

## **Journal de bord**

### **Semaine 1**

**17/06/20**

- Proposition d'une première architecture réseau
- Teste et manipulation de Proxmox pour se familiariser (création d'user, vm Windows/linux, création du par feu/VPN, ParrotSecurity)
- Téléchargement iso Windows, Linux
- Connexion SSH via mobaXterm

**18/06/20**

- Recherche de tuto sur internet pour la création de VM routeur et switch
- Recherche d'iso pour VM routeur et switch
- Recherche sur les clusters tuto et comment créer
- Création d'une VM routeur mikrotik

**19/06/20**

- Recherche sur le fonctionnement des IP public et privées
- Recherche sur le fonctionnement de la conteneurisation
- Recherche sur les clusters
- Recherche de tutos « comment faire des cluster »
- Manipuler les carte réseau des VM Windows

## **Principe de fonctionnement des IP public et privé**

Avant de voir ce qu'est une adresse IP publique et privée nous allons commencer par définir ce qu'est une adresse IP.

Une adresse IP est ce qui permet d'identifier chaque machine connecté à un réseau utilisant le protocole IP. L'adresse IP est composée de 4 octets allant de 0 à 255 séparés par des points.

Chaque adresse IP appartient à une classe qui correspond à une plage d'adresses IP.

Au total 5 classes existent A, B, C, D et E, cela sert à adapter l'adressage selon la taille du réseau.

Voici les plages d'adresse selon les classes :

- La classe A de l'adresse IP 0.0.0.0 à 126.255.255.255
- La classe B de l'adresse IP 128.0.0.0 à 191.255.255.255
- La classe C de l'adresse IP 192.0.0.0 à 223.255.255.255
- La classe D de l'adresse IP 224.0.0.0 à 239.255.255.255
- La classe E de l'adresse IP 240.0.0.0 à 255.255.255.255

Les adresses IP des classes D (adresses de multicast) et E (adresses réservées par IETF) sont des adresses IP réservés donc non utilisables.

### **Qu'est-ce qu'une adresse IP Privée ?**

Une adresse IP privée ce sont toutes les adresses IP qui ne sont pas utilisables sur internet, par exemple le réseau de votre entreprise ou le réseau domestique. Un réseau privé est un réseau qui utilise les plages d'adresses IP non accessibles depuis Internet.

Elles permettent de communiquer localement avec vos différents périphériques..

Les adresses IP privées se trouvent dans les classes A, B et C.

Voici les plages d'adresse IP privée selon les classes :

- Les adresses privées de la classe A : 10.0.0.0 à 10.255.255.255 (comprend 16 millions d'adresses)
- Les adresses privées de la classe B : 172.16.0.0 à 172.31.255.255 (comprend 65535 adresses)
- Les adresses privées de la classe C : 192.168.1.0 à 192.168.255.255 (comprend 256 adresses)

Pour permettre un appareil ayant une adresse privée d'accéder à l'internet, cette adresse doit d'abord être traduite en adresse publique. Cette traduction ou translation est appelée NAT (Network Adresse Translation). Il existe 3 types de traduction NAT :

- NAT statique : correspondance un pour un établie entre les adresses locale et globale.
- NAT dynamique : mappage de plusieurs adresses locales vers plusieurs adresses globales.
- Traduction d'adresses de port (PAT) : mappage de plusieurs adresses locales et globales vers une seule. Cette méthode est également appelée « surcharge » (surcharge NAT).

### **Qu'est-ce qu'une adresse IP Publique ?**

Les adresses IP publiques ne sont pas utilisées dans un réseau local mais uniquement sur internet.

Une adresse IP publique est unique dans le monde alors que pour une adresse IP privée c'est dans le réseau local qu'elle est unique.

Les adresses IP publiques représentent toutes les adresses IP des classes A, B et C qui ne font pas partie de la plage d'adresses privées de ces classes ou des exceptions de la classe A qui sont le réseau 127.0.0.0 qui est réservé pour les tests de boucle locale et le réseau 0.0.0.0 qui est réservé pour définir une route par défaut sur un routeur.

La différence se manifeste donc au niveau du type de réseau qu'on utilise, si on souhaite rester dans son réseau local il faudra utiliser une adresse IP privée et au contraire, il faudra utiliser une adresse IP publique.

## Conteneurisation

### Que sont les conteneurs ?

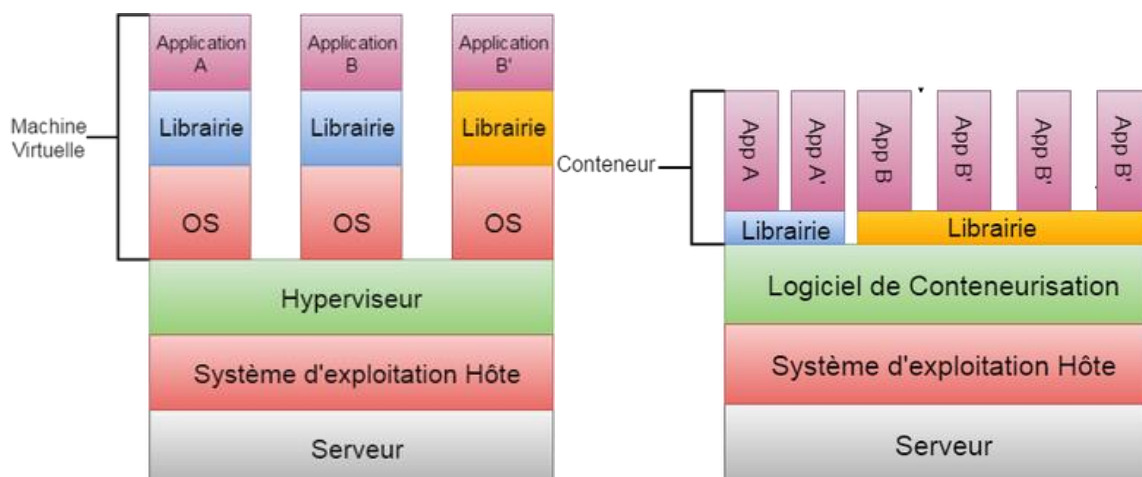
Tout comme dans le domaine des transports, les conteneurs informatiques stockent des objets pour les transporter. Ils permettent d'expédier des applications et leurs dépendances sur de multiples systèmes d'exploitation, quels qu'ils soient. Ils garantissent que leur contenu est identique au départ et à l'arrivée, et qu'il est sécurisé, grâce à leur mise en isolation.

### À quoi servent-ils ?

Ils servent à minimiser la complexité liée à la configuration et à l'administration applicatives, à accélérer les cycles de développement et de production applicatifs, et, grâce à leur flexibilité et à leur portabilité, ils constituent l'une des briques qui permettent de faire de l'« infrastructure as a service », c'est-à-dire d'automatiser les infrastructures IT.

### Fonctionnement

La conteneurisation est une méthode qui permet de virtualiser, dans un conteneur, les ressources matérielles – systèmes de fichiers, réseau, processeur, mémoire vive, etc. – nécessaires à l'exécution d'une application. Dans cet espace sont aussi stockées toutes les dépendances des applications : fichiers, bibliothèques, etc. Pour déplacer les applications virtuelles d'un système d'exploitation à un autre, le conteneur se connecte à leur noyau (*kernel*), ce qui permet aux différents composants matériels et logiciels de communiquer entre eux.



## Les outils de conteneurisation

LXC « LinuX Containers »

Le noyau de linux à la possibilité de créer des conteneurs. Les conteneurs Linux ont une isolation des systèmes de fichier, des identifiant réseau et utilisateur. Et également une isolation des ressources (processeur, mémoire, etc).

Ce système de virtualisation est vraiment la base de la conteneurisation

### **Docker (logiciel libre)docker**

Docker est la solution de conteneurisation la plus utilisée aujourd'hui. Il utilise une Interface de programmation « Libcontainer » pour démarrer, gérer et arrêter des conteneurs. Il est basée sur le fonctionnement de LXC et y ajoute des capacités de niveau supérieur. La gestion des versions permet de comprendre certains problèmes, il est possible de revenir à une version antérieure. De plus, les conteneurs peuvent servir d'images à un autre, donc le partage de conteneurs en public est possible. Ce service en ligne est appelée Docker Hub, il contient des images de conteneurs, ce qui permet aux utilisateurs de faire des échanges. Cela rend l'installation d'un conteneur extrêmement facile (aussi simple qu'un téléchargement sur internet).

Docker permet donc de faciliter l'installation d'application dans des conteneurs et la mise à jour, mais c'est le noyau linux qui s'occupe de la création de conteneurs.

Docker est disponible sur linux comme sur Windows.

### **RKT « rocket »**

Cet outil est édité par CoreOS et est le concurrent de Docker. Il prend en charge les Images Docker et le format ACI (App Container Images). Les éditeurs se concentrent sur la sécurité (le plus gros point faible de Docker), la compatibilité et une intégration aux standards.

Le but étant de fournir les mêmes fonctionnalités que docker et être complémentaires.

a noter la conteneurisation n'utilise pas d'os (iso) contrairement au Vm, ce qui la rends tout de suite beaucoup plus légère.

## Cluster

### **Qu'est-ce qu'un cluster ?**

Le gestionnaire de cluster de ProxmoxVE pvecm est un utilitaire qui permet de créer un groupe de serveur physique. Ce groupe s'appelle un cluster contenant un certain nombre de nœuds (nodes) correspondants à vos machines physiques.

Les avantages de créer un cluster de machines sont :

Une gestion centralisée via l'interface web ;

Un cluster multi-maître : chaque nœud peut réaliser les tâches d'administration ;

Migration simplifiée des machines virtuelles ou des conteneurs entre les machines physiques ;

Des services étendus au cluster tels que la haute disponibilité et le pare-feu.

