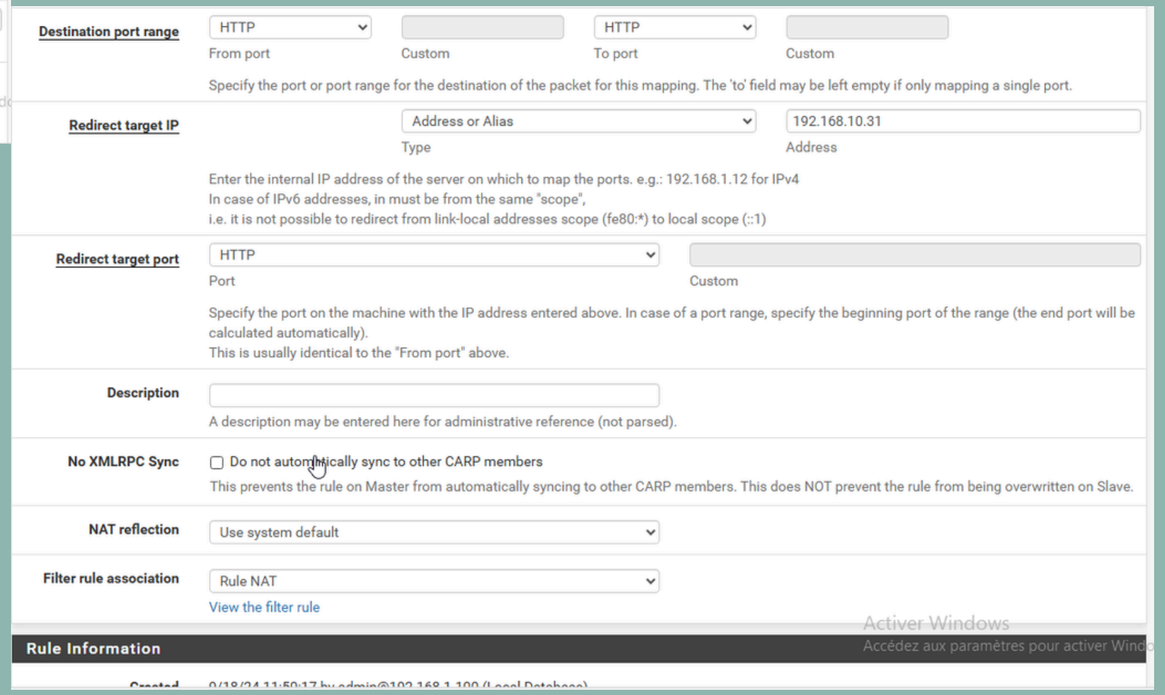


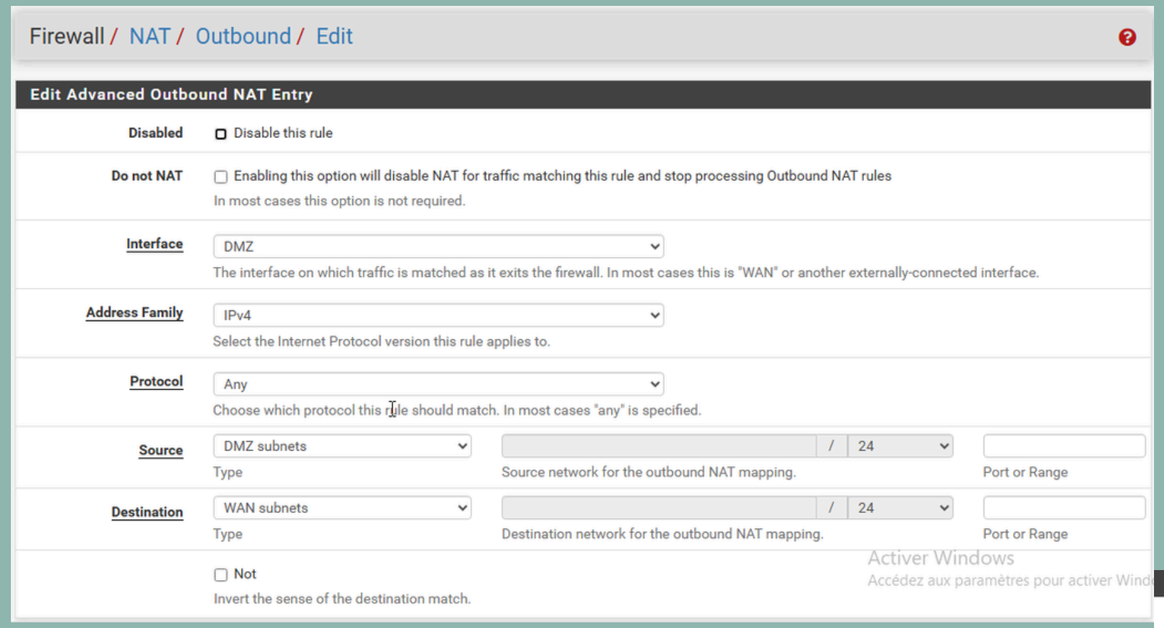
Cette règle autorise les flux sortants de la DMZ.



