

DOCUMENTATION D’ARCHITECTURE

PROJET INFRA & SI

MISTRAL / PHAM / MARTHELY | Ynov 2021/2022

# Sommaire

1. Définition du réseau

* Schéma Réseau
* Plan d’adressage

1. Bonnes pratiques

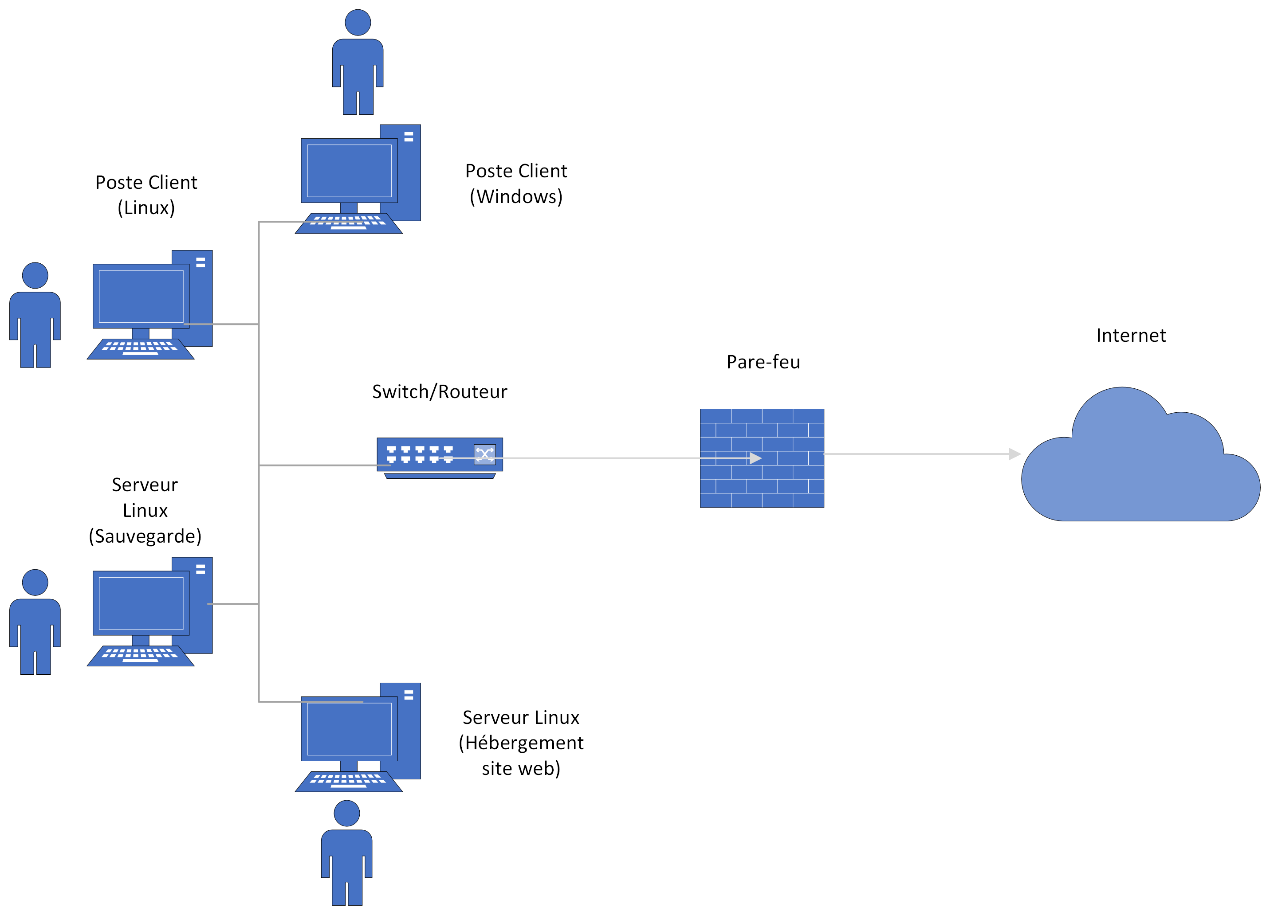
* Configuration des Clés Privées
* Configuration des MDP root

1. Mise en œuvre de la solution

* Configuration du Pare-Feu
* Configuration des Clients
* Configuration du Serveur
* Configuration du Service de Backup

