**Utilisation de puTTY pour se connecter en SSH à "Ubuntu Server".**

**Objectifs**

Le but est d’utiliser **putty.exe** pour administrer "**Ubuntu server**" avec une adresse IP 10.57.**x**.**y**.

L'avantage d'utiliser puTTY est que vous pouvez copier-coller des commandes de l'ordinateur réel vers la fenêtre puTTY ou de copier des commandes de la fenêtre puTTY vers l'ordinateur réel.

**Mise en place**

Il faut vérifier que le serveur SSH est installé et fonctionnel sur "Ubuntu Server".

Il faut configurer le pare-feu sur "Ubuntu Server" pour autoriser l'accès au serveur SSH.

Il faut créer une redirection de port dans le pare-feu du routeur pfSense.

La modification des paramètres du routeur pfSense se fait en utilisant l'interface WEB.

Pour modifier la configuration du routeur pfSense à partir de votre serveur réel.

**https://10.57.x.y**

nom d'utilisateur = admin

mot de passe = pfsense

**Étape 1 - Vérification de la configuration du serveur SSH dans "Ubuntu server"**

Voici la commande qui permet de vérifier l’état du serveur SSH.

**sudo systemctl status ssh**

Si vous voyez ce message dans le résultat de la commande précédente c'est que le serveur SSH est installé et fonctionnel.



**Voici deux commandes supplémentaires à utiliser si le serveur SSH n'est pas installé.**

Voici la commande qui permet d’installer le package openssh-server.

**sudo apt-get install openssh-server**

Voici la commande qui permet d’activer le serveur SSH.

**sudo systemctl enable ssh**

**Voici des commandes supplémentaires à utiliser seulement en cas de besoin.**

Voici les commandes pour démarrer, arrêter ou redémarrer le service du serveur SSH.

**sudo systemctl start ssh**

**sudo systemctl stop ssh**

**sudo systemctl restart ssh**

**Voici des commandes supplémentaires à utiliser seulement en cas de besoin.**

Voici les commandes nécessaires pour supprimer le serveur SSH.

**sudo systemctl stop ssh**

**sudo systemctl disable ssh**

**sudo apt-get remove opnessh-server**

**Étape 2 - Vérification de la configuration du pare-feu dans "Ubuntu server"**

Voici la commande qui permet de vérifier l’état du pare-feu.

**sudo ufw status**

Voici la commande qui permet d’installer **ufw**.

**sudo apt-get install ufw**

Voici la commande qui permet d’activer le pare-feu.

**sudo ufw enable**

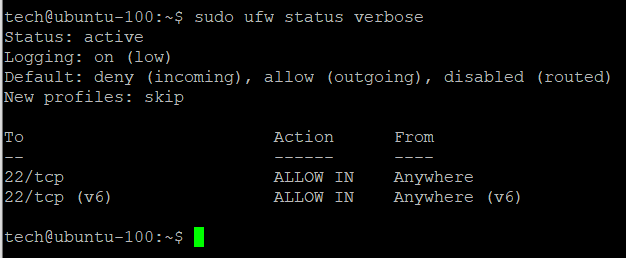
Voici la commande qui permet d’autoriser l'accès au serveur SSH.

**sudo ufw allow ssh**

**Voici des commandes supplémentaires qui permettent d'afficher des informations sur la configuration du pare-feu.**

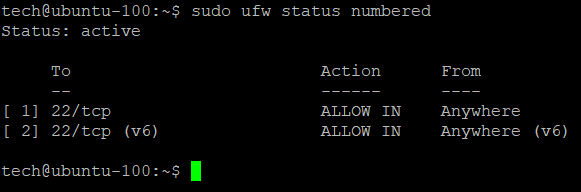
Voici la commande qui affiche les règles du pare-feu