## Semaine 2

**22/06/20**

- Recherche de tutos pour créer un Lan et connecter les VM entre elles
- Paramétrage de PfSense

**23/06/20**

- Toujours en recherche pour connecter les VM a un Lan pour les faire communiquer
- Schématisation de ce que l'on a compris théoriquement (reste la pratique)
- Crash du server

**24/06/20**

- Création du Roadmap sur Planner office 365 :  
Partage du travail, attribution des missions
- Schématisation de l'architecture via PacketTracer : Xavier Tristant  
Objectif à atteindre, pouvoir faire communiquer les 2vm Windows entre elle

Pratique réaliser ce jour : Erwin Yazid Alexandre

- Installation des Vm Windows et Pfsens
- Paramétrage des interface réseaux virtuelle (server et VM)

Avancé :

Test de ping : via les VM Windows

- IP bridge du réseau LAN 192.168.9.0/24  
Ping de l'IP 192.168.9.1 (Vmbr2) depuis PC-vm1, FONCTIONEL

```
C:\Users\stageiris1>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::21c4:503f:1a9f:a070%11
    Adresse IPv4. . . . . : 192.168.9.101
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.9.1

C:\Users\stageiris1>ping 192.168.9.1

Envoi d'une requête 'Ping' 192.168.9.1 avec 32 octets de données :
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.9.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Ping de l'IP 192.168.9.1 (Vmbr2) depuis PC-vm2, FONCTIONNEL

```
C:\Users\stageiris2>ipconfig

Configuration IP de Windows

.

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::29a8:30b:758e:9e08%4
    Adresse IPv4. . . . . : 192.168.9.102
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.9.1

C:\Users\stageiris2>ping 192.168.9.1

Envoi d'une requête 'Ping' 192.168.9.1 avec 32 octets de données :
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.9.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

- IP bridge du réseau WAN 10.0.0.0/30

Ping de l'IP 10.0.0.1 (Vmbr1) depuis PC-vm1, FONCTIONNEL

```
C:\Users\stageiris1>ping 10.0.0.1

Envoi d'une requête 'Ping' 10.0.0.1 avec 32 octets de données :
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.0.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Ping de l'IP 10.0.0.1 (Vmbr1) depuis PC-vm2, FONCTIONNEL

```
C:\Users\stageiris2>ping 10.0.0.1

Envoi d'une requête 'Ping' 10.0.0.1 avec 32 octets de données :
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.0.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

- IP bridge du server 176.31.123.32/24

Ping 176.31.123.32 (Vmbr0) depuis PC-vm1, FONCTIONNEL

```
C:\Users\stageiris1>ping 176.31.123.32

Envoi d'une requête 'Ping' 176.31.123.32 avec 32 octets de données :
Réponse de 176.31.123.32 : octets=32 temps<1ms TTL=64
Réponse de 176.31.123.32 : octets=32 temps<1ms TTL=64
Réponse de 176.31.123.32 : octets=32 temps<1ms TTL=64
Réponse de 176.31.123.32 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 176.31.123.32:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Ping 176.31.123.32 (Vmbr0) depuis PC-vm2, FONCTIONNEL

```
C:\Users\stageiris2>ping 176.31.123.32

Envoi d'une requête 'Ping' 176.31.123.32 avec 32 octets de données :
Réponse de 176.31.123.32 : octets=32 temps<1ms TTL=64
Réponse de 176.31.123.32 : octets=32 temps<1ms TTL=64
Réponse de 176.31.123.32 : octets=32 temps<1ms TTL=64
Réponse de 176.31.123.32 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 176.31.123.32:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

- Ping des Deux Vm entre elles :

Ping de 192.168.9.102 depuis le Pc-Vm1 qui à l'IP 192.168.9.101, ECHEC

```
C:\Users\stageiris1>ping 192.168.9.102

Envoi d'une requête 'Ping' 192.168.9.102 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.9.102:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Ping de 192.168.9.101 depuis le Pc-Vm2 qui à l'IP 192.168.9.102, ECHEC

```
C:\Users\stageiris2>ping 192.168.9.101

Envoi d'une requête 'Ping' 192.168.9.101 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.9.101:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```



### Problème rencontré :

Le problème que nous rencontrons est que nous n'arrivons toujours pas à connecter les deux VM Windows entre elles. Nous devons trouver comment configurer le router Pfsense.

**24/06/20**

- Installation de Fail2ban : Tristan et Xavier  
Problème rencontre lors du test 1 ;  
Test de connexion avec de mauvais ID mais apparemment la configuration faites ne fonctionne pas (configuration faite grâce au suivi d'un tuto).  
<https://pve.proxmox.com/wiki/Fail2ban>  
Après avoir essayé de mauvais ID nous teston cette commande :

```
regex /var/log/daemon.log /etc/fail2ban/filter.d/proxmox.conf
```

Cette commande devrait nous donner un résultat tel que :

\* au moins \* un "Failregex: 1 total" en haut de la section "Résultats" (et "1 correspondant" en bas)

Or nous avons eu ce résultat :

```
Running tests
=====

Use   failregex filter file : proxmox, basedir: /etc/fail2ban
Use   log file : /var/log/daemon.log
Use   encoding : UTF-8

Results
=====

Failregex: 0 total

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
| [15501] (?:DAY )?MON Day 24hour:Minute:Second(?:\.Microseconds)?(?: Year)?
|_

Lines: 15501 lines, 0 ignored, 0 matched, 15501 missed
[processed in 0.85 sec]
```

Autre problème c'est que même après 3 tentatives de mauvaise connexion nous ne sommes pas bannies.



Suppression de fail2ban pour le réinstaller : Tristan

Commande utiliser : `rm -r /etc/fail2ban/`

Résultat Fail2ban toujours défaillant.

Paramétrage des Vm Windows : Xavier

Après avoir tester des pings entre les Deux Vm le message afficher qu'il ne pouvait pas rejoindre l'hôte de destination, j'ai donc désactivé les pare-feu Windows des deux coté. Puis j'ai retester un ping et cette fois le ping à fonctionner et les deux vm ont pu communiquer.

- Ping des Deux Vm entre elles :

Ping de 192.168.9.102 depuis le Pc-Vm1 qui à l'IP 192.168.9.101, FONCTIONNEL

```
C:\Users\stageiris1>ping 192.168.9.102

Envoi d'une requête 'Ping' 192.168.9.102 avec 32 octets de données :
Réponse de 192.168.9.102 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.102 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.102 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.102 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.9.102:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Ping de 192.168.9.101 depuis le Pc-Vm2 qui à l'IP 192.168.9.102, FONCTIONNEL

```
C:\Users\stageiris2>ping 192.168.9.101

Envoi d'une requête 'Ping' 192.168.9.101 avec 32 octets de données :
Réponse de 192.168.9.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.101 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.9.101:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

24/06/20

Teste de re-paramétrage de Fail2ban : Tristan et Lyazid

Le problème que nous rencontrons et que l'ont à mal supprimer Fail2ban et on a du mal à le réinstaller.

Lyazid :

Désinstallation des dépendances de Fail2ban avec la commande apt-get purge fail2ban

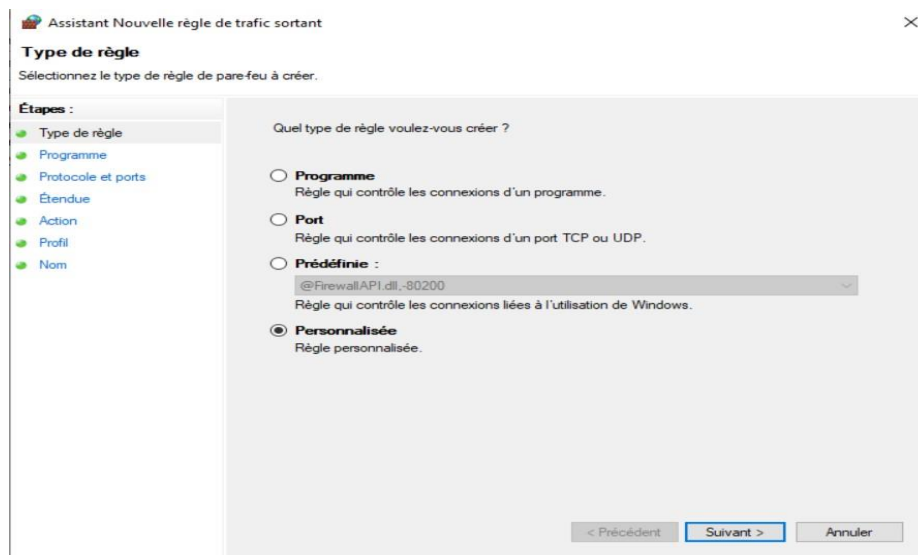
Ensuite nous avons tenté de nous connecter au server en ssh via nos machines et après 3 mauvais essaie nous ne pouvons plus essayer de s'y connecter :

```
26/06/2020 09:57.16 /home/mobaxterm ssh 176.31.123.32
ssh: connect to host 176.31.123.32 port 22: Connection timed out
```

On en conclu donc que le fail2ban fonctionne.

Paramétrage du pare-feu Windows defender : Yazid Xavier

Nous avons défini une nouvelle règle dans les règles de trafic entrent du firewall que nous avons nommé Ping. Dans cette règle nous spécifions qu'elle est personnalisée



Définissons les règles :

Nous spécifions que la règle s'applique à tous les programmes

The screenshot shows the 'Assistant Nouvelle règle de trafic sortant' window, specifically the 'Programme' step. The left sidebar lists the steps: 'Type de règle', 'Programme', 'Protocole et ports', 'Étendue', 'Action', 'Profil', and 'Nom'. The main area contains the following text and options:

**Programme**  
Spécifiez le chemin d'accès complet au programme et le nom du fichier exécutable du programme auquel correspond cette règle.