# Définition du réseau

Schema reseau



PLAn d’adressage

|  |  |  |  |
| --- | --- | --- | --- |
| Service | Adresse Réseau | Masque | Passerelle |
| Client 1 | 10.10.10.1 | 255.255.255.284 | 10.10.10.6 |
| Client 2 | 10.10.10.2 | 255.255.255.284 | 10.10.10.6 |
| Serveur Web | 10.10.10.3 | 255.255.255.284 | 10.10.10.6 |
| Serveur Backup | 10.10.10.4 | 255.255.255.284 | 10.10.10.6 |
| Libre | Libre | Libre | Libre |
| Pare-feu | 10.10.10.6 | 255.255.255.284 | 10.10.10.6 |

# 2.Bonnes pratiques

* Configuration des Clés Privées
* Configuration des MDP root

# 3.Mise en œuvre de la solution

* Configuration du Pare-Feu

Nous allons présenter ici la démarche de configuration du pare-feu étape par étape, ici à l’aide d’une nouvelle machine virtuelle.

|  |
| --- |
| Utiliser le type de configuration « Typical » qui est celle recommandée, pas besoin d’option avancée pour le moment  Une image contenant texte  Description générée automatiquement  Après avoir préalablement télécharger l’iso PfSense, indiquer le chemin de ce dernier à la VM  Une image contenant texte  Description générée automatiquement  Ici il est possible de renommer directement le nom de la VM ainsi que son emplacement. L’emplacement n’est pas nécessaire à la modification cependant.  Une image contenant texte  Description générée automatiquement  Vient ensuite la possibilité d’allocation de l’espace disque, ici nous mettons 20GB de façon à être large mais le pare-feu ne demande pas autant d’espace. Sélectionner l’option de séparation du disque virtuel en plusieurs fichiers.  Une image contenant texte  Description générée automatiquement  Ici vient le récap de la création de notre VM. Pour finir le processus appuyer tout simplement sur « Finish » si tous les éléments vous conviennent    Petite étape à ne pas oublier, notre pare-feu doit comporter 2 adaptateurs internet, car c’est ce dernier qui fera office de passerelle entre le WAN et le LAN. Pour ce faire sur la VM, effectuer un clic droit et ensuite sur « Settings ».    Appuyer sur « Add », ensuite sélectionner « Network Adpatater ».  Une image contenant texte  Description générée automatiquement  Une fois ce nouvel adaptateur ajouté, mettre celui-ci en « host-only ». Il ne reste plus qu’à lancer maintenant le pare-feu. |

Ci-joint une série de captures des étapes à suivre

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

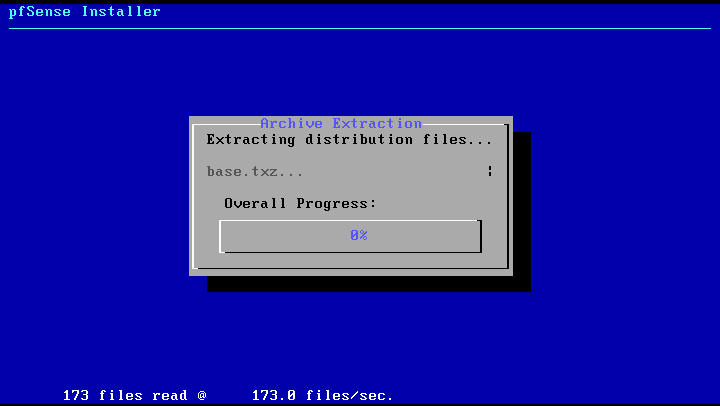
Description générée automatiquement



Ici appuyer sur la touche espace pour que l’étoile apparaisse signifiant ainsi « all »

Une image contenant texte

Description générée automatiquement



Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

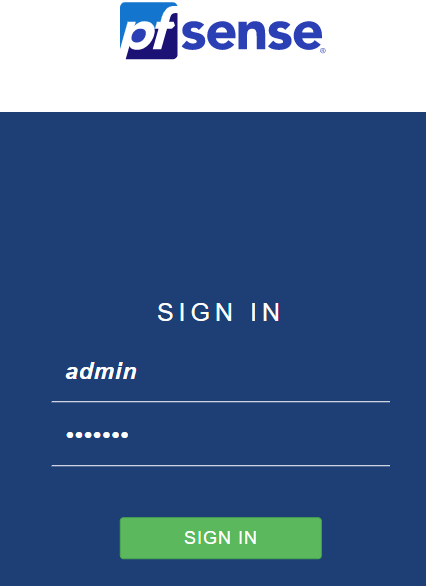
Description générée automatiquement

Nous remarquons ici la présence d’un WAN et d’un LAN avec chacun une adresse IP attitrée. Appuyer sur 8 pour accéder à l’interface de commande qui nous sera utile par la suite

