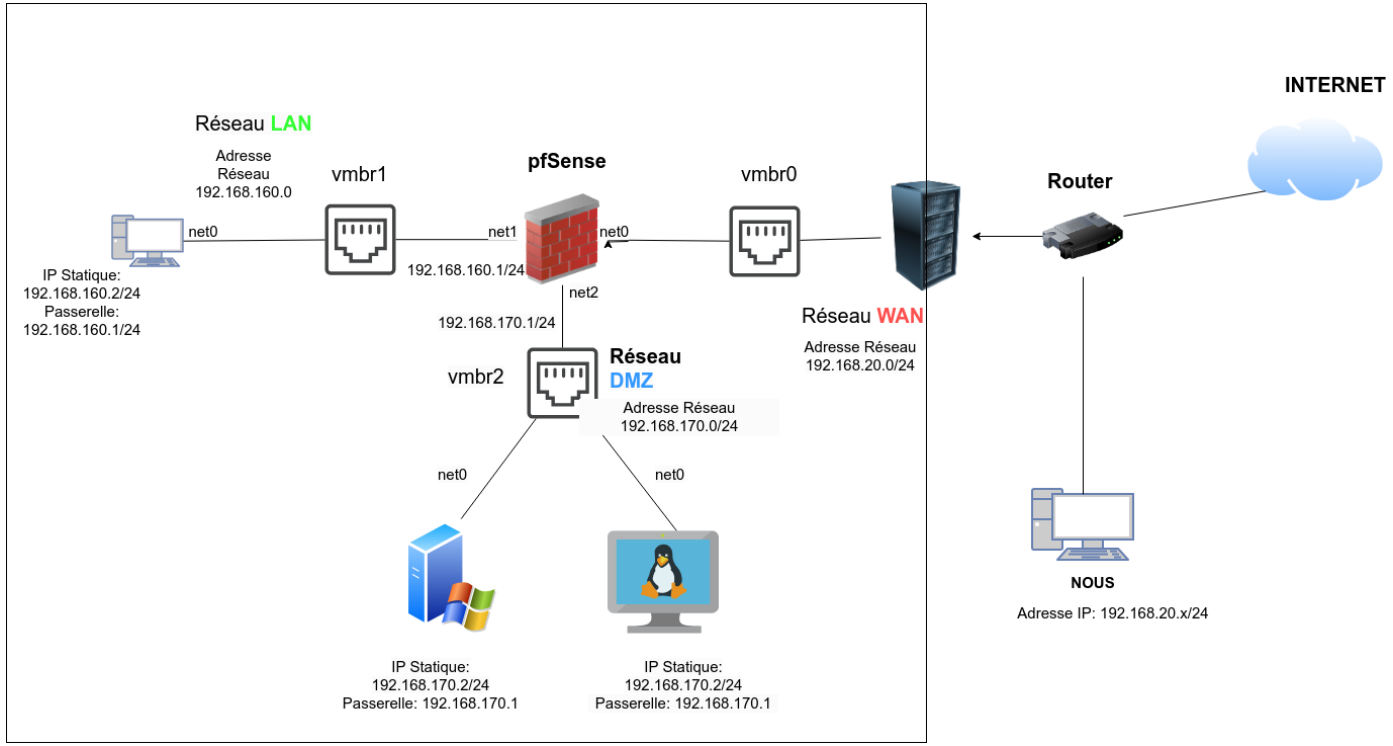
TP-PfSense

THOMAS GRZESINSKI

C’est quoi pfSense ?

pfSense est un système d’exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d’exploitation FreeBSD.

Schéma réseau



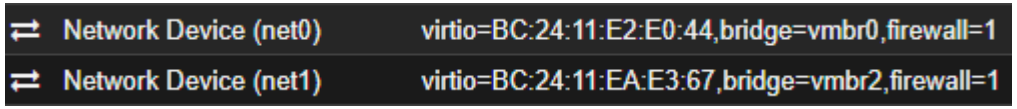
Installation de pfSense

- Tour d'abord il vous faudra installer l'iso pfSense

- Ensuite une fois dans le promox vous devez créer une nouvelle carte réseau, cette carte réseau nous servira à y attribuer une adresse LAN tandis que la carte réseau configurer de base nous servira de WAN,

- Maintenant vous devez créer votre machine virtuelle pfSense, ajouter lui 2 cœurs, 2048 mbit et 20go de stockage ce qui est largement suffisant pour pfSense une fois ceci fait il ne faut surtout pas lancer la machine virtuelle

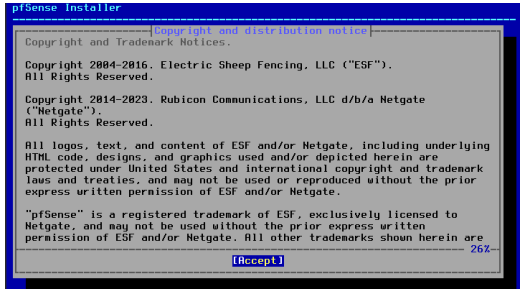
- En effet vous devez ajouter votre carte réseau « vmbr » sur cette machine pour pouvoir avoir un réseau LAN. Vous devez donc avoir deux cartes réseau



Installation de pfSense

- Une fois ceci fait vous devez lancer votre machine virtuelle et l'installation se mettra en place