Étapes :

- Type de règle
- Programme**
- Protocole et ports
- Étendue
- Action
- Profil
- Nom

Cette règle s'applique-t-elle à tous les programmes ou à un programme spécifique ?

☒ **Tous les programmes**  
La règle s'applique à toutes les connexions de l'ordinateur qui correspondent à d'autres propriétés de règles.

☐ **Au programme ayant pour chemin d'accès :**  
[Text field]  
Exemples : c:\path\program.exe  
              %ProgramFiles%\browser\browser.exe

**Services**  
Vous pouvez également spécifier à quels services cette règle s'applique.

Personnaliser...

< Précédent   Suivant >   Annuler

Cette règle s'applique aussi à tous les protocoles

The screenshot shows the 'Assistant Nouvelle règle de trafic sortant' window, specifically the 'Protocole et ports' step. The left sidebar lists the steps: 'Type de règle', 'Programme', 'Protocole et ports', 'Étendue', 'Action', 'Profil', and 'Nom'. The main area contains the following text and options:

**Protocole et ports**  
Spécifiez les protocoles et les ports auxquels s'applique cette règle.

Étapes :

- Type de règle
- Programme
- Protocole et ports**
- Étendue
- Action
- Profil
- Nom

À quels ports et protocoles cette règle s'applique-t-elle ?

Type de protocole : Tous

Numéro de protocole : 0

Port local : Tous les ports  
Exemple : 80, 443, 5000-5010

Port distant : Tous les ports  
Exemple : 80, 443, 5000-5010

Paramètres ICMP (Internet Control Message Protocol) : Perso...

< Précédent   Suivant >   Annuler

Ainsi que pour toutes les IP local et distante :

Assistant Nouvelle règle de trafic sortant

**Étendue**

Spécifiez les adresses IP locales et distantes auxquelles s'applique cette règle.

**Étapes :**

- Type de règle
- Programme
- Protocole et ports
- Étendue
- Action
- Profil
- Nom

**À quelles adresses IP locales cette règle s'applique-t-elle ?**

☒ Toute adresse IP

☐ Ces adresses IP :

Apporter...  
Modifier...  
Supprimer...

Personnaliser les types d'interfaces auxquels cette règle s'applique :

**À quelles adresses IP distantes cette règle s'applique-t-elle ?**

☒ Toute adresse IP

☐ Ces adresses IP :

Apporter...  
Modifier...  
Supprimer...

< Précédent

Autorisation de la connexion a toutes les connexions qui réponde aux spécifications

Assistant Nouvelle règle de trafic sortant

**Action**

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

**Étapes :**

- Type de règle
- Programme
- Protocole et ports
- Étendue
- Action
- Profil
- Nom

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

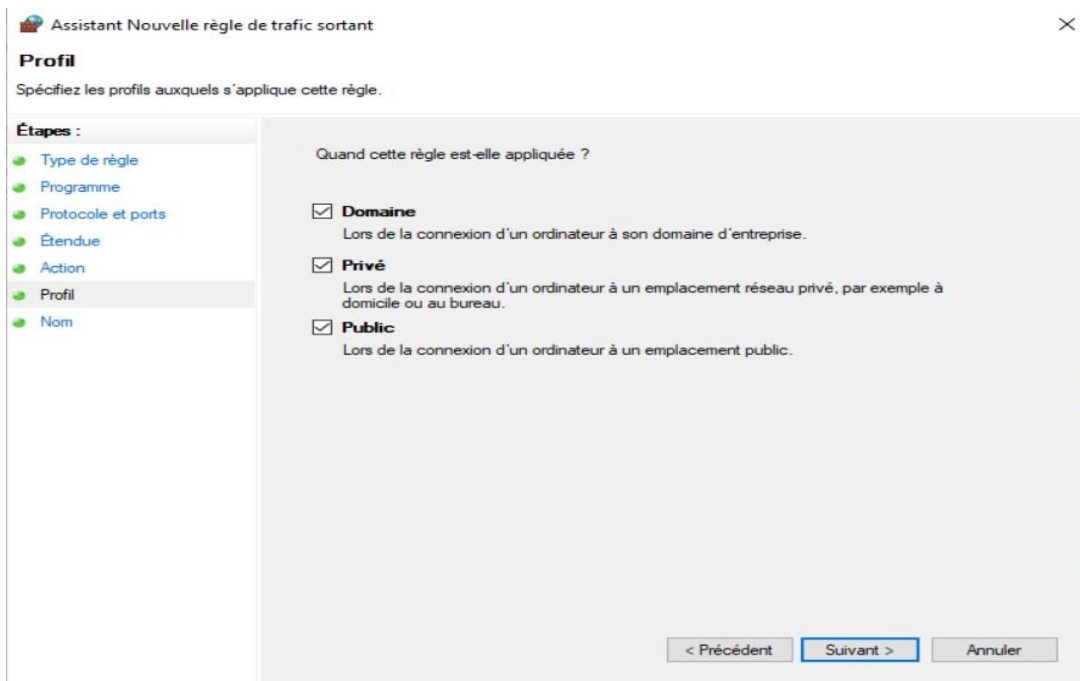
☒ **Autoriser la connexion**  
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

☐ **Autoriser la connexion si elle est sécurisée**  
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

☐ **Bloquer la connexion**

< Précédent

## Spécification des profils auxquels s'applique la règle



Puis pour tester si la nouvelle règle « ping » fonctionne nous avons réactiver le pare-feu Windows defender et tester de ping les machine entre elles :

Ping de 192.168.9.102 depuis le Pc-Vm1 qui à l'IP 192.168.9.101, FONCTIONNEL

```
C:\Users\stageiris1>ping 192.168.9.102

Envoi d'une requête 'Ping' 192.168.9.102 avec 32 octets de données :
Réponse de 192.168.9.102 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.102 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.102 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.102 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.9.102:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Ping de 192.168.9.101 depuis le Pc-Vm2 qui à l'IP 192.168.9.102, FONCTIONNEL

```
C:\Users\stageiris2>ping 192.168.9.101

Envoi d'une requête 'Ping' 192.168.9.101 avec 32 octets de données :
Réponse de 192.168.9.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.9.101 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.9.101:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

### Semaine 3

29/06/2020

Yazid, Tristan, Xavier

Screen shoot de pfsense :

```
pfSense - Netgate Device ID: e9e8f8f03ac68605327f
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 10.0.0.2/30
LAN (lan)      -> em1      -> v4: 192.168.9.254/24

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: █
```

- Erreur remarquer au niveau des interface réseau  
L'erreur était que les interface vmbr1 et 2 était inversé et donc sur pfsense les IP attribuer à l'interface LAN et WAN été fausses.
- Correction de l'erreur résultat ping de l'interface 10.0.0.2(interface WAN définis dans le pfsens) fonctionnel depuis pfsense

Suite a la correction de l'erreur remarquer, nous avons donc pus accéder à l'interface de PFSense et donc ainsi pu commencer à le paramétrer :

La première chose qui a été faite a été le changement du mot de passe admin, le mot de passe donc pour accéder à l'interface de pfsense en tant qu'admin est « IRIS ».

Ensuite nous avons vérifier sur le Dashboard que les adresse IP passerelle étai bien celle que l'on avait attribuer. Donc maintenant nous avons donc un pfsense qui communique bien avec la vmbr1, et donc nous avons essayer de faire en sorte que l'on puisse sortir sur internet via la patte WAN de pfsense qui est connecter à vmbr1 et aussi pour le LAN. Pour cela nous avons entré un petit script sur le server Proxmox :

Nous sommes entrés dans le fichier suivant « vi /root/kvm-networking-up.sh »



Et nous y avons entré le script suivant :

```
1  #!/bin/sh
2
3  ## IP forwarding activation
4  echo 1 &&&> /proc/sys/net/ipv4/ip_forward
5
6  # Point PFSense WAN as route to VMs
7  ip route change 192.168.9.0/24 via 10.0.0.2 dev vmbr1
8
9  # Point PFSense WAN as route to VPN
10 ip route add 10.2.2.0/24 via 10.0.0.2 dev vmbr1
```

- La première ligne active le routage
- La deuxième indique au serveur de sortir par vmbr1 puis de passer par le **WAN** du PFSense pour communiquer avec les VMs. Cela permet d'isoler **vmbr2** du reste de « PrivNET », cette sécurité sera renforcée, lors de la configuration d'iptables par un blocage complet des flux sur **vmbr2**.
- Même chose pour la dernière mais pour communiquer avec le(s) client(s) du VPN que nous configurerons par la suite.

Nous avons donc décider de faire en sorte que le script soit lancé automatiquement au boot lors du démarrage de vmbr1 :

Pour lui permettre de s'exécuter nous avons passé cette commande :

- `chmod +x /root/kvm-networking-up.sh`

Ensuite nous avons paramétrer son appel dans le fichier « interfaces » :

- `vi /etc/network/interfaces`

Et nous y avons rajouter la ligne suivante a la fin de la configuration du bridge vmbr2 :

**post-up /root/kvm-networking-up.sh**

Nous avons ensuite Reboot le server et nous avons constater quelque problème tel que :

Lorsque l'on essaye de ping les passerelle 10.0.0.1 et 192.168.9.1 les pings ne fonctionnent plus.

Or il le ping de l'adresse IP 192.168.9.254 qui permet d'accéder à l'interface de pfsense est désormais fonctionnel.

Depuis la vm Pfsense tous les pings sont fonctionnel.

Nous cherchons donc un moyen de paramétrer le pfsense de tel sorte à ce que notre machine virtuelle puisse sortir sur internet via la patte Wan.