Une image contenant texte

Description générée automatiquement

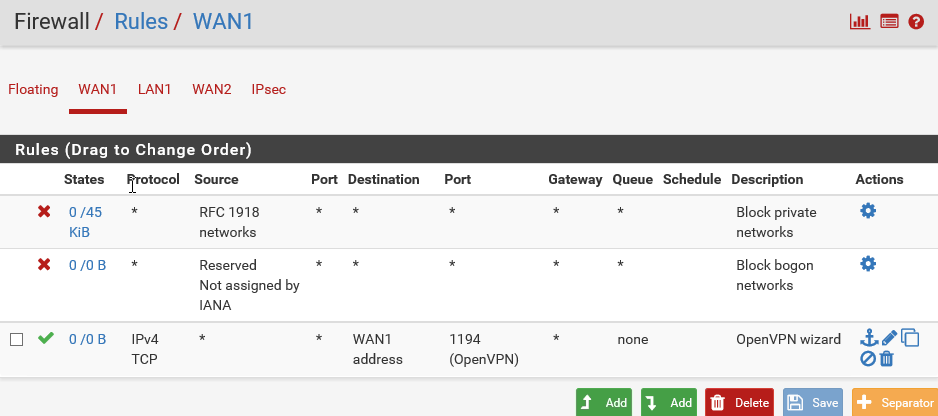
Entrer l’adresse IP Em0 (WAN) dans le navigateur internet de votre choix. Il est normal de tomber sur cette page, sélectionner simplement « continuer sur *adresse\_ip-em0* »



Une fois sur cette page ID : admin, Mot de passe : pfsense. Afin d’accéder à l’interface PfSense



Dans le menu dépliant sélectionner « Firewall » puis « Rules »



2 règles sont déjà ici prédéfinies, nous allons les supprimer. Pour ce faire, appuyer sur l’engrenage en fin de ligne de l’un ou de l’autre

Une image contenant texte

Description générée automatiquement

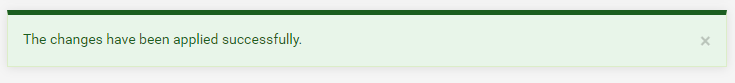
Aller en bas de page et désélectionner ces 2 options. Puis appuyer sur « Save ».



Appuyer ensuite sur « Apply Changes » pour littéralement appliquer les changements.



Cependant notre pare-feu va bloquer le rafraîchissement de notre page. Dans l’interface de notre VM taper la commande *pfctl -d* qui va désactiver le pare-feu pour nous permettre d’affecter nos changements.



En retournant sur notre navigateur nous avons ce message qui s’affiche nous confirmant notre opération



Juste en dessous de la liste des règles sélectionner l’un des boutons « Add »

Une image contenant texte

Description générée automatiquement

Dans le champ « Destination », changer le type en « Wan adress » et le Port Range en « http ». Puis sur « Save »

Une image contenant texte

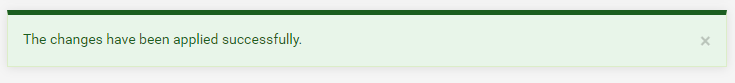
Description générée automatiquement

Réitérer l’opération pour le port « Https » cette fois-ci afin de pouvoir complètement utiliser notre pare-feu sans avoir à le désactiver à chaque fois.

Une image contenant table

Description générée automatiquement





Tout comme pour la suppression des règles principales après avoir fait la « Save », appuyer sur « Apply Changes » et taper dans l’interface de commande du pare-feu sur la VM la commande *pfctl -d* pour appliquer les changements. Une l’opération terminée le message de confirmation s’affichera.

Une image contenant texte

Description générée automatiquement

En appuyant sur le logo PFSense en haut a gauche, vous accédez au récapitulatif de votre pare-feu avec en bas à droite les règles d’interfaces que nous avons programmées.