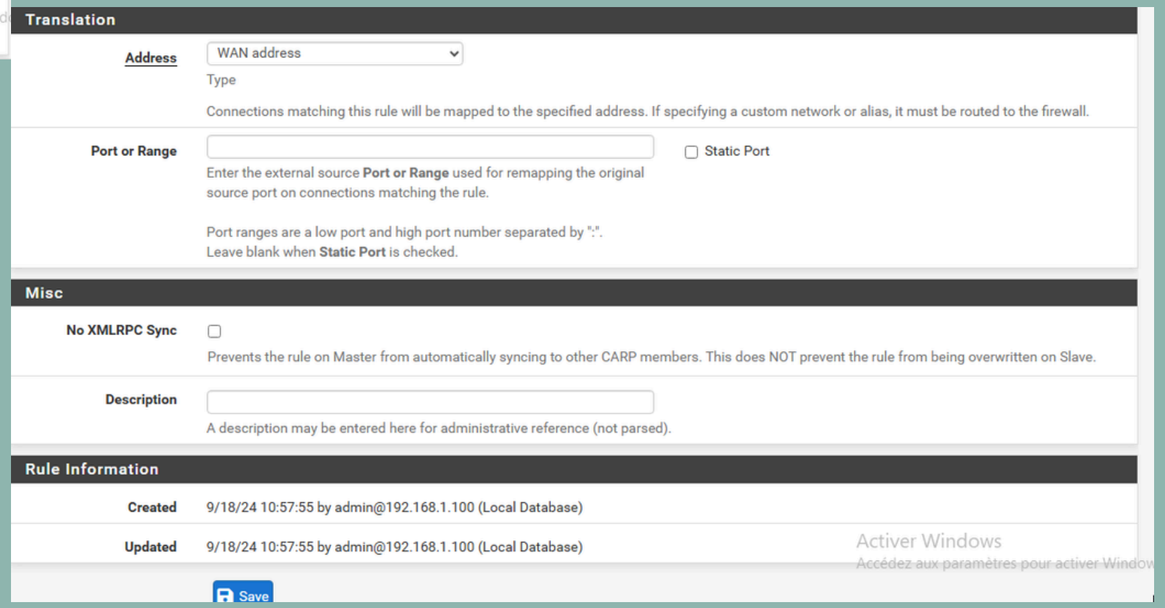
Pour les redirections de port, rendez-vous dans Firewall, puis NAT, et sélectionnez Port Forward. Cliquez ensuite sur Add.
Cette redirection fera en sorte que, si le WAN tente de se connecter à votre pfSense, il sera immédiatement redirigé vers votre serveur web.







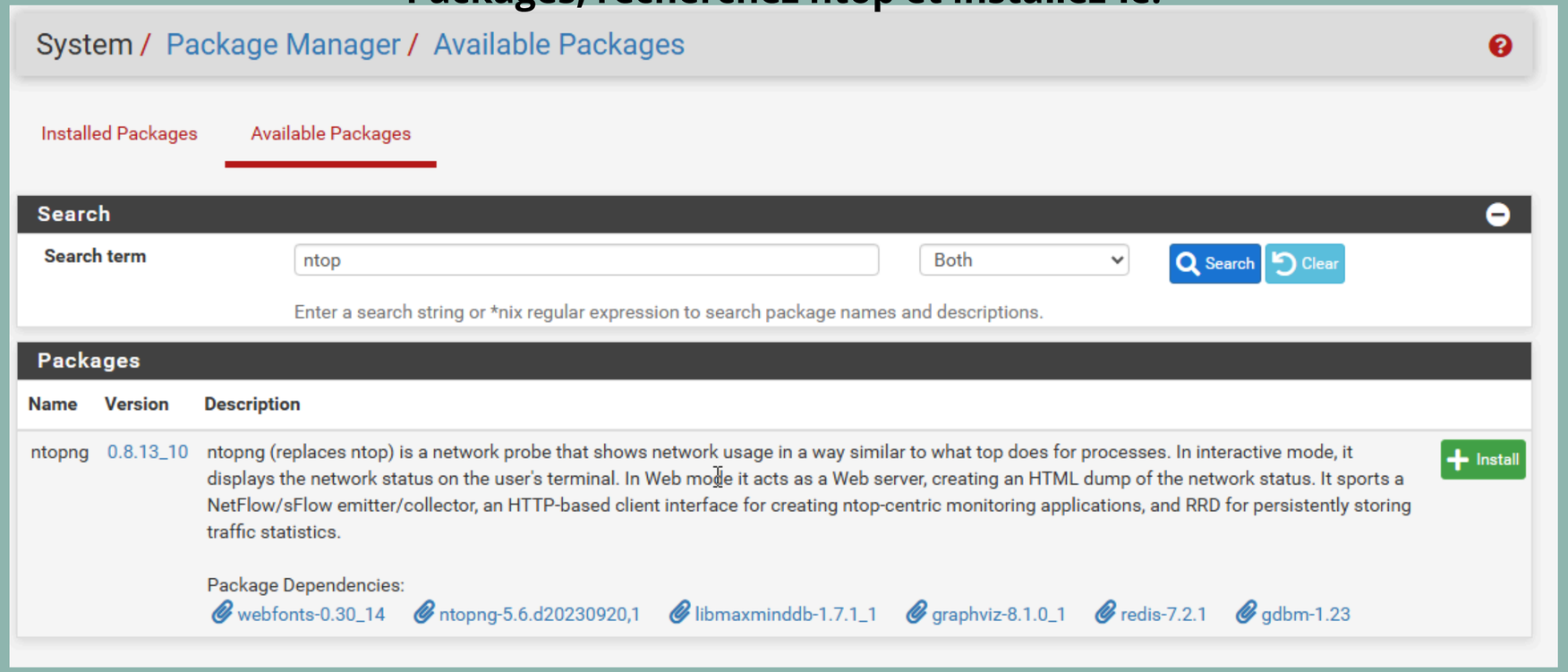
Ici, vous trouvez la règle permettant à la DMZ d'accéder à Internet via le WAN.