Nous avons donc essayé de créer des règles dans le firewall pfsense, mais cela ne fonctionne toujours pas

**30/06/2020**

Yazid, Tristan, Xavier

Récapitulatif de la situation actuelle :

Aujourd'hui nous avons donc, 3VM Windows qui communique entre elles dans un même LAN (IP LAN : 192.168.9.0/24), ainsi qu'une VM Ubuntu qui est dans se LAN et qui répond aussi au ping des 3 autres PC. Nous avons également une VM PFsense qui tourne avec 2 pattes une LAN en 192.168.9.254/24 et une WAN en 10.0.0.2/30. Notre serveur dispose d'une carte réseau bridger à l'interface vmbr0, ainsi que d'une interface vmr1 qui sert de passerelle a notre patte WAN et une autre interface vmbr2 qui sert de passerelle à notre patte LAN.

Donc aujourd'hui :

Xavier

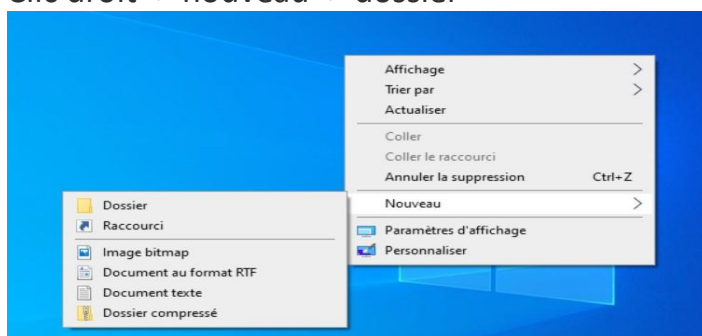
- Création d'un dossier de partage  
Ce dossier est accessible par toute les VM qui se trouve dans le même LAN, il permet à ces VM de se partager des fichiers ou autre.

Marche suivis :

### **Etape 1**

Sur le bureau

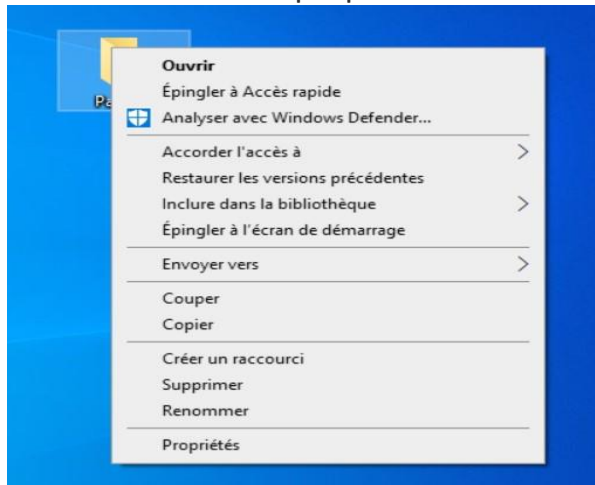
Clic droit -> nouveau -> dossier



## Etape 2

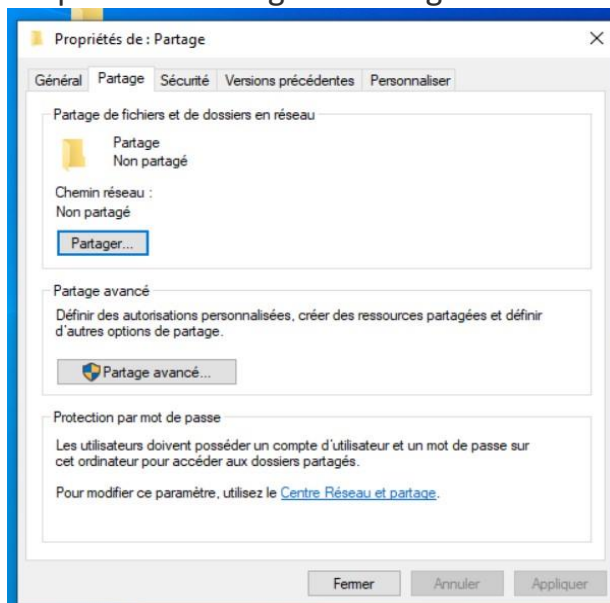
Nommer le dossier « Partage »