Une image contenant texte

Description générée automatiquement

Une fois ces étapes passées, nous allons configurer notre adresse IP de notre LAN. Pour ce faire taper « 2 »

dans l’interface de commande du pare-feu

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

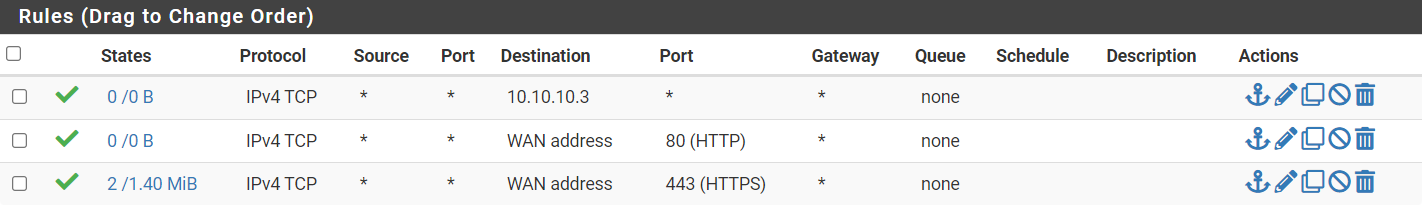
Tableau de filtrage :

Règles LAN :

Une image contenant texte

Description générée automatiquement

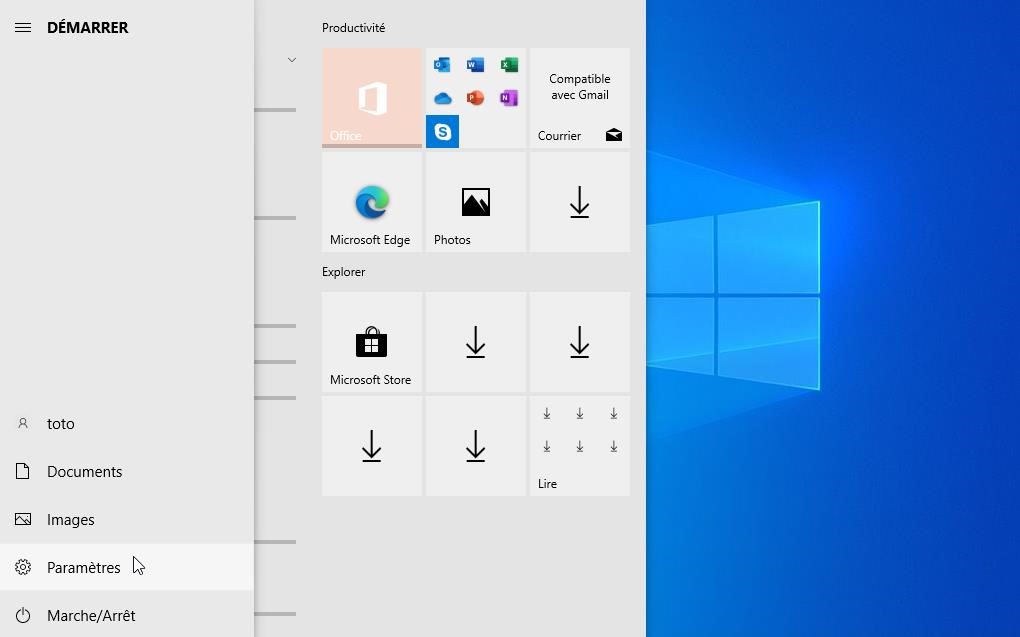
Règles WAN :