- Au démarrage vous êtes censé avoir un message qui affiche le début de pfSenseinstall,



Installation de pfSense

Pour avoir une bonne installation: Installer pfSense en auto (UFS)

- Installer le sur l'entièretè du disque
- Installer le sur le disque de démarrage (MBR)
- Choisir les 20 GO de disque qu'on a mis en place
- Confirmer (commit)
- Redémarrer

Une fois que ceci est fait pfSense s'installera, si tout est bien configuré lors de votre redémarrage alors votre elle détectera les deux cartes réseaux

C’est quoi la différence entre WAN et LAN

WAN: Réseau étendu (WAN en anglais), est un réseau informatique ou un réseau de télécommunication couvrant une grande zone géographique, typiquement à l’échelle d’un pays, d’un continent ou de la planète entière. Le plus grand WAN est le réseau internet

LAN: Réseau local (LAN en anglais) **est un réseau informatique où les terminaux qui y participent s'envoient des trames au niveau de la couche de liaison sans utiliser l’accès à internet.**

Configuration pfSense (proxmox) installation

Maintenant lors du redémarrage de vitre pfSense on vous demandera d'attribuer les cartes réseau au WAN et LAN

Choisissez vtnet0 pour le WAN car c'est la carte réseau du réseau étendu

Choisissez vtnet1 pour le LAN pour que se soit la carte réseau de notre réseau LAN

Assigner les deux cartes réseau en appuyant sur « y » (yes)

Vous êtes censés avoir ceci:

Configuration pfSense (proxmox) installation

Donc si vos cartes sont détectées on doit maintenant:

- Décider que notre vtnet0 soit notre WAN

```
Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 or a): vtnet0
```

- Et on décidera donc pour notre Lan la carte vtnet1,

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

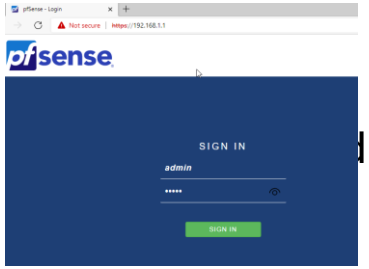
- Maintenant saisissez « y » pour assigner les deux cartes

```
The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1

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

Writing configuration...done.
One moment while the settings are reloading... done!
Configuring loopback interface...done.
Configuring LAN interface...done.
```

Configuration pfSense sur la machine cliente (proxmox)

- Maintenant que tout est configuré nous pouvons enfin assimiler une machine cliente sur le réseau LAN. Pour qu'on est accès a pfSense version graphique pour mieux gérer notre réseau.
- Vous devez donc rajouter une machine (Linux ou Windows), mais aussi faire en sorte que la carte réseau de cette machine-ci soit la carte réseau du LAN

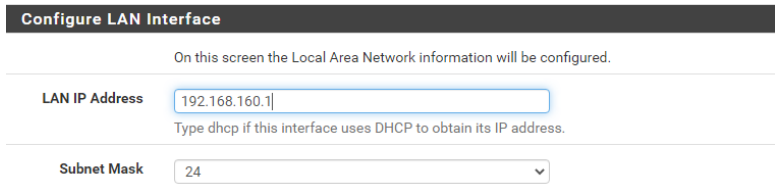
- Lancer la machine virtuelle
- Une fois ceci fait aller sur internet et entrer l'adresse IP LAN du pfSense (192.168.1.1) et la page de pfSense s'affcichera



Les logins et mot de passe sont admin et pfsense configurer
de base

Configuration pfSense sur la machine cliente (proxmox)

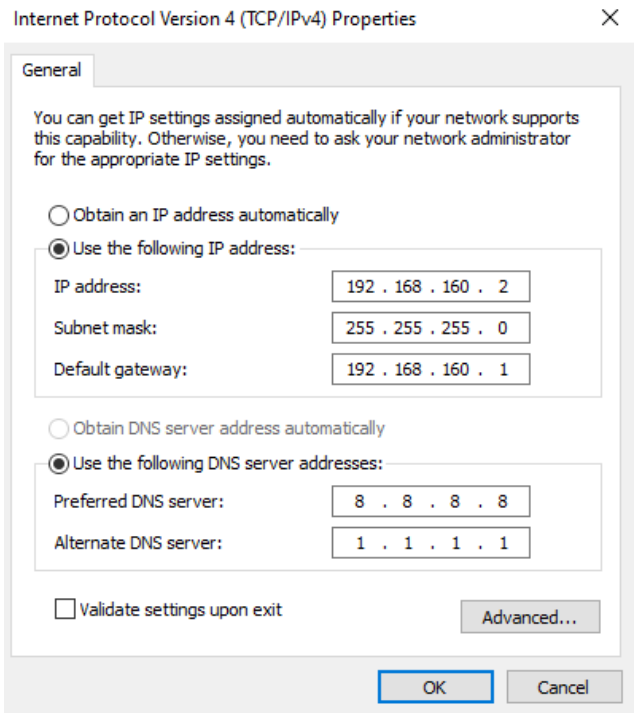
- Une page s'ouvrira et on vous y demandera de configurer votre pfsense:
- Vous pouvez changer le nom d'hôte
- Le domain
- En DNS primaire on peut y mettre 8.8.8.8 (Google DNS)
- En DNS secondaire on peut y mettre 1.1.1.1 (est un résolveur DNS public géré par Cloudflare, qui offre une solution rapide et privée pour la navigation sur Internet.)
- On ne met pas de DHCP en place
- ET ON MODIFIER LE LAN IP ADDRESS EN 192.168.x.1 en masque 24
- On défini un mot de passe administrateur
- Reloade et on patiente
- A partir de maintenant vous êtes censés ne plus avoir accès a internet (c'est normal)