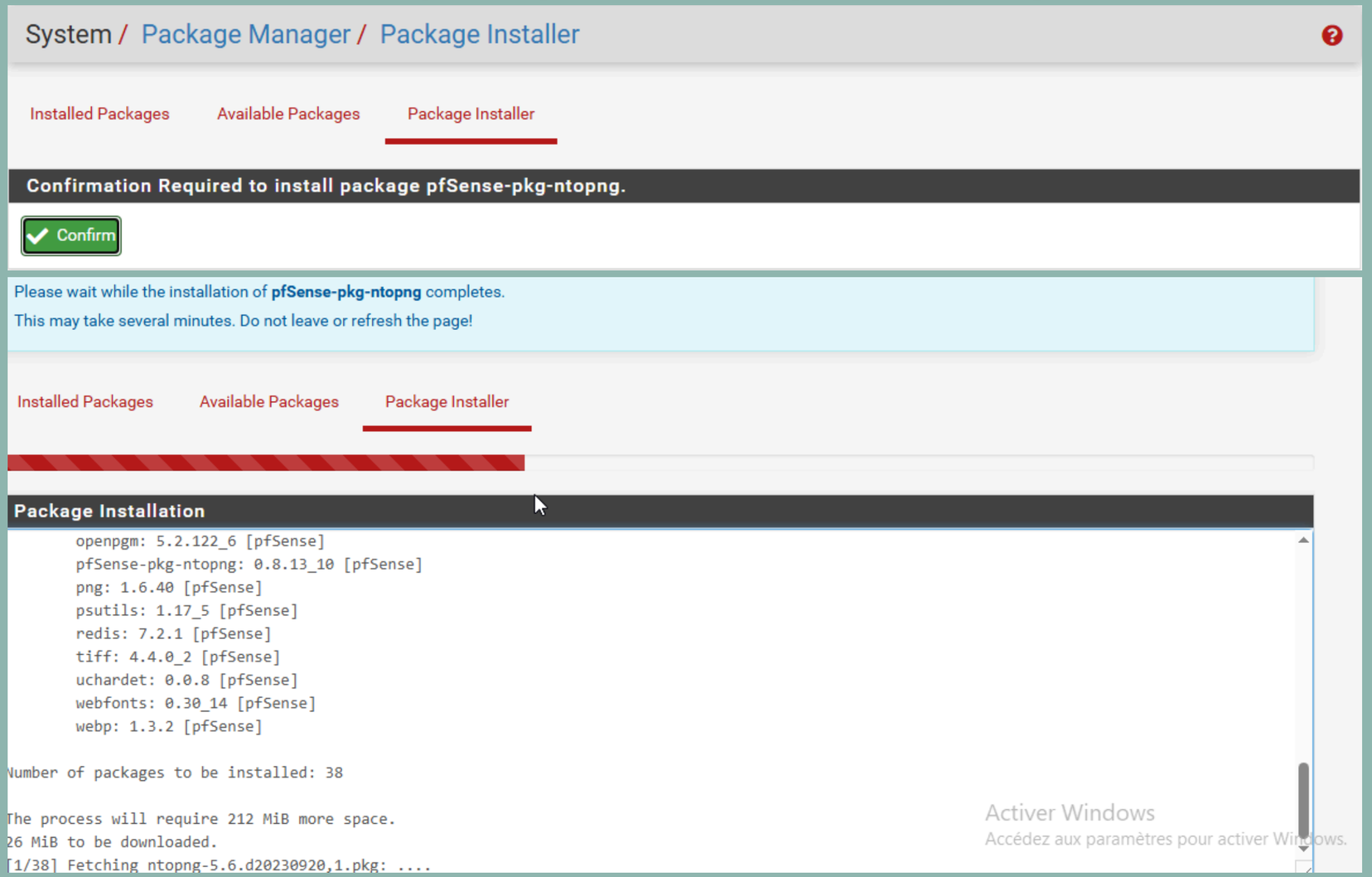
Si, depuis votre WAN, vous entrez l'IP de votre pfSense dans votre navigateur, vous serez redirigé vers votre serveur web situé dans votre DMZ.

NTOP

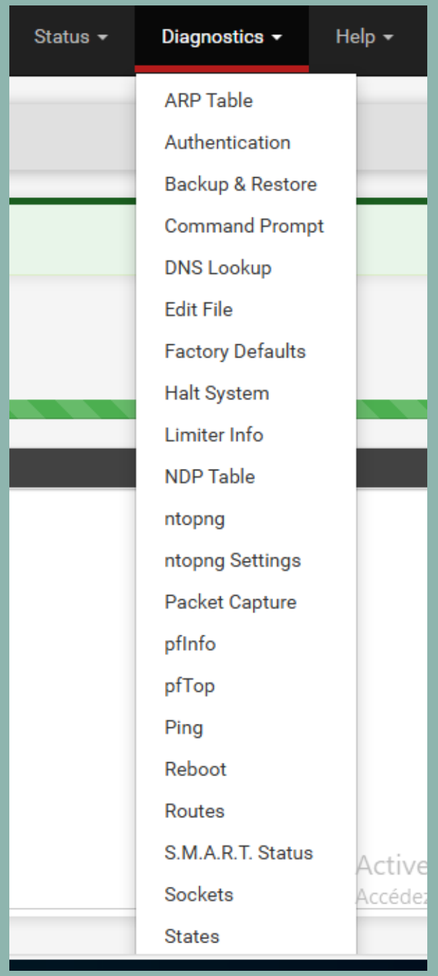
NTOP est un outil très utile si vous souhaitez superviser l'activité qui se déroule sur votre pfSense, il est inclus dans celui-ci il vous suffit juste de mettre un plugin.
Pour l'installer, vous devrez vous rendre dans l'onglet System, puis Package Manager. Cliquez sur Available Packages, recherchez ntop et installez-le.