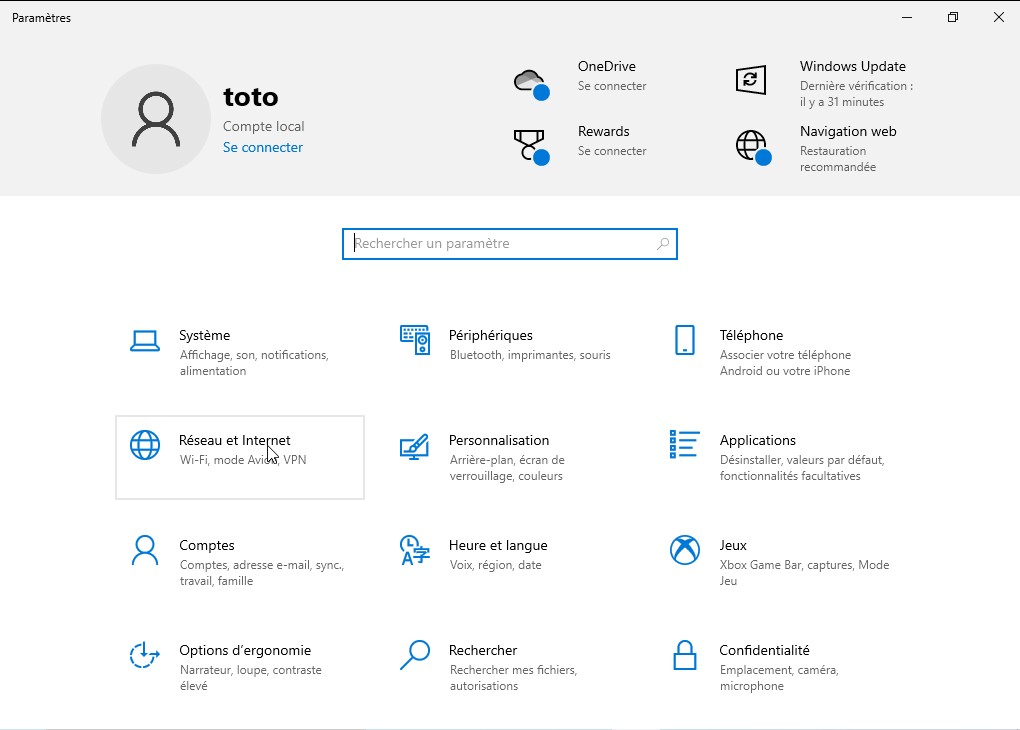
* Configuration des Clients

Dans cette partie, nous allons traité de la configuration nécessaire aux machine clients de notre sous-réseau.

SOUS WINDOWS



Aller dans les paramètres

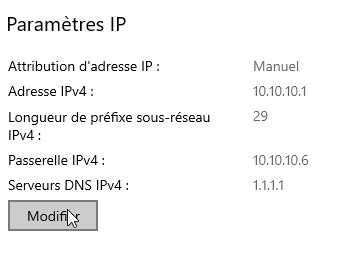


Sélectionner « réseau et Internet »

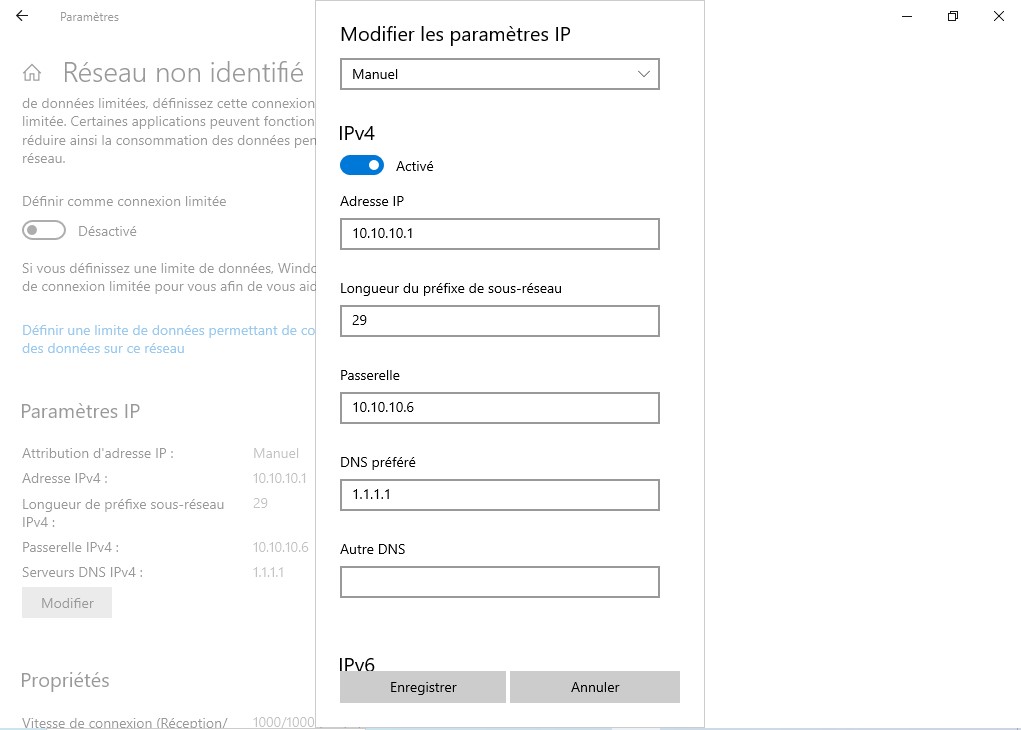
Une image contenant texte

Description générée automatiquement

Puis aller dans « Propriétés »