Configuration pfSense sur la machine cliente (proxmox)

On va devoir maintenant modifier l'adresse IP de notre machine cliente comme ceci:

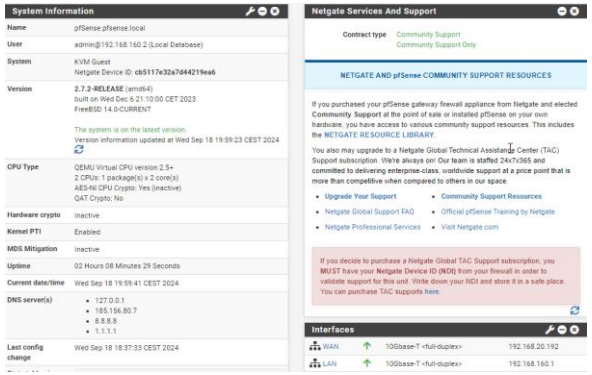
- On y met une adresse IP a notre machine cliente
- On met comme passerelle l'IP LAN du pare-feu
- Et en DNS préféré 8.8.8.8
- DNS secondaire 1.1.1.1



Configuration pfSense sur la machine cliente (proxmox

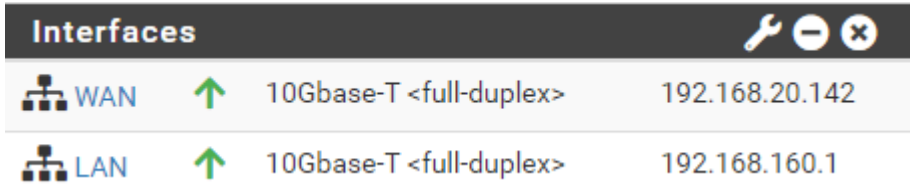
Une fois ceci fait on entre la nouvelle adresse IP LAN dans internet et on peut enfin accéder a notre pfSense

L'interface pfSense s'affichera enfin:



Cette interface nous permettra de configurer des règles, notre dmz et la redirection de nos ports pour notre pfSense

On y retrouve d'ailleurs nos cartes réseaux



Configuration DMZ

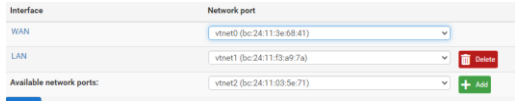
C’est quoi une DMZ ?

Zone démilitarisée (DMZ) est un sous-réseau séparé du réseau local et isolé de celui-ci ainsi que d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local. (Zone tampon entre réseau sécurisé et non sécurisé)

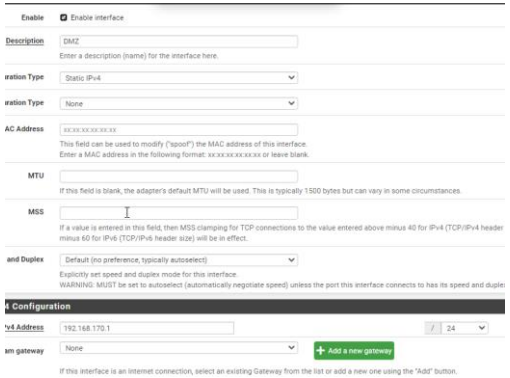
Configuration DMZ

Pour configurer une DMZ nous devons donc rajouter une troisième carte réseau sur notre pfSense que nous avions créé. Nous avons donc maintenant trois cartes réseau.

Retourner sur votre machine cliente pfSense puis aller dans « Interfaces -> Assignements » et vous pouvez observer qu'une troisième carte réseau est détecté.
Ajouter la et renommer la en « DMZ »



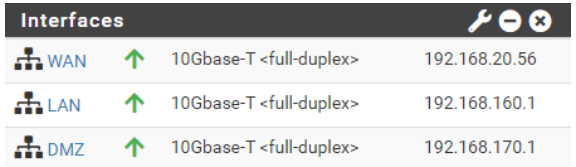
Ajouter lui une adresse IP static en 192.168.x.1 en 24



Confirmer et appliquer les changements

Configuration DMZ

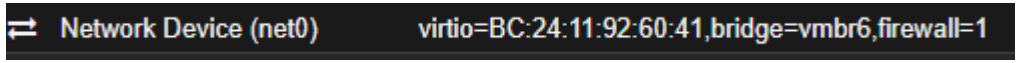
Retournez sur votre interface et la carte réseau pour la DMZ a bien été ajouté



Maintenant nous voulons donc mettre en place une machine Windows Server ou un serveur Apache