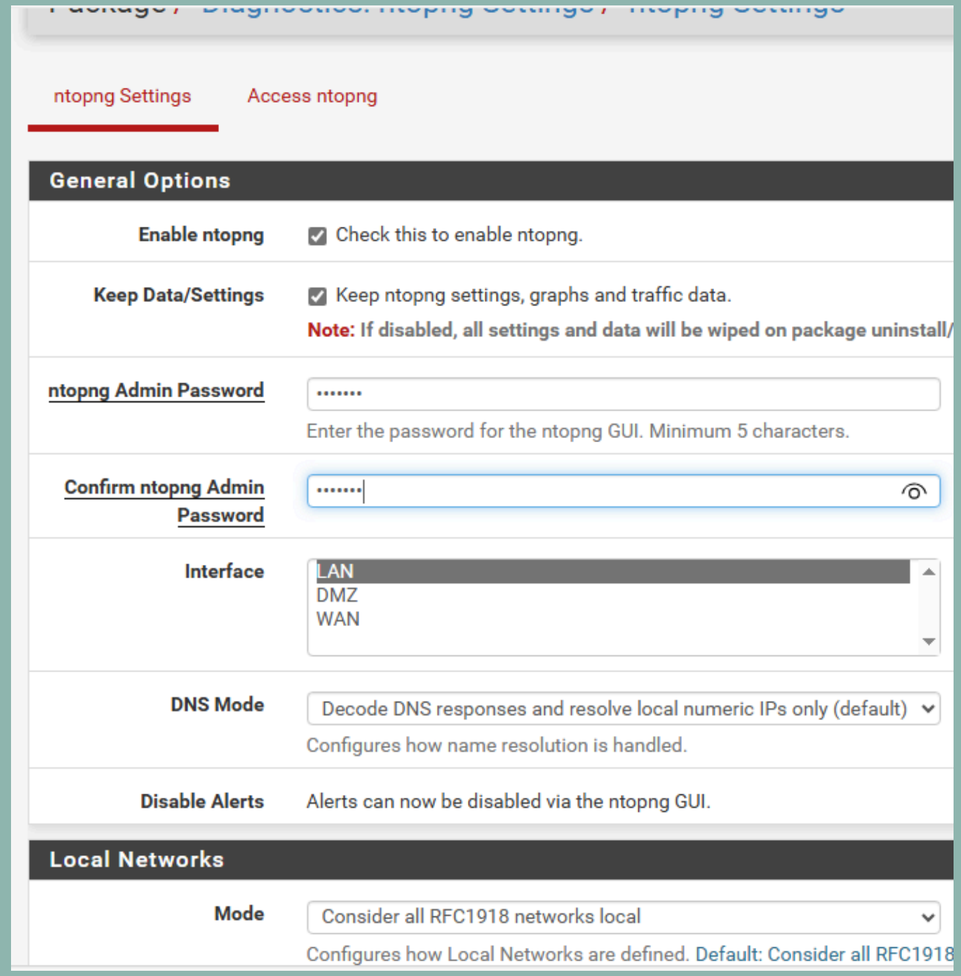


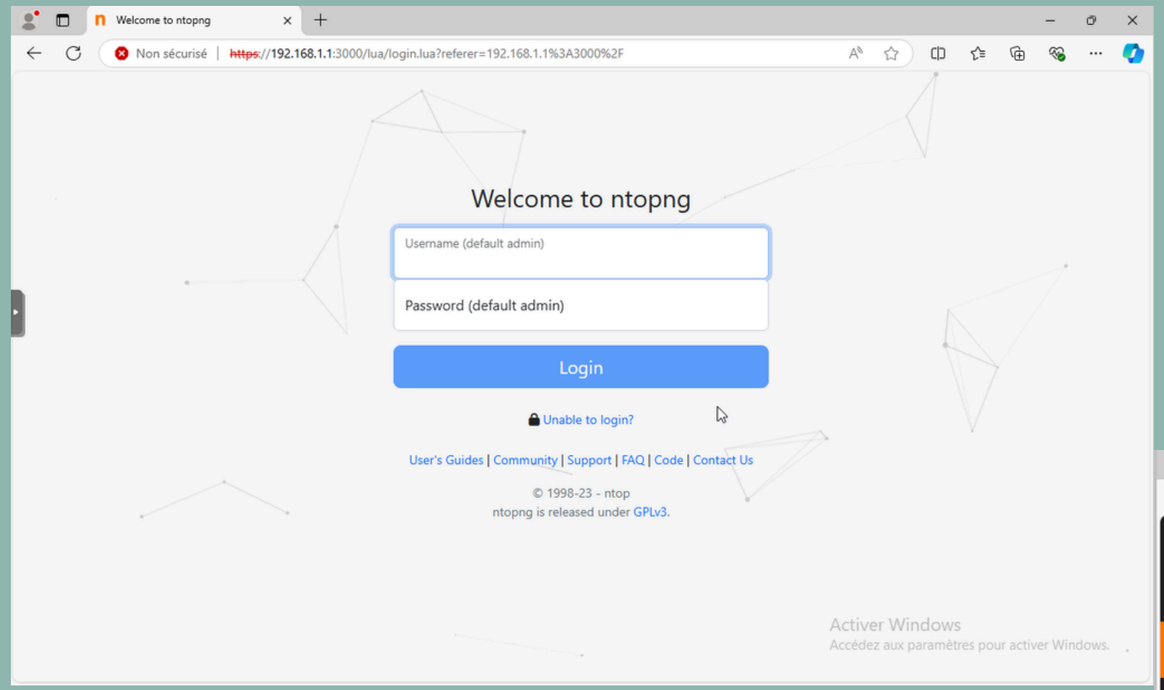
Confirmez l'installation, puis patientez pendant que celle-ci s'effectue.