Ensuite clic droit -> propriété



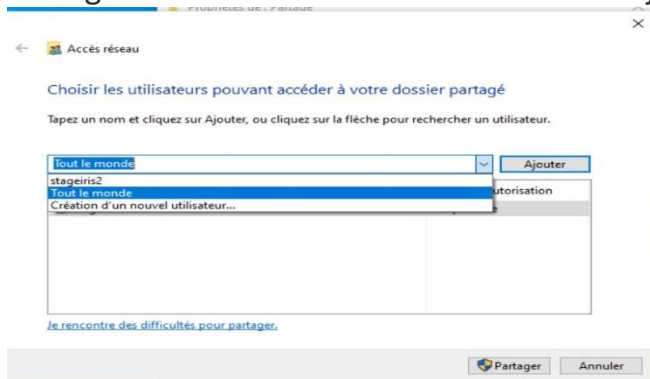
## Etape 3

Propriété -> Partage -> Partager



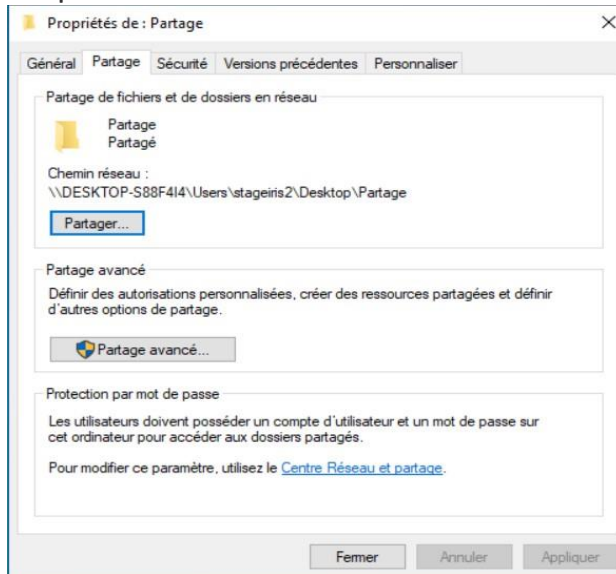
## Etape 4

Partager -> sélectionner Tout le monde -> Ajouter -> partager



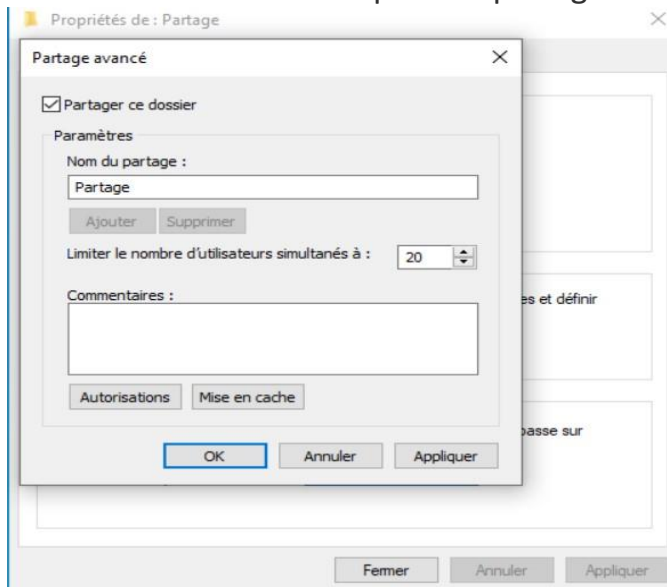
## Etape 5

Propriété -> Paramètre avancé



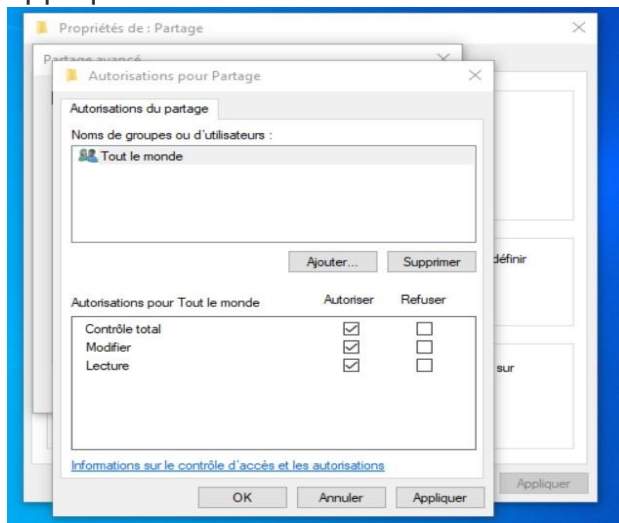
## Etape 6

Paramètre avancer -> cliquer sur partager ce dossier -> autorisation



## Etape 7

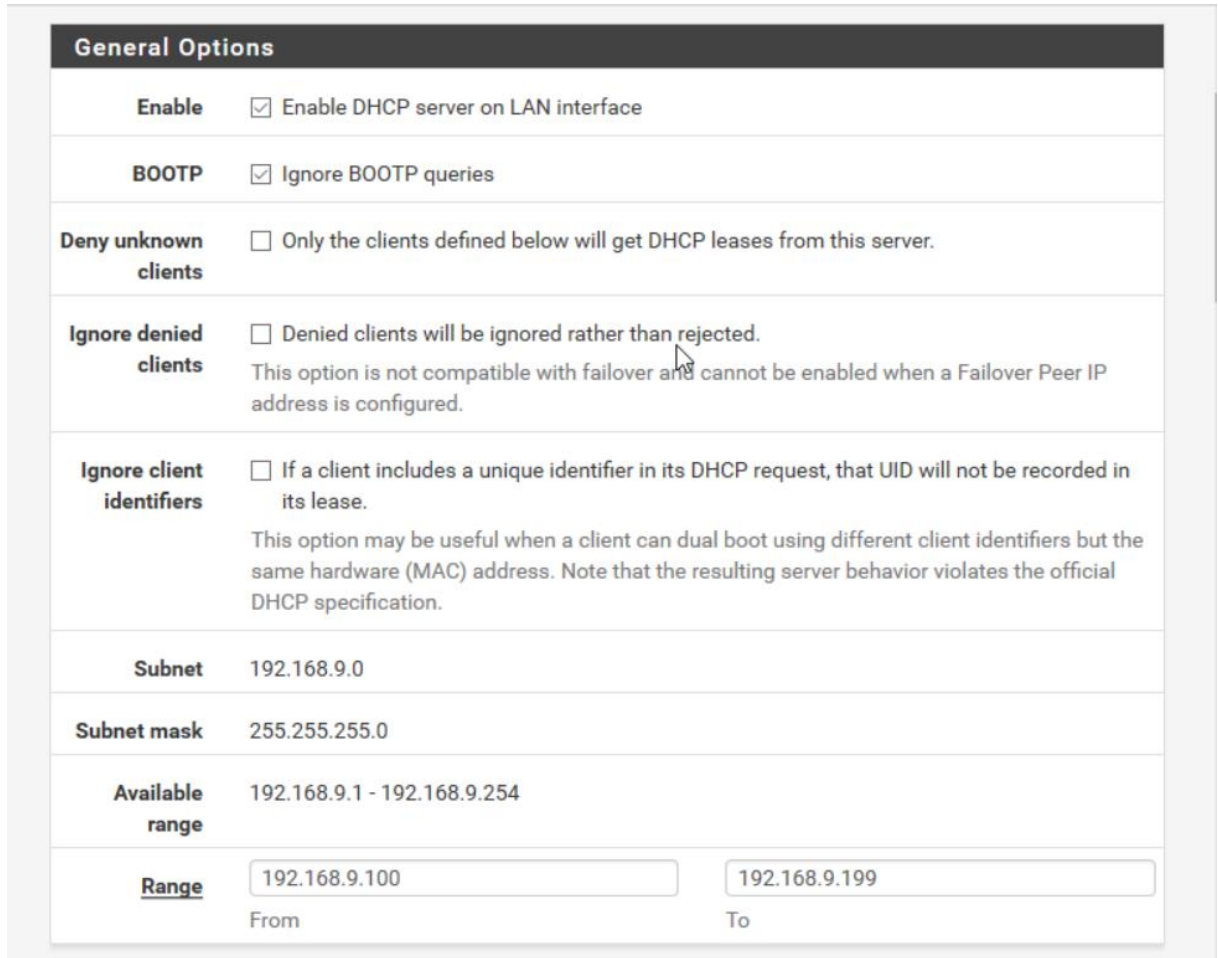
Autorisation -> autorisation pour tout le monde et cocher les 3 cases -> appliquer -> Ok



# Mise en place DHCP PFSense

Yazid

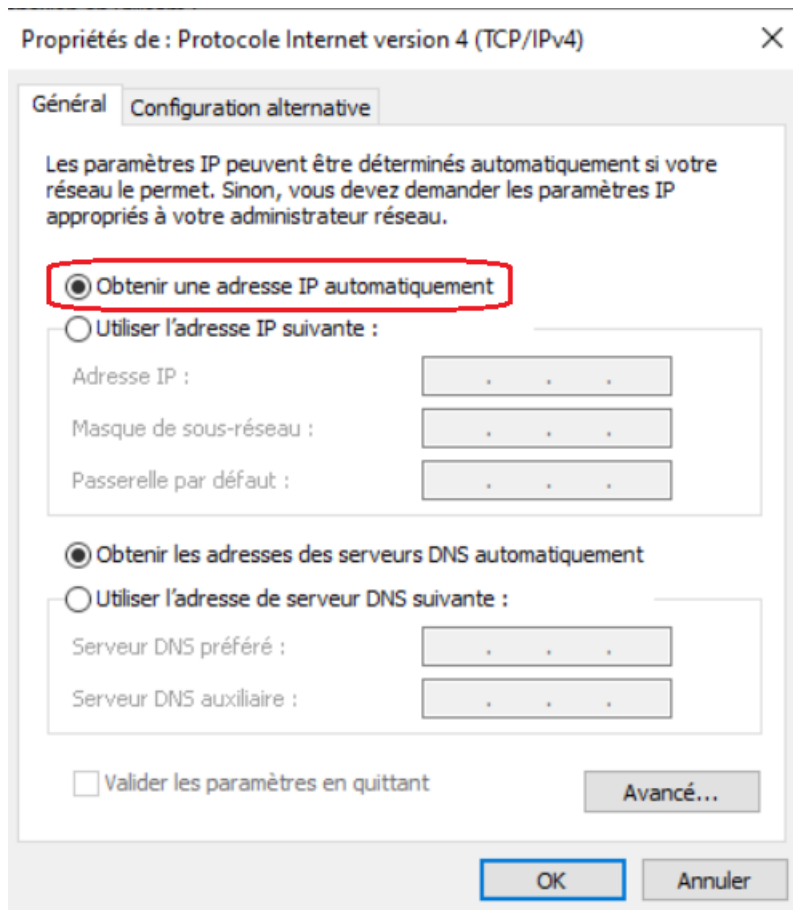
- 1ere étape : Configuration DHCP dans l'interface web de PFSense



The screenshot shows the 'General Options' tab for DHCP configuration in PFSense. The interface is a web form with various settings and input fields.

General Options	
<b>Enable</b>	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
<b>BOOTP</b>	<input checked="" type="checkbox"/> Ignore BOOTP queries
<b>Deny unknown clients</b>	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
<b>Ignore denied clients</b>	<input type="checkbox"/> Denied clients will be ignored rather than rejected. <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
<b>Ignore client identifiers</b>	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. <small>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.</small>
<b>Subnet</b>	192.168.9.0
<b>Subnet mask</b>	255.255.255.0
<b>Available range</b>	192.168.9.1 - 192.168.9.254
<b>Range</b>	<div><div>192.168.9.100</div><div>192.168.9.199</div><div>FromTo</div></div>

- 2eme étape : Configuration du mode de distribution de l'ip en automatique dans les VMs



- 3eme étape : Vérifier si la machine a bien reçu son IP avec la commande ipconfig



```
Invite de commandes
Microsoft Windows [version 10.0.18363.418]
(c) 2019 Microsoft Corporation. Tous droits réservés.

C:\Users\stageiris2>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : localdomain
    Adresse IPv6 de liaison locale. . . . : fe80::29a8:30b:758e:9e08%4
    Adresse IPv4. . . . . : 192.168.9.102
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.9.1

C:\Users\stageiris2>
```

- 4eme étape : être content que ça marche 😊

**01/07/2020**

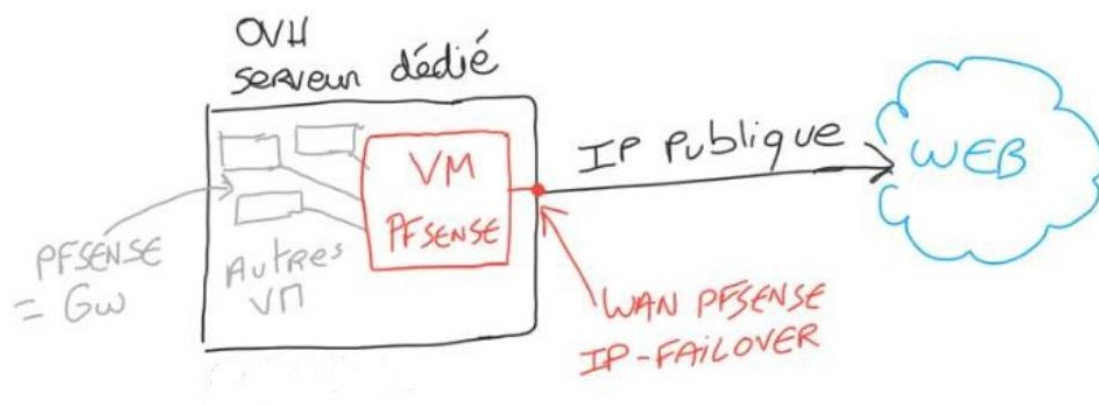
Point de situation avec les Professeurs. \*

**02/07/2020**

- Epluchage de tuto sur proxmox et les IPs fail
  - Paramétrage de proxmox avec l'IP fail donner
- Ce qui a permis à notre LAN d'accéder à internet

Marche suivis :

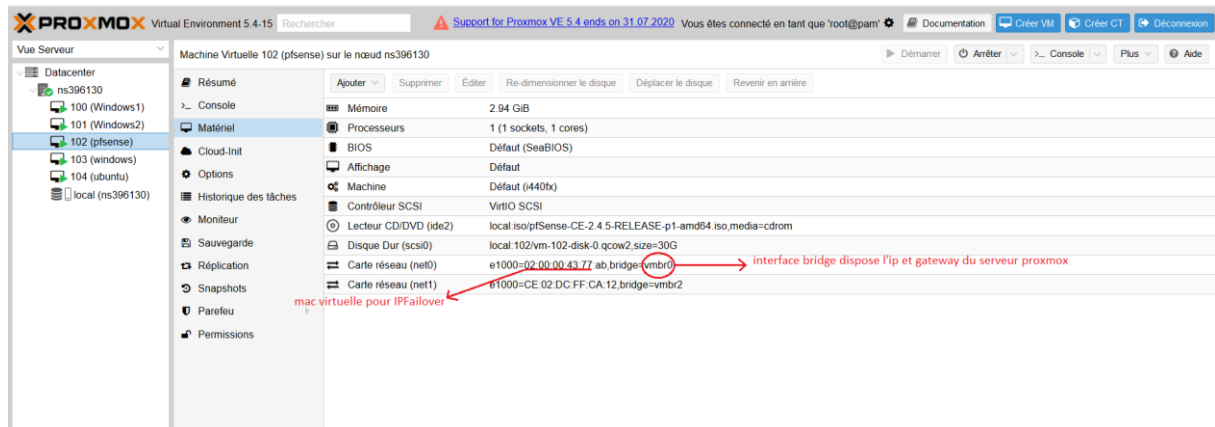
L'objectif de cette configuration est de conserver l'adresse IPv4 fournit par OVH pour administrer l'hyperviseur Proxmox. Tout en ayant une seconde adresse IPv4 (IP failover) pour sortir sur internet pour les machines virtuelles. On n'y vas 😊