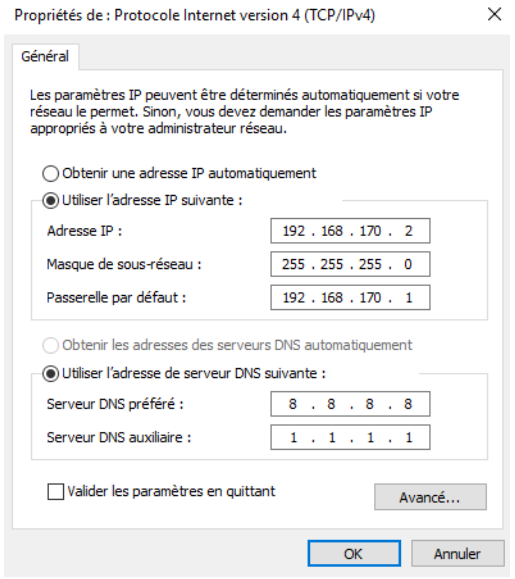
Méthode Windows Server

Ajoutez une machine Windows Server et modifié sa carte réseau pour y mettre la carte réseau de notre DMZ



Attribuer 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



Retourner donc sur votre pfSense et on va y configurer une règle pour y autoriser la navigation

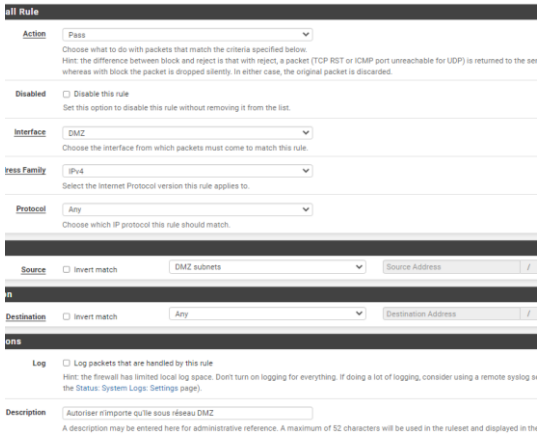
Méthode Windows Server

Lancer la machine Windows Server, allez sur internet et vous pouvez observer que vous ne pouvez pas naviguer sur le web et c’est tout à fait normal.

Vous devez donc ajouter une règle pour la DMZ dans pfsense:

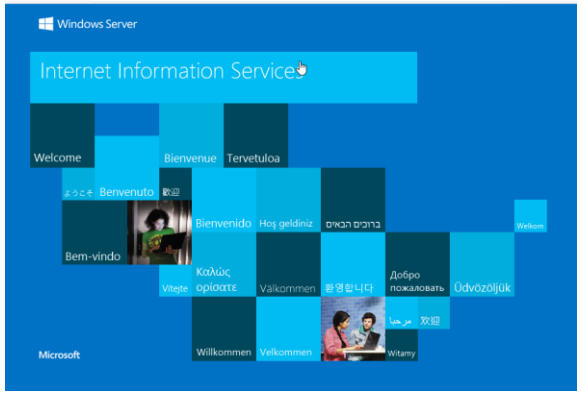
Il faut donc attribuer ces règles ci qui permettent de dire

que notre DMZ puisse accéder à internet



Méthode Windows Server

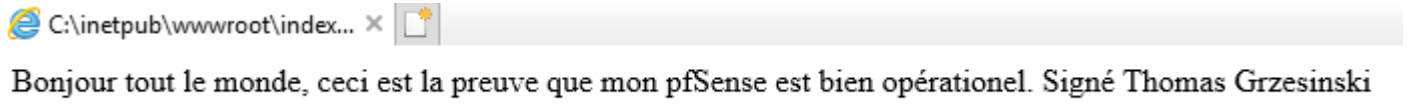
- Une fois que tout ceci est fait je voudrai faire en sorte qu'on puisse accéder a une page web mise sur ma DMZ, depuis mon réseau local et en dehors du pfSense
- Pour faire ceci vous devez installer un serveur web (IIS) voir le TP-Web DNS
- Si tout est bien installé entrer l'IP 127.0.0.1 sur internet et ceci est censé s'afficher pour confirmer que votre serveur est bien installé:



Méthode Windows Server

Maintenant ajouté dans le dossier C:\inetpub\wwwroot un fichier index.html

Ce dossier sert de base à la configuration du site web de base du gestionnaire IIS

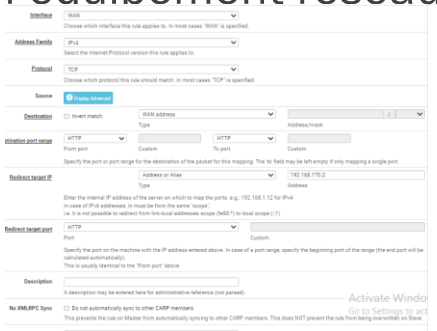


Maintenant on a un souci c'est que l'on ne peut pas accéder à ce site web en depuis notre WAN donc pour résoudre ce problème nous devons ajouter une redirection de port