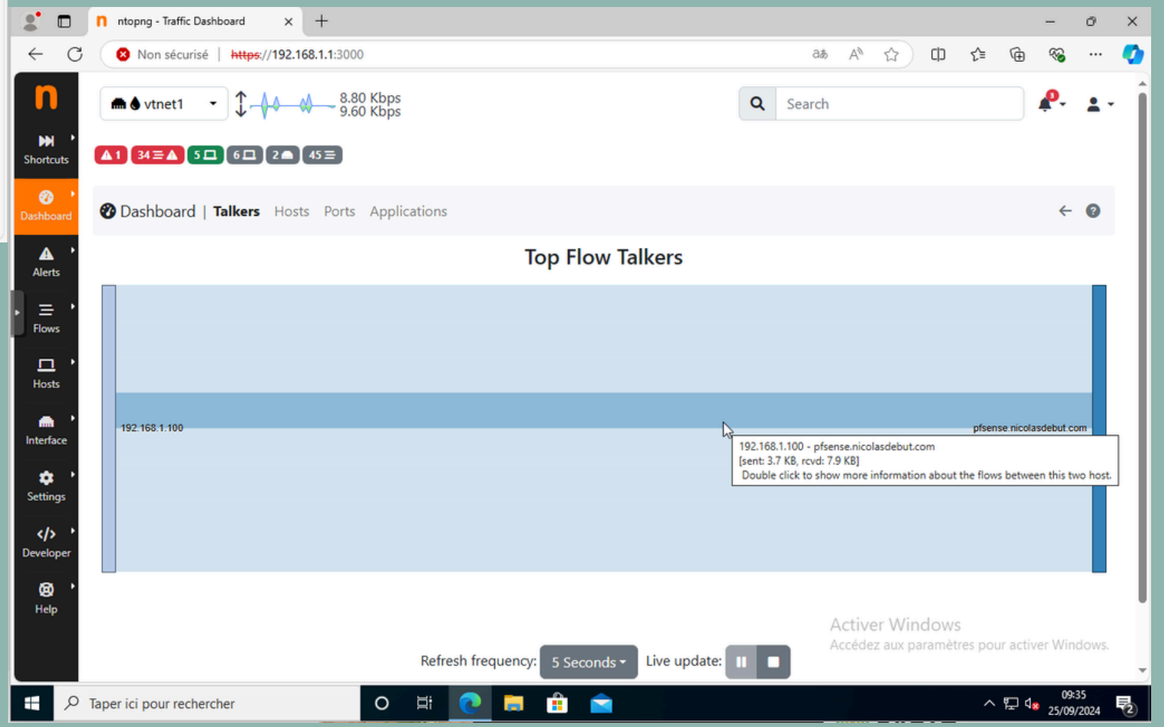
Une fois installé, allez dans Diagnostics, puis dans ntopng Settings, activez le service et indiquez l'interface à surveiller.





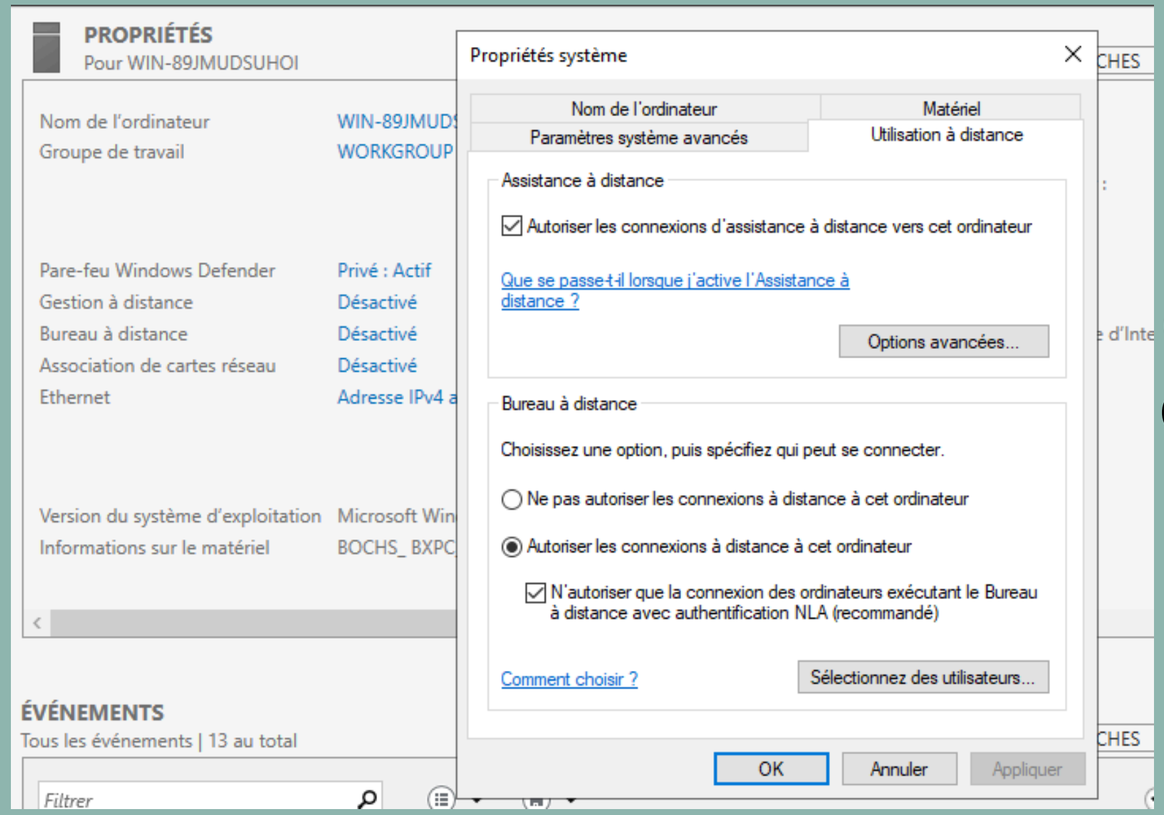


Cliquez ensuite sur Access ntopng pour accéder au service ; indiquez votre identifiant et votre mot de passe, et voilà, votre service est installé.