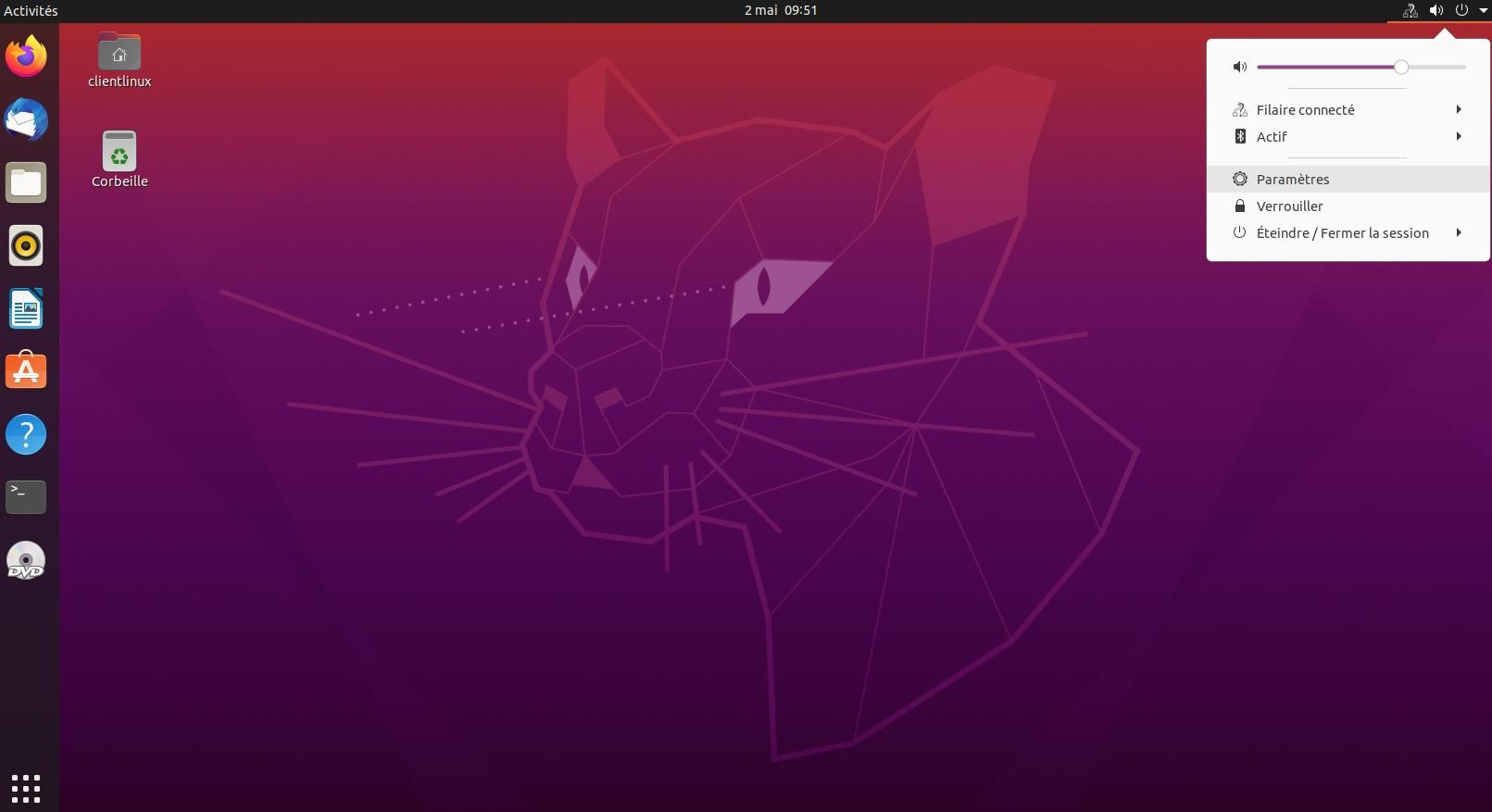
Ensuite sur « Modifier »