Méthode Windows Server redirection port

Retourner sur votre interface pfSense

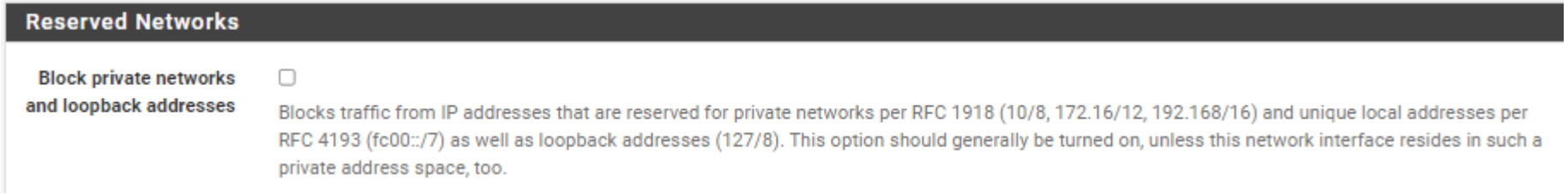
Et on va créer une règle de Nat Port Forward qui permettra a rediriger des paquets réseaux reçus sur un port donné d'n ordinateur ou d'un équipement réseau vers un autre ordinateurs ou équipement réseau sur un port donnée



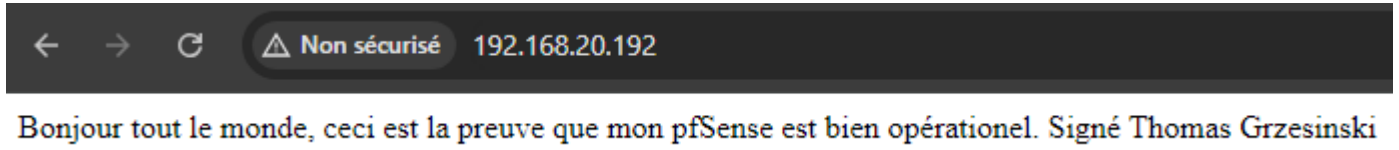
Donc il faut ajouter une règle NAT IP qui dit que pour les flux qui proviennent de l'interface WAN en TCP sur l'adresse publique du WAN on va relier le flux vers le serveur WEB en interne (notre adresse serveur WEB) et on applique

Méthode Windows Server redirection port

Il ne faut pas oublier dans l'interface WAN de désactiver la case « Bloquer les flux qui arrivent sur l'interface WAN »



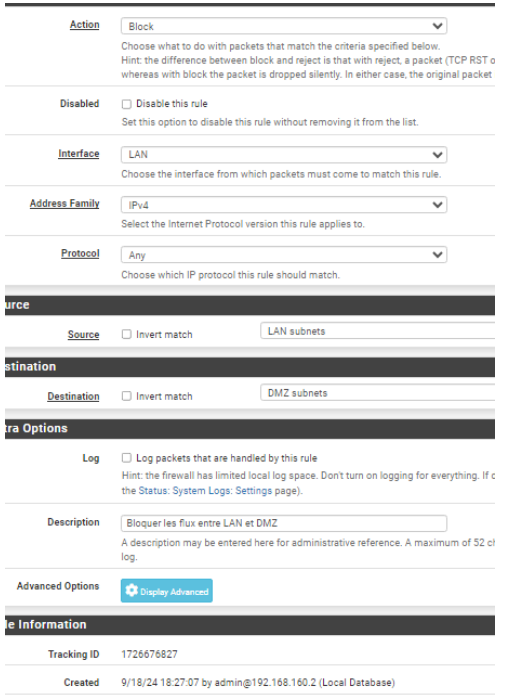
On entre l'adresse IP sur internet et on voit qu'on a accès à notre serveur web qui est dans notre réseau mais depuis le WAN



Notion de sécurité LAN

Une notion de sécurité importante à mettre en place, c’est que notre réseau LAN a accès à tout les réseau.

Première règle bloquer les flux entre le LAN et la DMZ

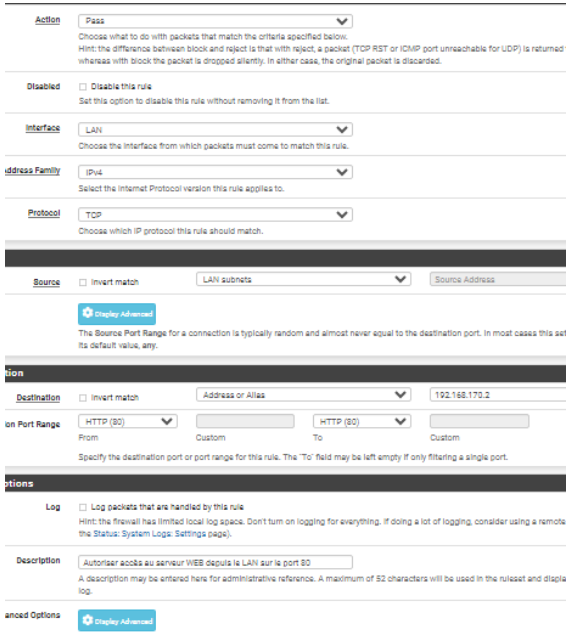


Notion de sécurité LAN

Mais je voudrai accéder à mon serveur web depuis le Lan donc:

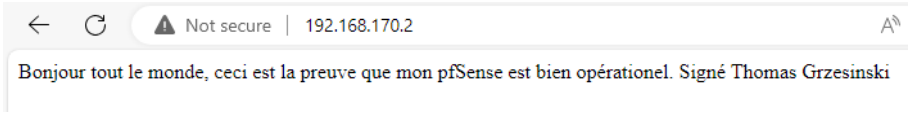
Deuxième règle: Quand la source c'est le LAN subnet et la destination