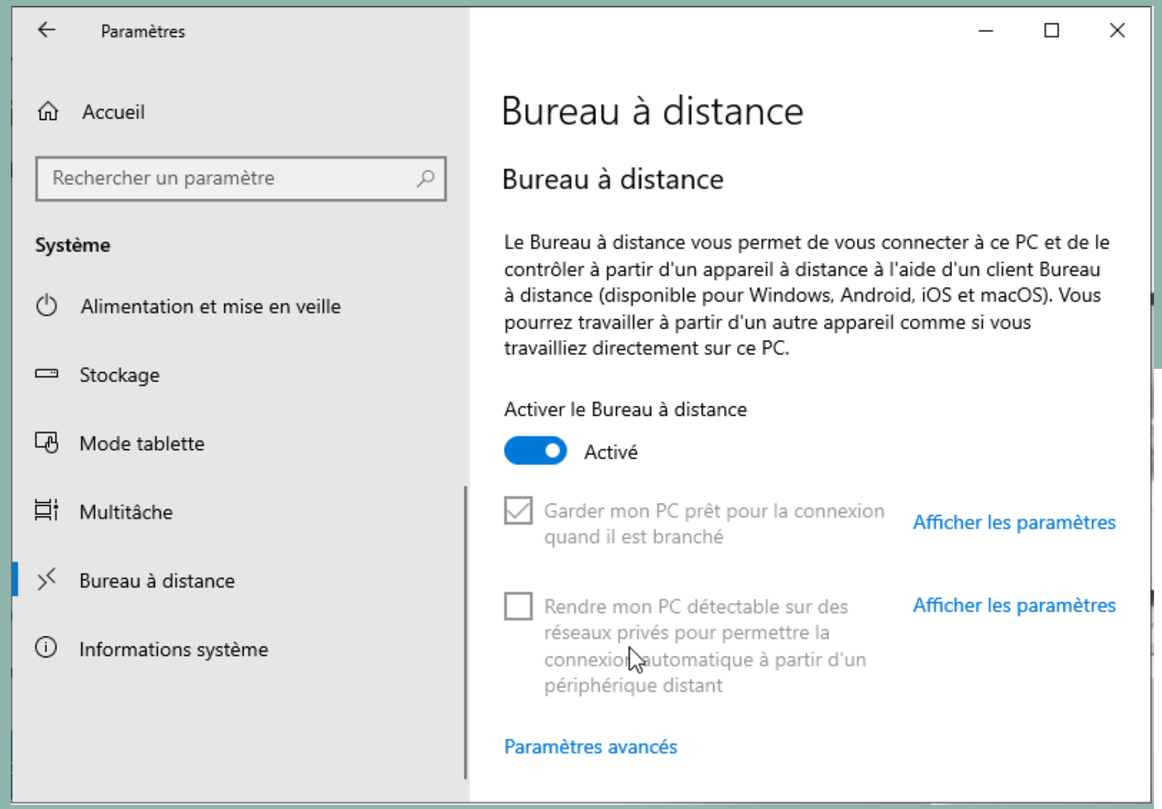


RDP

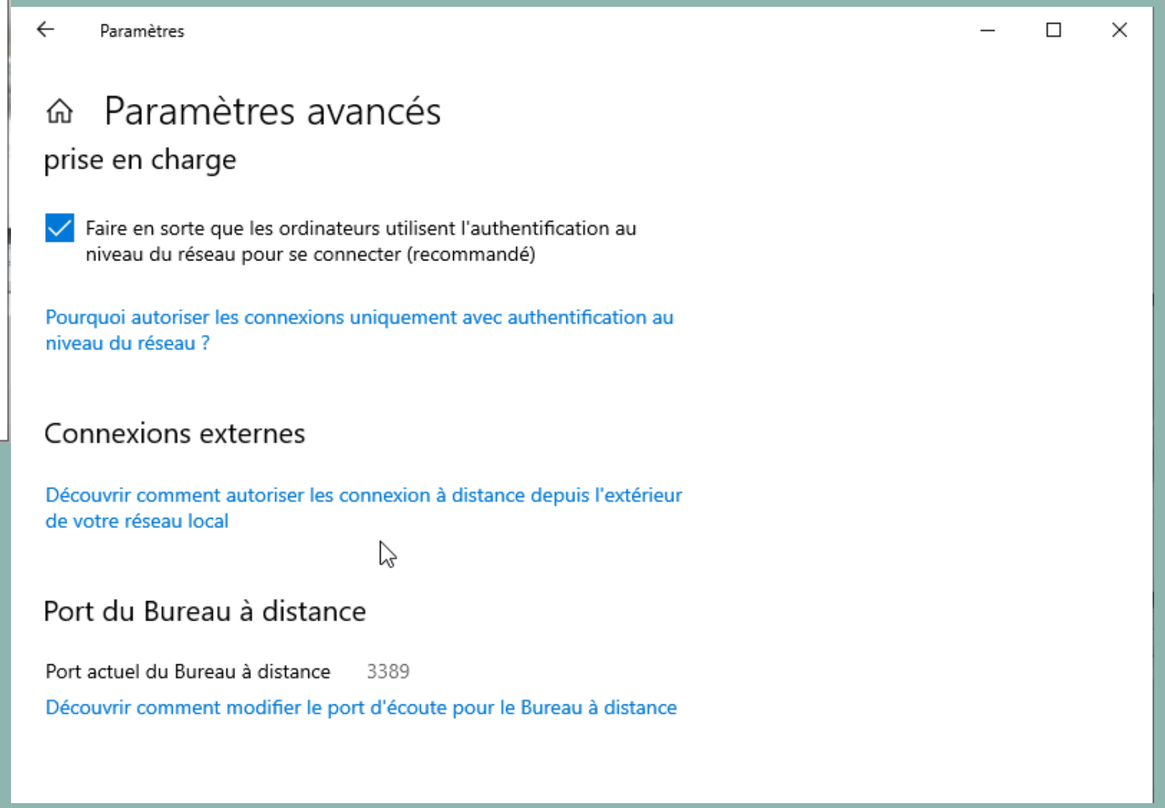
Nous allons maintenant voir comment activer le protocole RDP afin d’accéder à vos appareils à distance. Nous prendrons ici l’exemple d’un Windows Server 2019.