Pour mener à bien cette configuration, il nous faut :

- Un serveur dédié chez OVH
- Une adresse publique IP-Failover et l'adresse MAC virtuelle associée
- Une machine virtuelle pfSense
- Une machine virtuelle cliente pour administrer le pfSense et tester l'accès au web (Windows 10 dans mon cas).
- Un serveur Proxmox

# I. Configurer l'adresse MAC statique sur la VM PfSense : Xavier



## II. pfSense : Interface WAN et routage : Yazid

```
pfSense - Netgate Device ID: 003ef2dc6f54cad33ee0

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 54.38.230.190/24
LAN (lan)      -> em1      -> v4: 192.168.9.254/24

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: 
```

On attribue l'IP failover à l'interface em0, après avoir attribuer l'interface em0 au WAN et em1 au LAN. (em0 = vmbr0, em1 = vmbr2 dans notre cas).

Attention : ne pas mettre de passerelle pour l'instant quand vous attribuez l'ip à em0.

## Etapes à suivre :

- Tapez 2
- Choisir 1 (cas de wan)
- Entrez (n)
- Entrez l'ip failover
- Entrez le masque sous reseau
- Faites entrer pour ne pas mettre de passerelle (on l'ajoutera après par cmd shell).
- Entrez (n)
- Faites entrer
- Après on tape 8 pour ouvrir le shell :
- Et on fait entrer ces 3 commandes suivantes :

```
route del default (supprimer la passerelle par default)
```

```
route add -iface 176.31.123.254 -link -iface em0  
(definir la passerelle sur le wan)
```

```
route add default 176.31.123.254 (définir la passerelle par default)
```

Et après on ping la 8.8.8.8 pour vérifier si notre VM PFsense arrive à sortir sur internet avec son IP failover

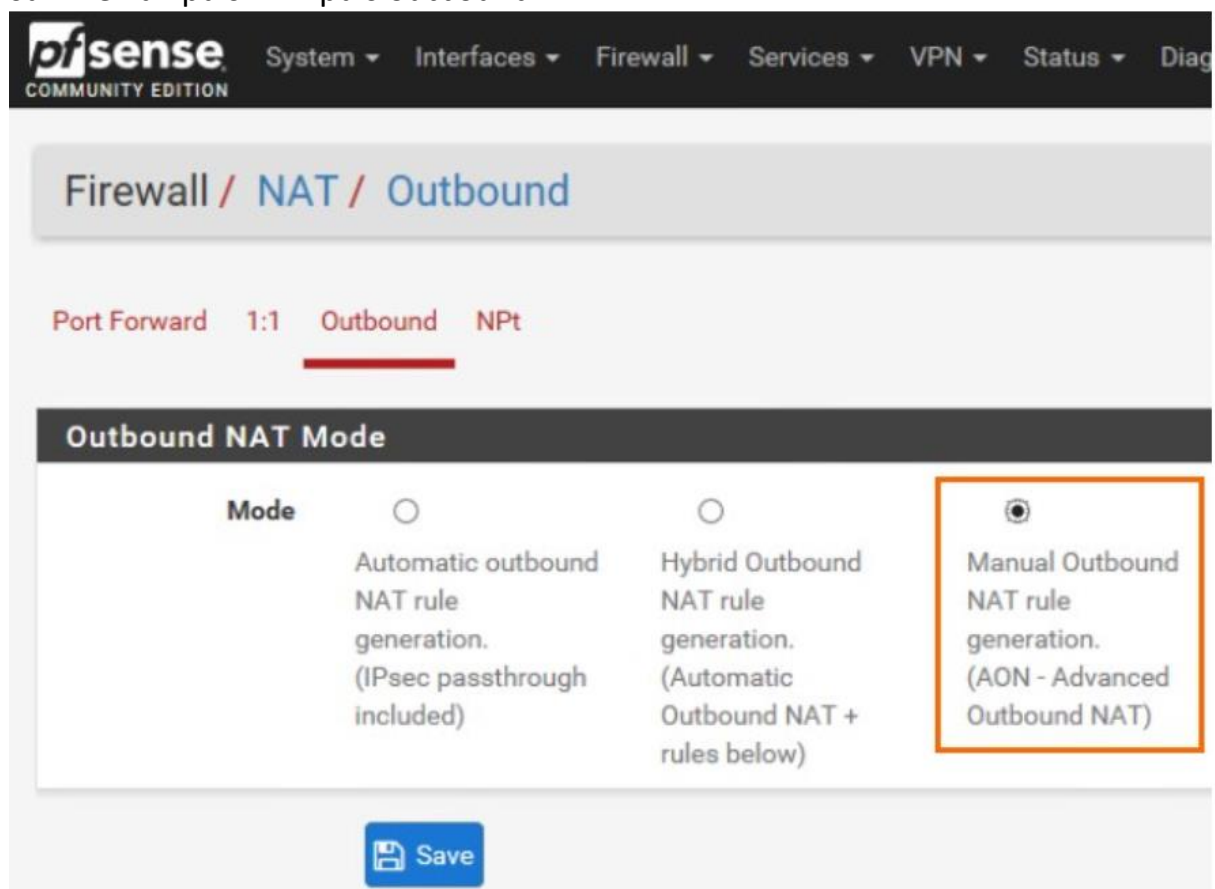
```
[2.4.5-RELEASE][root@pfSense.localdomain]/root:  
[2.4.5-RELEASE][root@pfSense.localdomain]/root: route del default  
del net default  
[2.4.5-RELEASE][root@pfSense.localdomain]/root: route add -iface 176.31.123.254  
-link -iface em0  
add host 176.31.123.254: gateway em0 fib 0: route already in table  
[2.4.5-RELEASE][root@pfSense.localdomain]/root: route add default 176.31.123.254  
add net default: gateway 176.31.123.254  
[2.4.5-RELEASE][root@pfSense.localdomain]/root: ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8): 56 data bytes  
64 bytes from 8.8.8.8: icmp_seq=0 ttl=117 time=4.297 ms  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=4.303 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=4.294 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=4.278 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=4.337 ms  
^C  
--- 8.8.8.8 ping statistics ---  
5 packets transmitted, 5 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 4.278/4.302/4.337/0.019 ms  
[2.4.5-RELEASE][root@pfSense.localdomain]/root:
```

Notre machine PFSense arrive bien à ping la 8.8.8.8 avec l'IP failover en passant par la passerelle du serveur proxmox mais pas nos machines Windows qui sont dans le LAN pour l'instant.

### III. pfSense : Règle de NAT

#### Tristan

On se connecte à pfsense avec l'administration web, on va dans menu on clique sur firewall puis NAT puis outbound.



On choisit le mode manuel et on enregistre.

Après, dans le bas de la page on clique sur le bouton ajouter une règle NAT et on fait entrer cette configuration

- Interface : WAN
- Protocol : Any
- Source : Network - 192.168.9.0/24 (adresse choisie pour l'interface LAN) pour NATer les hosts connectés au LAN isolé

- Destination : Any (Internet)
- Translation : Interface Adresse (c'est l'IP de l'interface WAN qui sera utilisée pour sortir sur Internet).

Après vous valider la création de la règle et appliquer la configuration.