L'adresse de la DMZ, et quand c'est du http j'autorise



Notion de sécurité LAN

On peut donc accéder a la page web depuis le LAN, mais on ne peut rien envoyer au serveur DMZ




```
C:\Users\sio>ping 192.168.170.2

Pinging 192.168.170.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.170.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Méthode Linux

Pour la méthode Linux il vous faudra donc : - Configurer une adresse IP statique comme sur Windows

-Installer un serveur Apache
- Configurer une adresse IP statique et son gateway
- Appliquer les mêmes règles
- Méthode a utilisé en AP (plus rapide et simple)

TP-DMZ ADDON

Choix de solution de monitoring

Comme choix de solution j'ai choisi Ntop, en effet Ntop permet de ne rien modifier à l'infrastructure présente, on peut le placer où on veut pour monitorer des sections précise ou le placer entre le switch cœur de réseau et le routeur de périphérie pour analyser le trafic vers internet

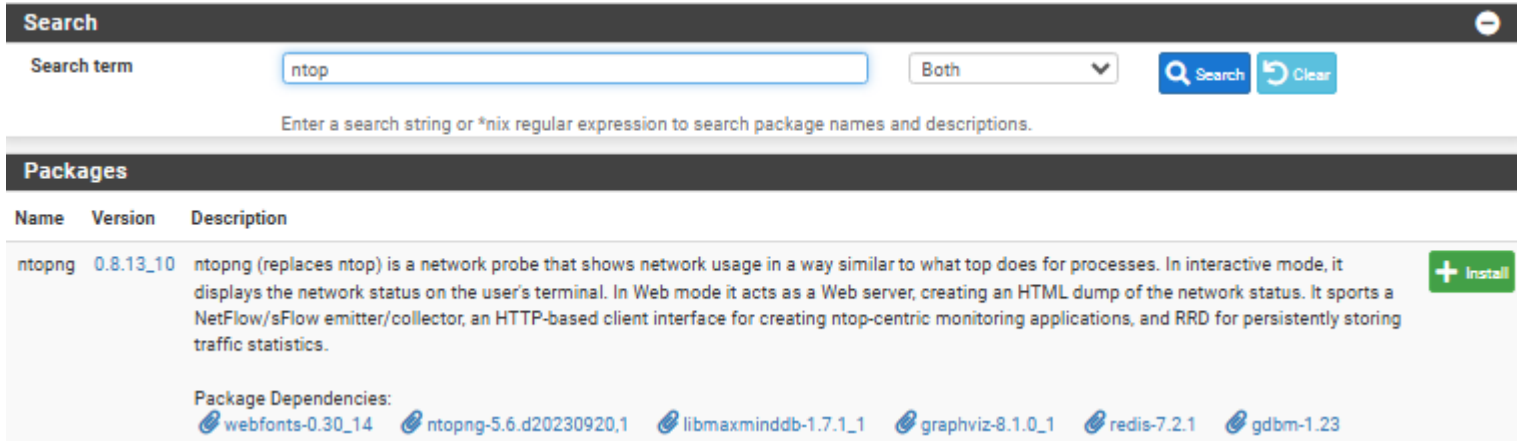
Pour pfSense:

- Une surveillance en temps réel
- Analyse détaillée du trafic
- Gestion des protocoles