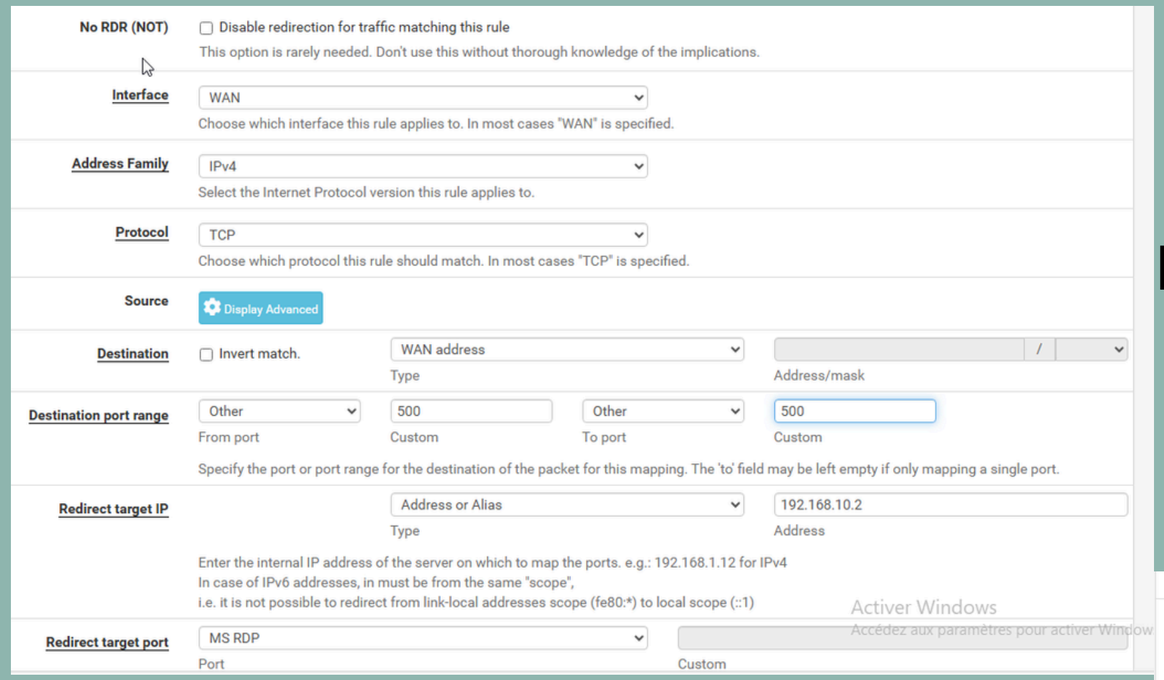


Commencez depuis votre gestionnaire de serveur en activant l'option Bureau à distance.

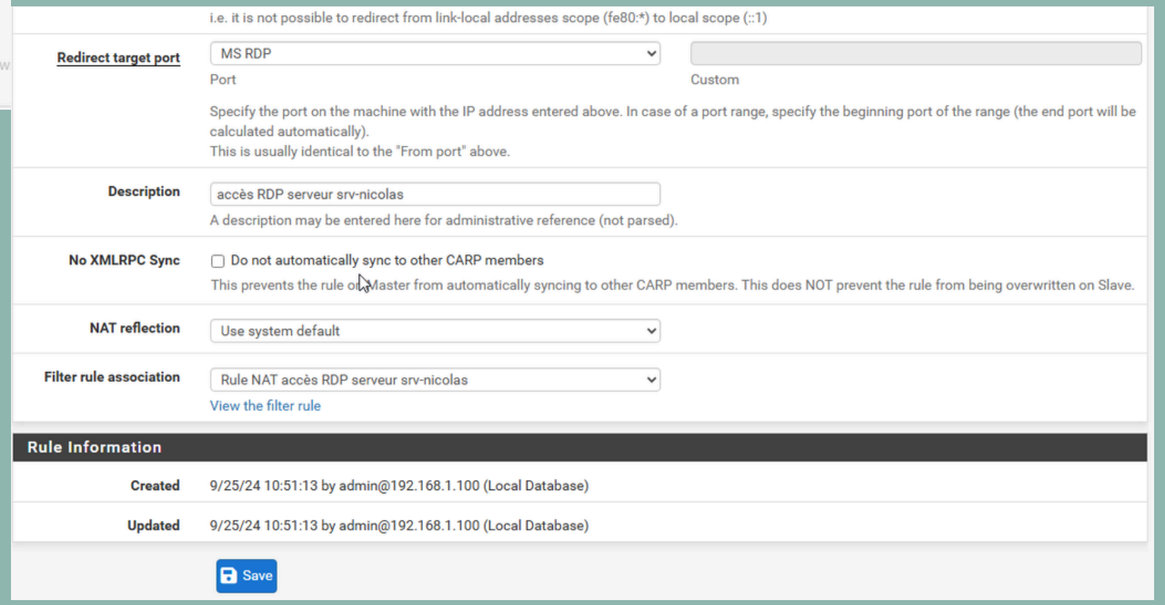


Allez ensuite dans vos paramètres avancés de Bureau à distance pour vérifier, dans un premier temps, s'il est actif, puis le port qui est utilisé (par défaut, le 3389).