Puis on ping la 8.8.8.8 dans une VM Windows du LAN pour tester

```

C:\Users\stageiris2>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=4 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=4 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=4 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=4 ms TTL=116

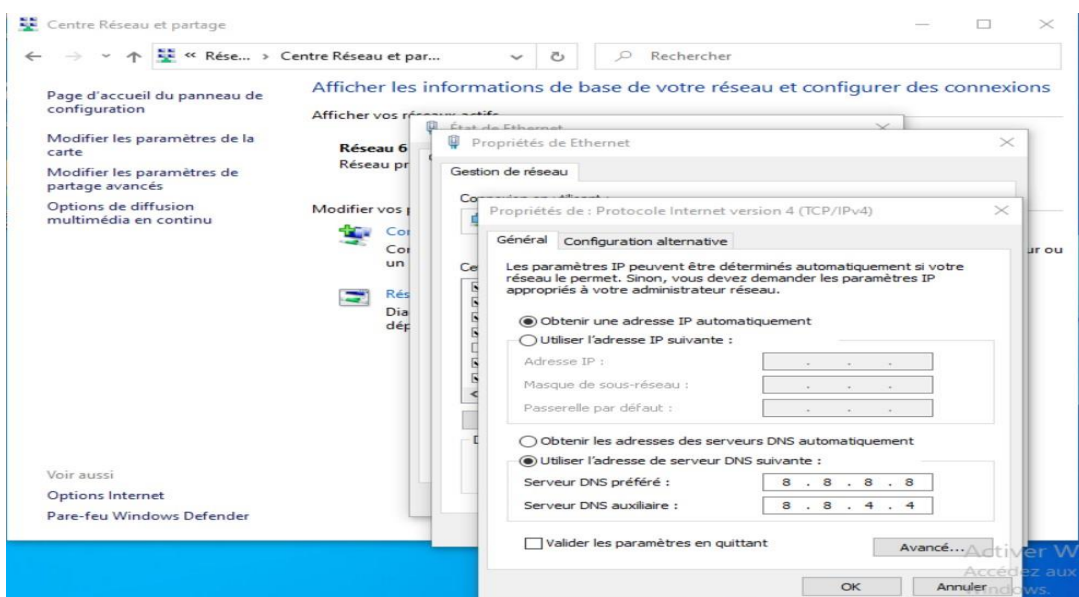
Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 4ms, Maximum = 4ms, Moyenne = 4ms

C:\Users\stageiris2>

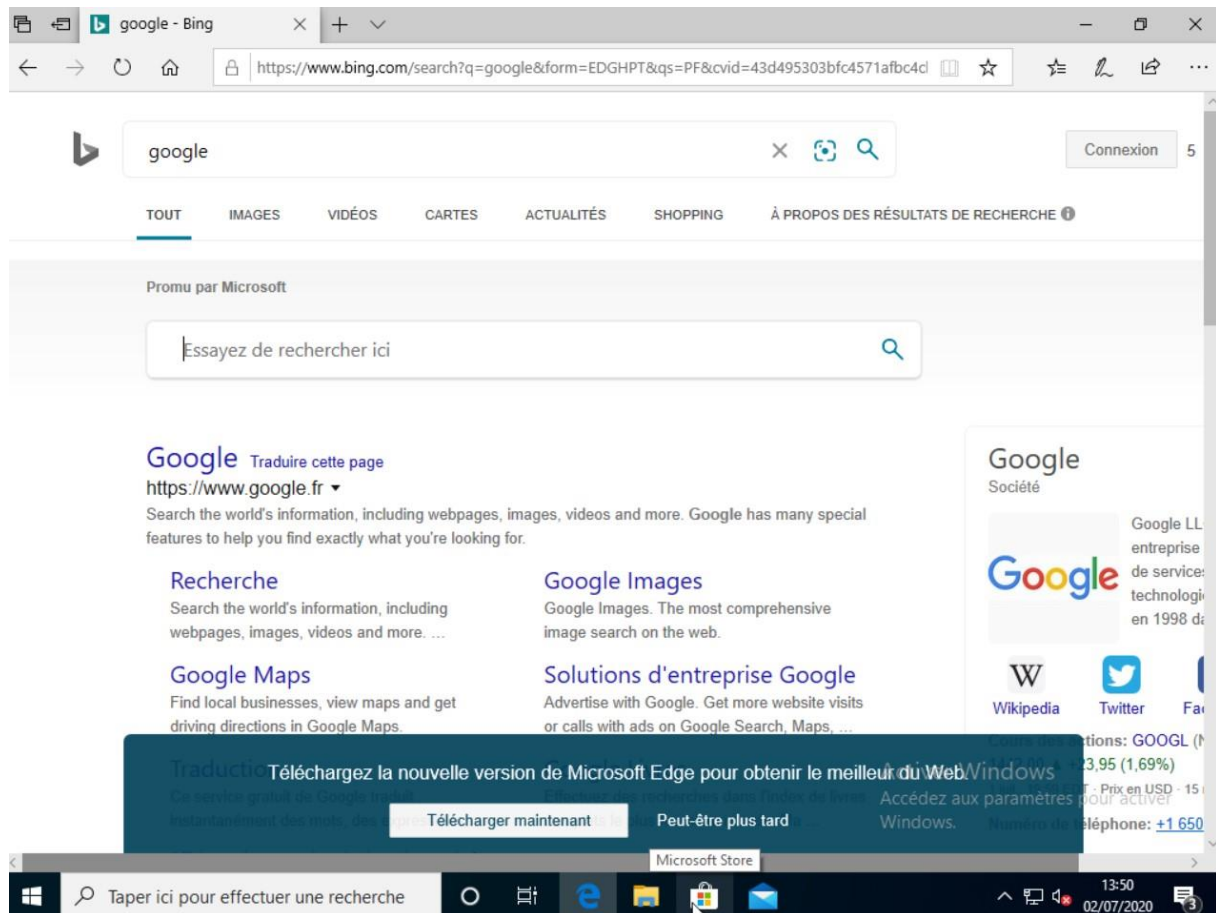
```

Ensuite on rajoute quelque configuration à nos Vm Windows :

Centre réseau et partage->Etat d'Ethernet->Gestion de réseau->Propriétés de : Protocole internet version4(TCP/IPV4)



Puis nous testons une recherche internet en ouvrant l'explorateur :



Ça marche ! 😊

A noter que cela nous aura pris la journée entière.



**03/07/2020**

- Installation de Windows server2019
- Installation serveur web apache sur Ubuntu
- Réalisation d'un schéma d'architecture illustrant l'imbrication de pfsense, des vms dans proxmox.
- Recherche sur les Fonctionnalité de Windows Server

#### Installation de Windows serveur : **Tristan et Xavier**

Pour l'installation de ce Windows serveur nous avons d'abord télécharger l'iso puis uploader sur le server proxmox. Ensuite grâce a une recherche de tuto d'installation que nous avons mener nous avons pus l'installer sur notre Proxmox a l'aide du tuto suivant :

<https://www.youtube.com/watch?v=7DPmNK5d-cY>

Dans ce tuto nous voyons son installation et quelque paramétrage de base pour faire accéder notre serveur a internet.

Pour la suite nous verrons comment paramétrer notre serveur Windows et comment exploré ses fonctionnalités.

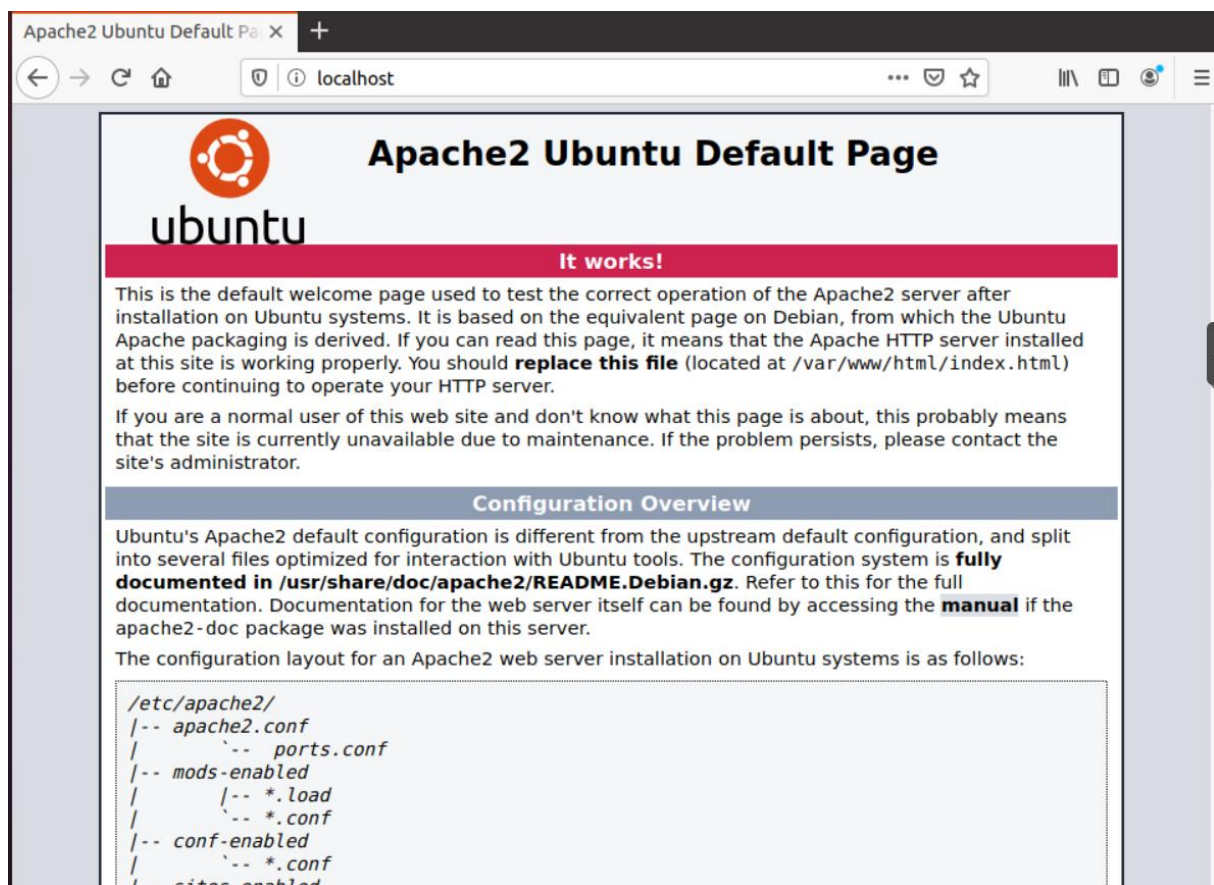
# REDIRECTION DE PORT POUR SERVEUR WEB APACHE DANS VM UBUNTU

I – Installation du serveur Apache dans une machine UBUNTU : **Yazid**

Ceci est assez simple, il suffit juste de passer une ligne de commande dans le terminal.

Commande : `apt install apache2`

Une fois l'installation terminée, on va sur localhost dans le navigateur web pour vérifier si notre serveur apache est bien fonctionnel.