- Performance et évolutivité
- Alertes et notifications

Installation ntop

On doit donc maintenant installer ntop vous devez donc sur votre interface pfSense aller dans:

- System -> Available Packages -> on recherche ntop et on l'installe

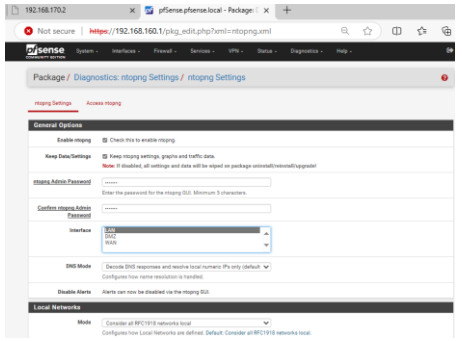


Installation ntop

Ensuite dans diagnostics deux nouveaux onglets sont donc apparus « ntopng » et « ntopng settings »

Cliquer sur ntoppng settings configurer un mot de passe et choisissez l'interface LAN

Une fois que ceci est fait cliquer sur le lien dans la section Accès ntopng



Interface ntopng

Vous devez donc arriver sur cette interface avec l’adresse

IP de votre machine LAN.

Vous pouviez donc maintenant monitorer votre réseau

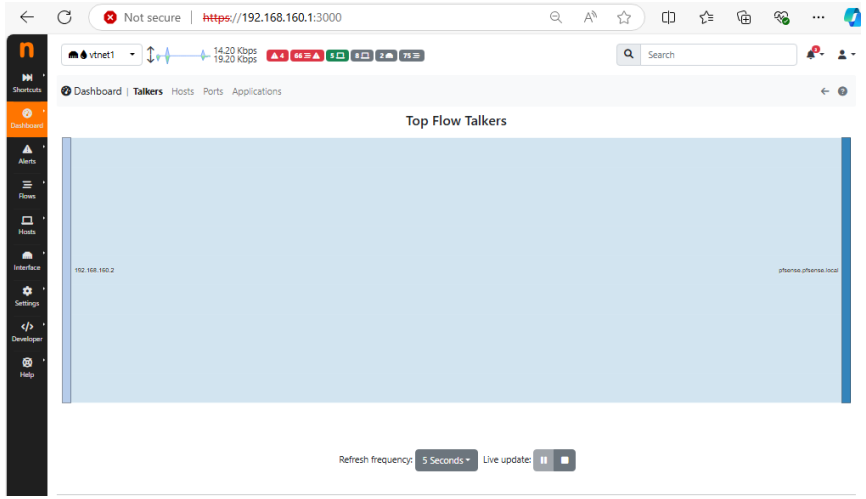
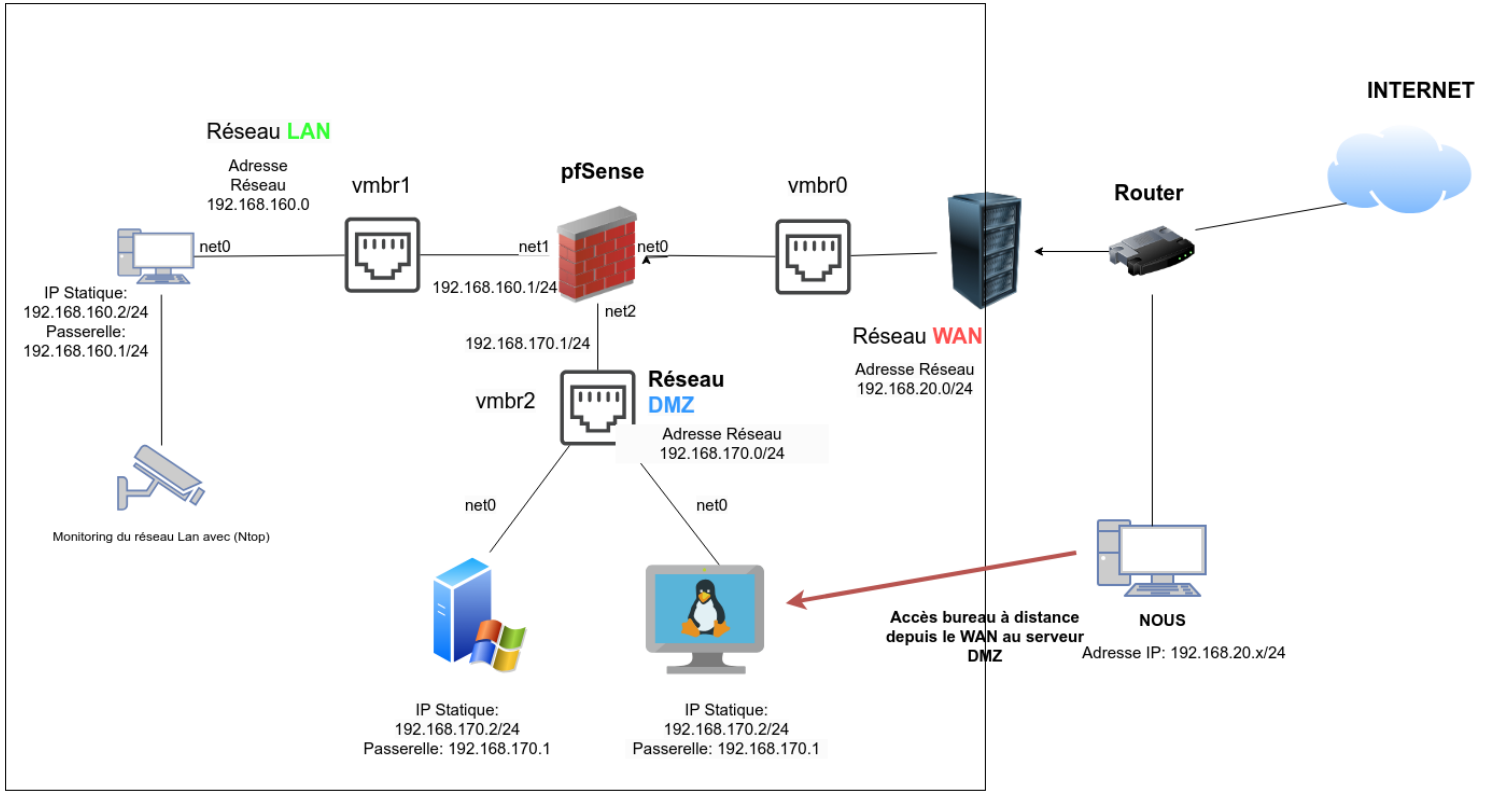


Schéma réseau accès bureau à distance



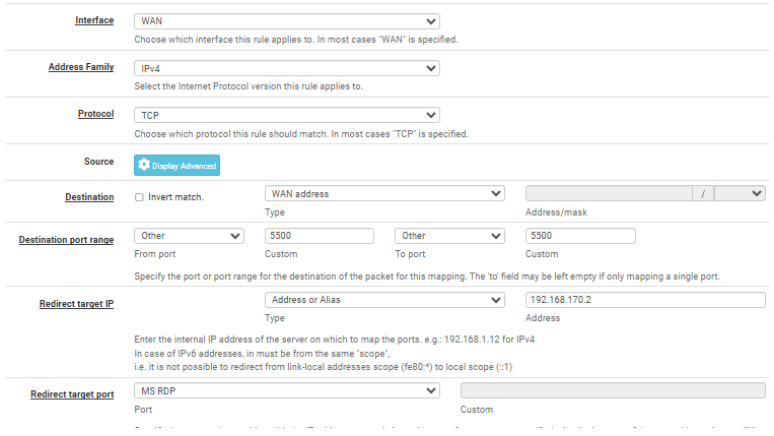
Accès bureau à distance

Maintenant je voudrai pouvoir accéder à mon Windows Serveur mais à distance

Pour faire ceci on doit tout d'abord rajouter une redirection de port donc NAT->Port Forward->Edit