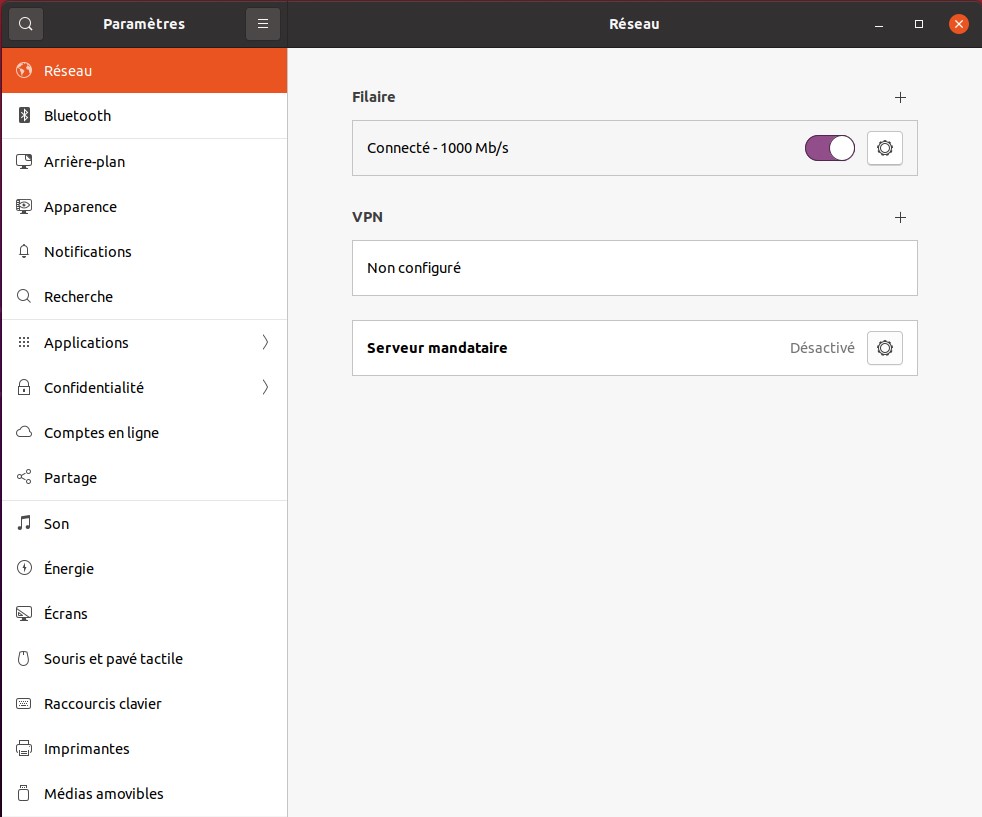
Basculer en mode « Manuel » si nécessaire et configurer l’adresse IP de votre Pc. La longueur du sous-réseau, de même que la passerelle correspondent à celles de votre pare-feu préalablement configuré. Le DNS quant à lui peu rester du « 1.1.1.1 » le choix ici n’est pas très important.

Une fois ces modifications effectuées, appuyer sur « Enregistrer ». Ca y est votre Client Windows est lié à votre pare-feu et à un accès internet fonctionnel grâce à ce dernier.