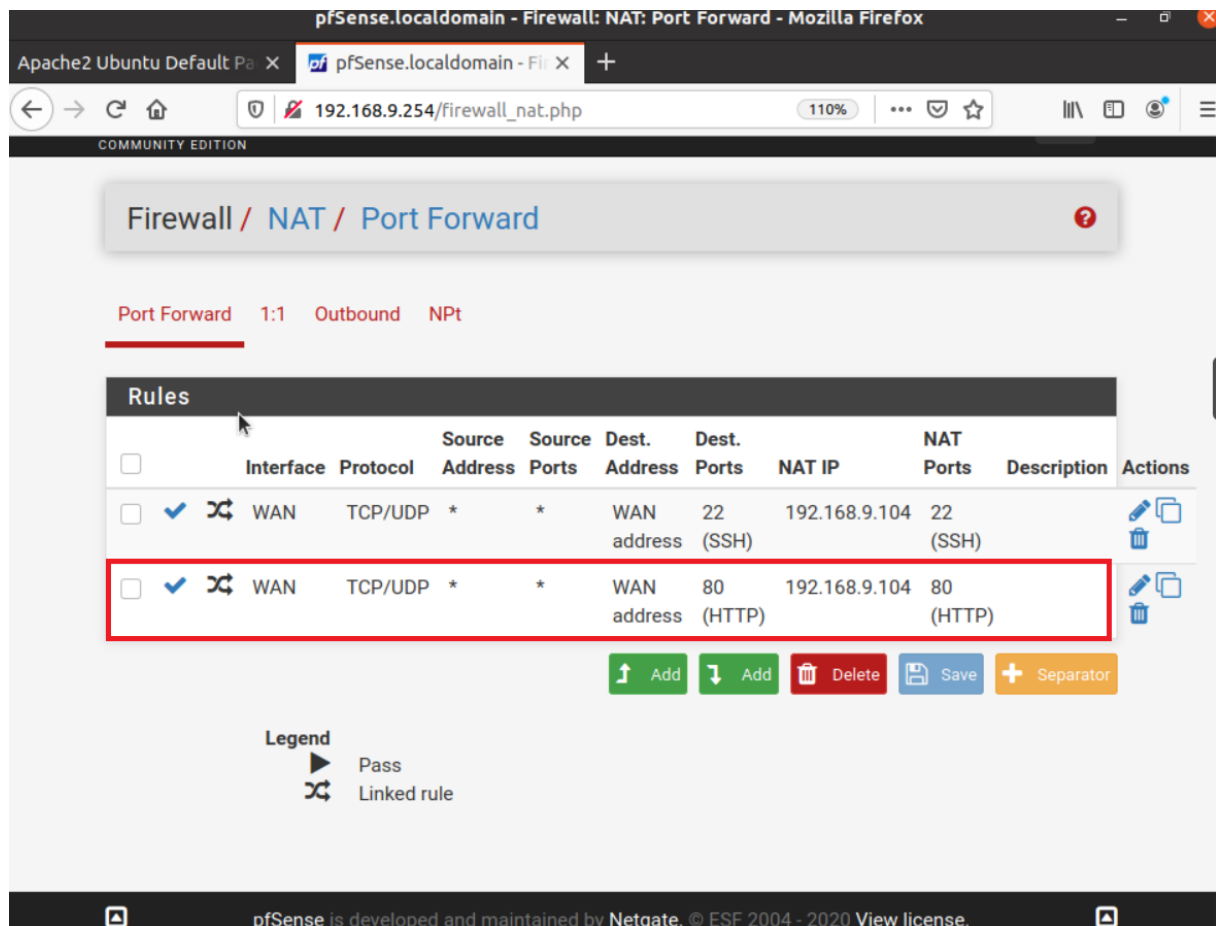


Voilà ce qui s'affiche, la page html par défaut d'apache, qui peut être modifiée en accédant au répertoire /var/www/html au cas ou si vous voulez la remplacer par la vôtre.

## II – Redirection de port :

Pour l'instant notre serveur web est accessible qu'à l'intérieur de votre réseau local. Afin de pouvoir y accéder de l'extérieur (internet), on va faire alors une redirection de port du WAN vers l'ip de la machine Ubuntu, à travers le port http.

Du coup, on ouvre la page de configuration pfsense et on accède à FIREWALL > NAT > Port forwarding. Puis on rajoute une règle comme il est indiqué sur la photo si dessous.



Et après essayez de lancer cette adresse <http://votreippublique> dans votre téléphone en 3G préféablement pour voir si vous pouvez bien y accéder de l'extérieur.

Windows server 2019 fonctionnalités

Windows Server 2019 est le système d'exploitation qui relie les environnements locaux avec Azure. Il ajoute de nouvelles couches de sécurité tout en vous aidant à moderniser vos applications et votre infrastructure.

Gérez vos serveurs, vos cluster, votre infrastructure hyperconvergente et vos ordinateurs Windows 10 grâce à cette application sur navigateur.

Découvrez comment migrer vos charges de travail Windows vers Azure en utilisant nos guides et ressources étape par étape

Mettre à jour votre infrastructure de stockage et de serveur sur site avec le système d'exploitation le plus récent pour garantir la sécurité et bénéficier du meilleur rapport prix/performances.

Faciliter la création d'applications Cloud natives et mettre à jour les applications classiques avec des conteneurs et des microservices.

Gérer les serveurs, les clusters et l'infrastructure hyperconvergente avec Windows Admin Center, une nouvelle application gratuite basée sur un navigateur.

Étendre les serveurs sur site à Azure pour les services, y compris la sauvegarde, la récupération d'urgence et les ressources de calcul et de stockage à la demande.

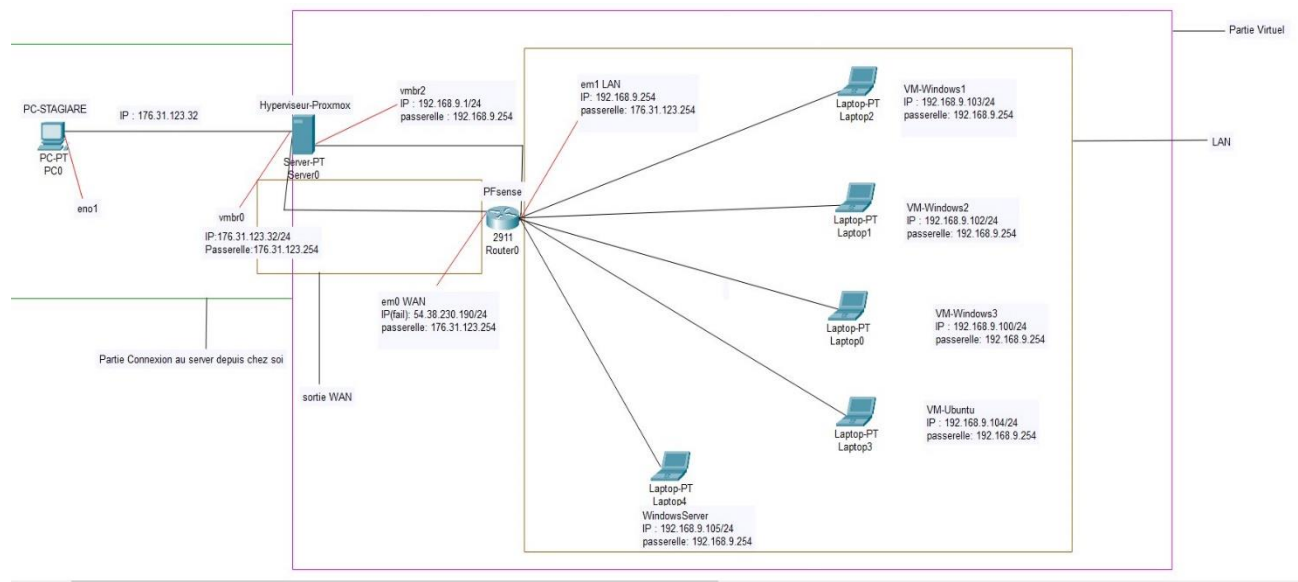
<https://docs.microsoft.com/fr-fr/windows-server/get-started-19/whats-new-19>

<https://www.ionos.fr/digitalguide/serveur/outils/windows-server-2019/>

- Amélioration de la prise en charge des scénarios de cloud hybride pour permettre aux utilisateurs de combiner une infrastructure on-premise et cloud
- Prise en charge complète du nouveau système [Windows Admin Center](#) pour la gestion des infrastructure standards et hybrides
- Intégration de Windows Defender Advanced Threat Protection pour offrir une protection plus complète
- Intégration des sous-système Windows pour Linux
- Possibilité d'installer des conteneurs Linux sur Windows Server 2019

- Support et sécurité améliorée des machines virtuelles blindées (Shielded VM) avec Hyper-V
- Réduction de la taille de l'image Core de Windows Server
- Gestion Kubernetes des hôtes
- Amélioration des solutions Hyperconvergées

Schéma d'architecture d'imbrication de pfsens et vm : **Xavier**



## **Semaine 4**

**06/07/2020**

- Mise en place d'un portail captif via PFSense (Tristan, Alexandre)  
Cela permettra de demander à l'utilisateur de se logger pour accéder à internet.
- Création de Vlan (Configuration test) (Yazid)  
But : faire communiquer les différents VLAN.
- Exploration de Windows Server et ses fonctionnalités (Xavier, Erwin)  
BUT : connaître les fonctionnalités d'un serveur Windows et ainsi savoir le manipuler.

Notre travail du jour a été basé essentiellement sur de la recherche et compréhension avant de passer à la manipulation.

**07/07/2020**

- Mise en place d'une page de connexion en PHP : (Yazid, Tristan, Xavier, Erwin)

Le but sera que lorsqu'un utilisateur de n'importe quel type veut se connecter à internet, il devra ouvrir son navigateur web et une fois sur le navigateur la page de connexion PHP sera affichée. Il n'aura plus qu'à s'identifier et il sera redirigé vers la page de login du portail captif de PFSense qui lui demandera de se logger et ainsi accéder à internet.

### **Etape 1**

Installation d'Apache, PHP, MySQL sur une VM Ubuntu.

### **Etape 2**

Création d'un script.sql qui créera la DATABASE qui contiendra les identifiants des utilisateurs

### **Etape 3**

Écriture du code PHP de la page de connexion et redirection de la page vers le portail captif.