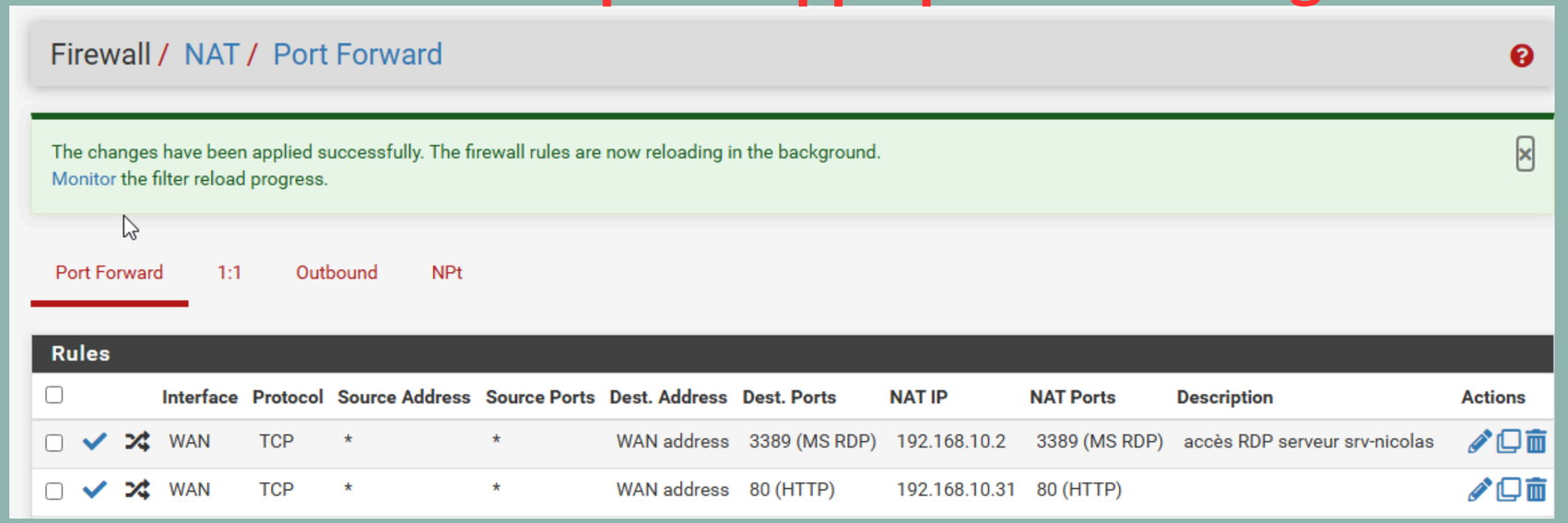


Allez ensuite dans votre pfSense afin de configurer une nouvelle redirection de port pour permettre au WAN d'accéder à distance au Windows Server.
Pour des raisons de sécurité, j'ai modifié le port de connexion à 500.

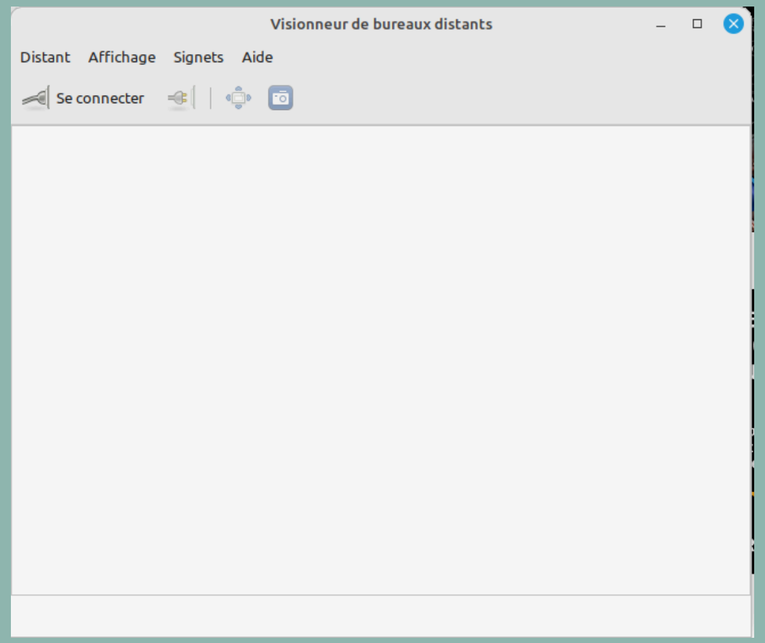


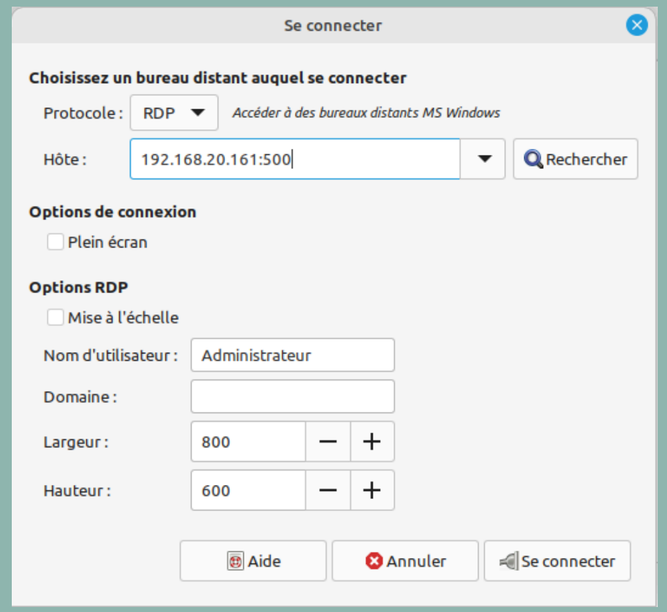
Voici ce qui devrait s'afficher ensuite.

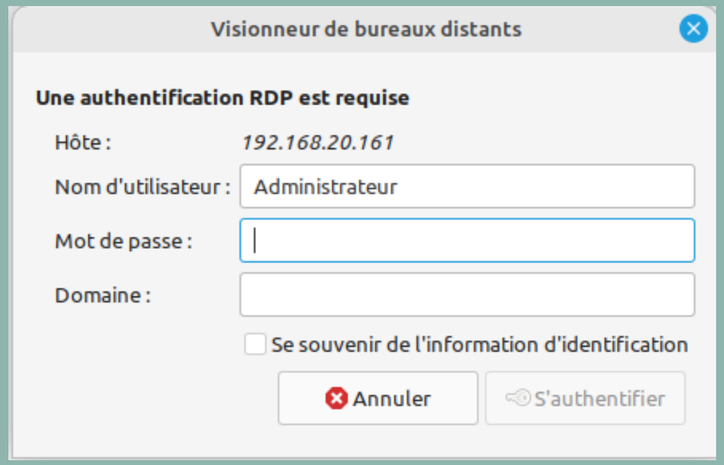
Attention : n'oubliez pas d'appliquer vos changements.



Essayons maintenant de nous connecter depuis notre WAN (j'utilise personnellement Vinagre, mais tout outil permettant la connexion RDP est utilisable).







Indiquez ensuite l'IP de votre pfSense avec le port que vous avez configuré, puis spécifiez l'utilisateur avec lequel vous souhaitez vous connecter.

Vous êtes maintenant connecté à distance à votre Windows Server.