**sudo ufw status verbose**



Voici la commande qui affiche les règles du pare-feu en numérotant les règles

**sudo ufw status numbered**

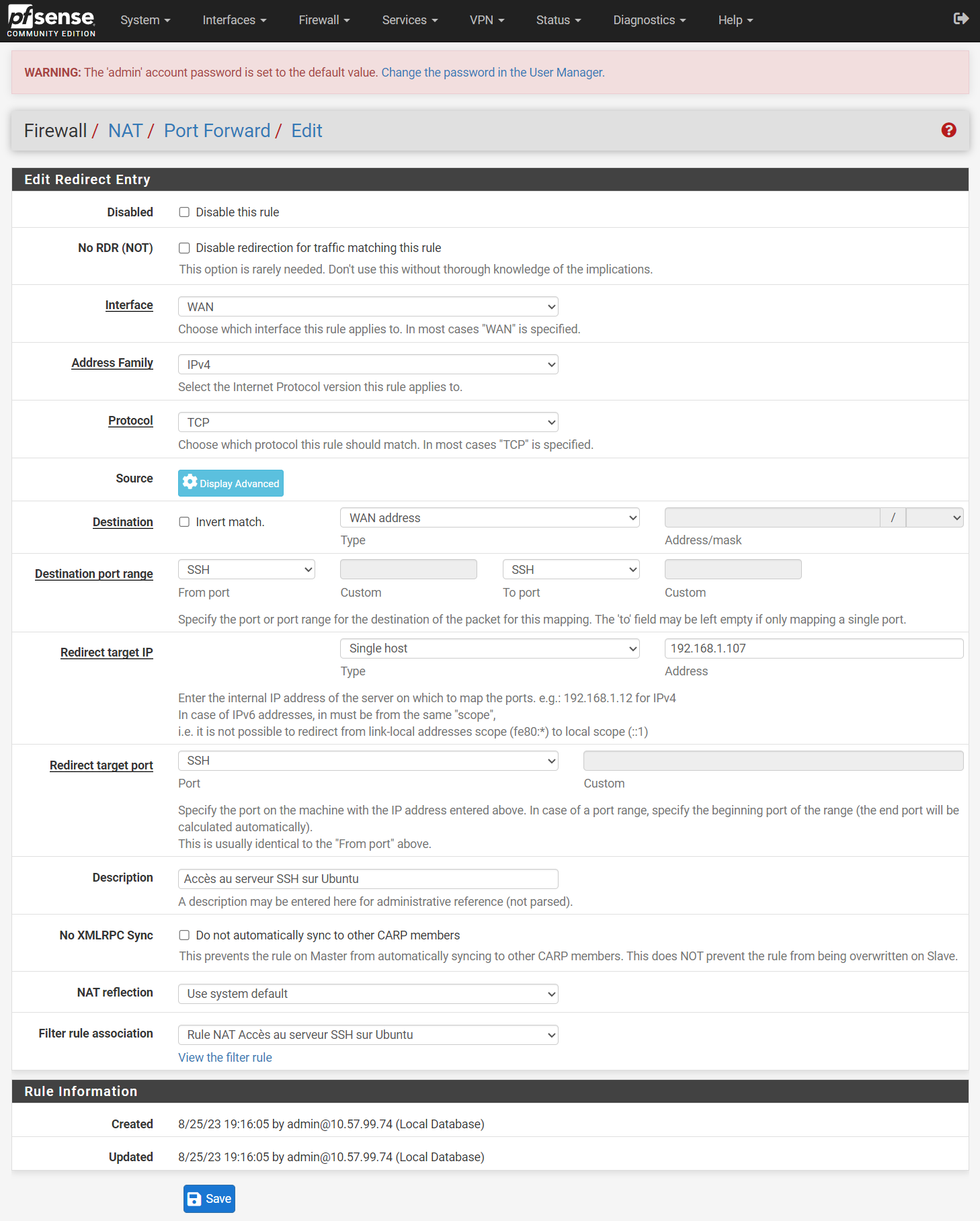


**Voici une commande supplémentaire à utiliser seulement en cas de besoin.**

Voici la commande qui supprime la règle qui autorise le port 22.