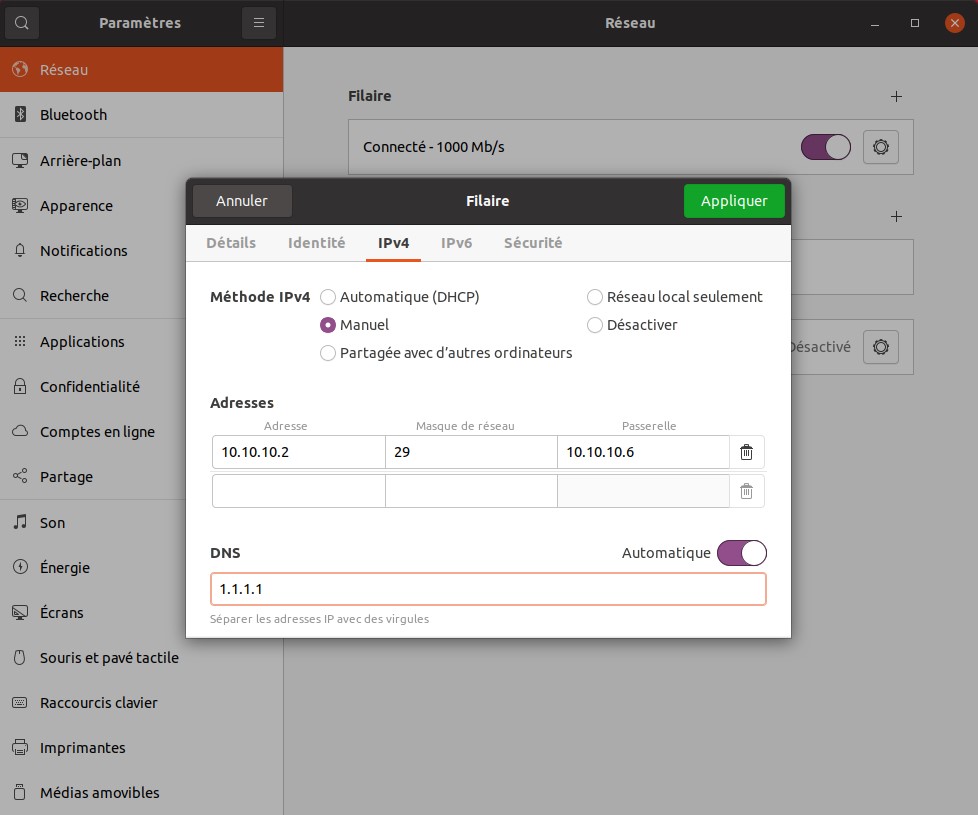
SOUS LINUX



En haut à droite sélectionner le menu démarrer, puis cliquer sur «Paramètres».



Appuyer sur l’engrenage de « Filaire » pour entrer dans le menu de configuration.



Sélectionner ensuite « IPv4 », puis passer en mode « Manuel ». Il ne vous reste plus qu’à définir tout comme votre client Windows, votre adresse IP, ainsi que le masque de sous-réseau et la passerelle (correspondant

ici aussi au pare-feu). Le DNS lui aussi peut rester 1.1.1.1

* Configuration du Serveur

Dans cette partie, nous allons traité de l’installation de notre serveur web.

* Configuration du Service de Backup

Dans cette partie, nous allons voir comment instaurer une sauvegarde des fichiers du site web.

Pour ce faire, nous devons mettre en place un script sur notre machine de backup.

Tout d’abord, en allant dans le terminal de commande, entrer la commande « sudo su root » . Ceci va nous permettre de rentrer dans le mode root du terminal, ainsi nous pourrons paramétrer nos configurations de la même manière que le mode cron (que nous verrons plus tard).

Une fois en mode root, nous allons entrer la commande « ssh-keygen » :

Une image contenant texte

Description générée automatiquement

Ceci viens de créer une clé public et privé d’identification.

Suite à ça, il faut entrer la commande suivante « ssh-copy-id USER@ADDRESS » (où USER = le nom de compte d’utilisateur de la machine serveur et ADDRESS = adresse IP de la machine serveur) :

Une image contenant texte

Description générée automatiquement

Cette commande va ainsi copier la clé publique de notre machine de backup dans les fichiers de notre machine serveur. Ainsi, lors de notre transfert de données, les clés d’identifications ne seront pas demandées car elles seront déjà renseignés.

Nous allons maintenant passer à l’élaboration de notre script de récupération.

Il faut d’abord créer un fichier .sh, dans lequel nous mettrons ces lignes suivantes :

Une image contenant texte

Description générée automatiquement

Explication des lignes :

3 – Création d’une variable qui servira de nom de fichier de sauvegarde (« backup\_{date/heure} »)

5 – Création du nouveaux dossier qui accueillera la sauvegarde

7 – Commande SCP qui va récupérer le fichier index.html en indiquant d’abord le nom de l’utilisateur sur la machine visé, son adresse IP, puis le chemin où se trouve le fichier voulu, et ensuite on indique le chemin dans lequel le fichier récupéré doit être mit

8 – Même commande mais pour le fichier index.css

Maintenant, passons à la dernière étape, l’automatisation de ce script.

Pour ce faire, nous devons ouvrir l’outil « crontab ». Il s’agit d’un outil d’automatisation de tâches, dans lequel on peut indiquer une fréquence de réalisation. Toujours dans le terminal de commande, nous allons faire la commande « crontab -e » :



Ce qui va ouvrir un éditeur de texte du fichier crontab :



Dans ce fichier la ligne présente ci-dessus va faire en sorte de lancer le script « GetBackup.sh » (notre script de récupération) tous les jours à 12h00.

Et voilà, notre système de récupération des données est établie fonctionnel !