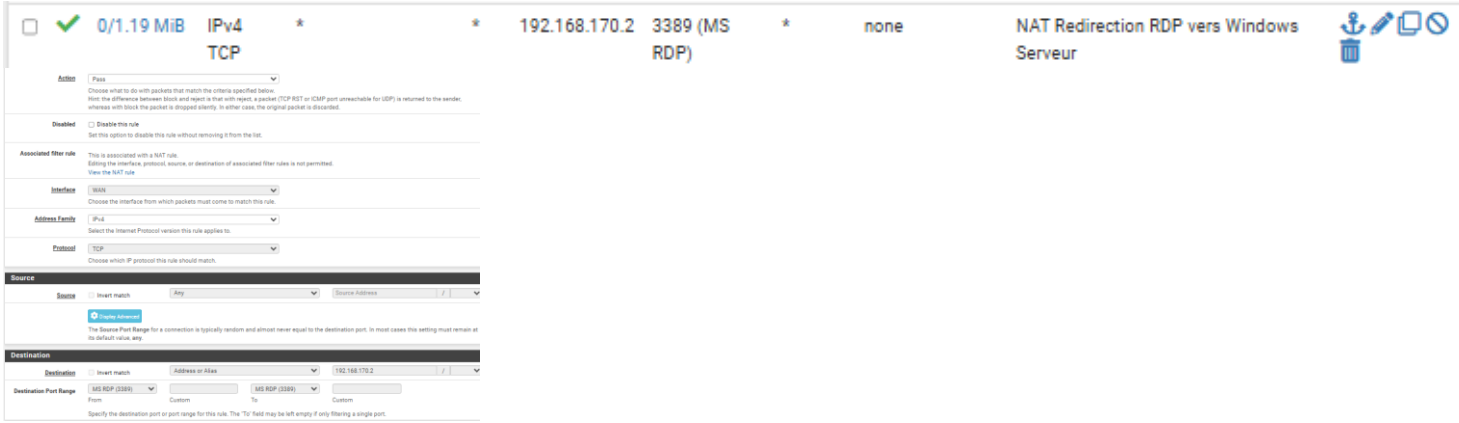
Ajouter une règle comme celle-ci qui dit:

On fait 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



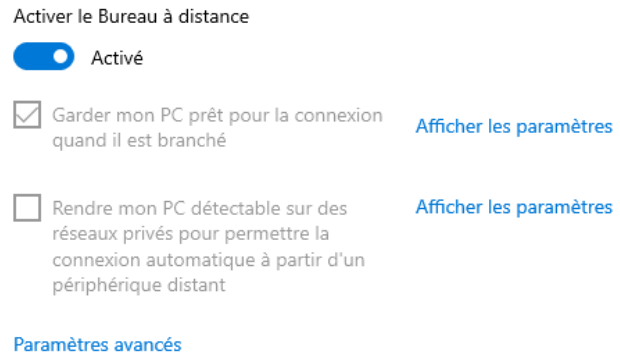
Accès bureau à distance

Il faut donc maintenant vérifier dans les règles du WAN si on a une règle qui dit confirme bien la redirection RDP vers Windows serveur



Accès bureau à distance

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



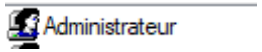
Une fois ceci fait on ajoute va dans la gestion de l’ordinateur et on y ajoute un user si on n'a pas de Active Directory (Utilisation de l’administrateur perso)

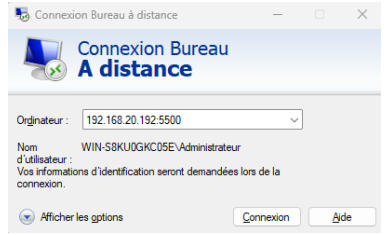
Ensuite on va dans groupes on clique sur « Serveurs Accès Distant RDS » et on ajoute notre user

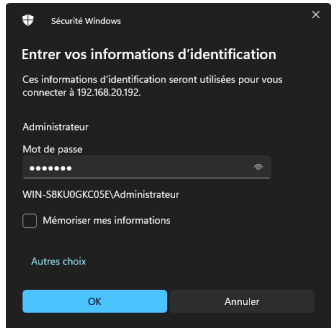
Accès bureau à distance

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 

Maintenant sur notre machine connectée au réseau WAN aller dans le bureau à distance et connecter vous a votre Windows Server avec l'IP Windows server et son port 

Entrer les logs 

et vous avez accès au serveur