**sudo ufw delete allow ssh**

**Étape 3 - Création de la redirection de port dans le pare-feu de pfSense**



Destination WAN address

Destination port range From port = SSH To port = SSH

Redirect target IP Type = Single host Address = 192.168.1.**x**

* L’adresse IP correspond à l’adresse IP de "**Ubuntu server**".

Redirect target port Port = SSH

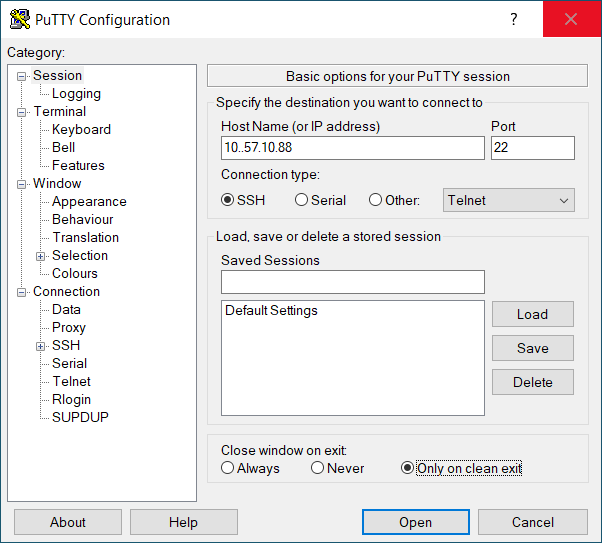
Description Accès au serveur SSH sur Ubuntu

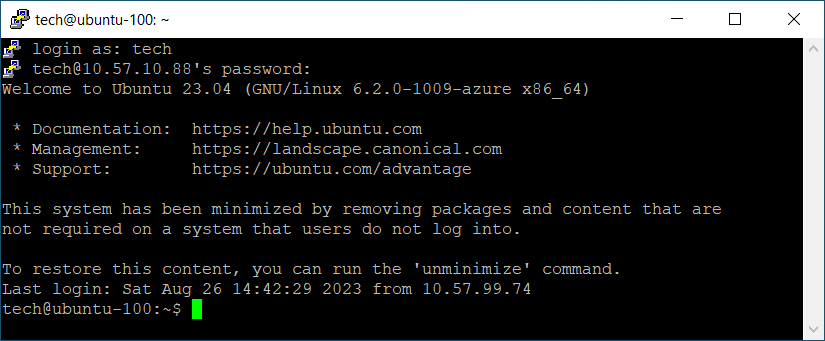
**Étape 4 - Installation et utilisation de puTTY**

Voici le lien pour télécharger directement putty.exe

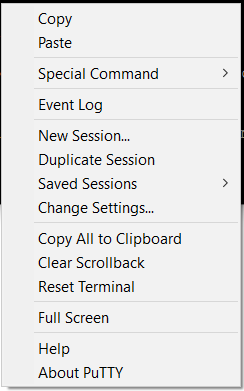
https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe

10.57.**x**.**y** est l’adresse IP du routeur "**pfSense**".

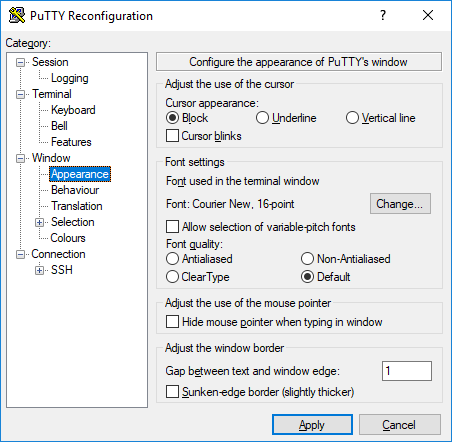




Appuyez sur la touche Ctrl à la droite du clavier et le bouton droit de la souris dans la fenêtre de puTTY.



L’option "**Change Settings…**"



"**Apperance**" permet de modifier le type de police et la taille de la police.