|B3| TP N° 2: PFsense

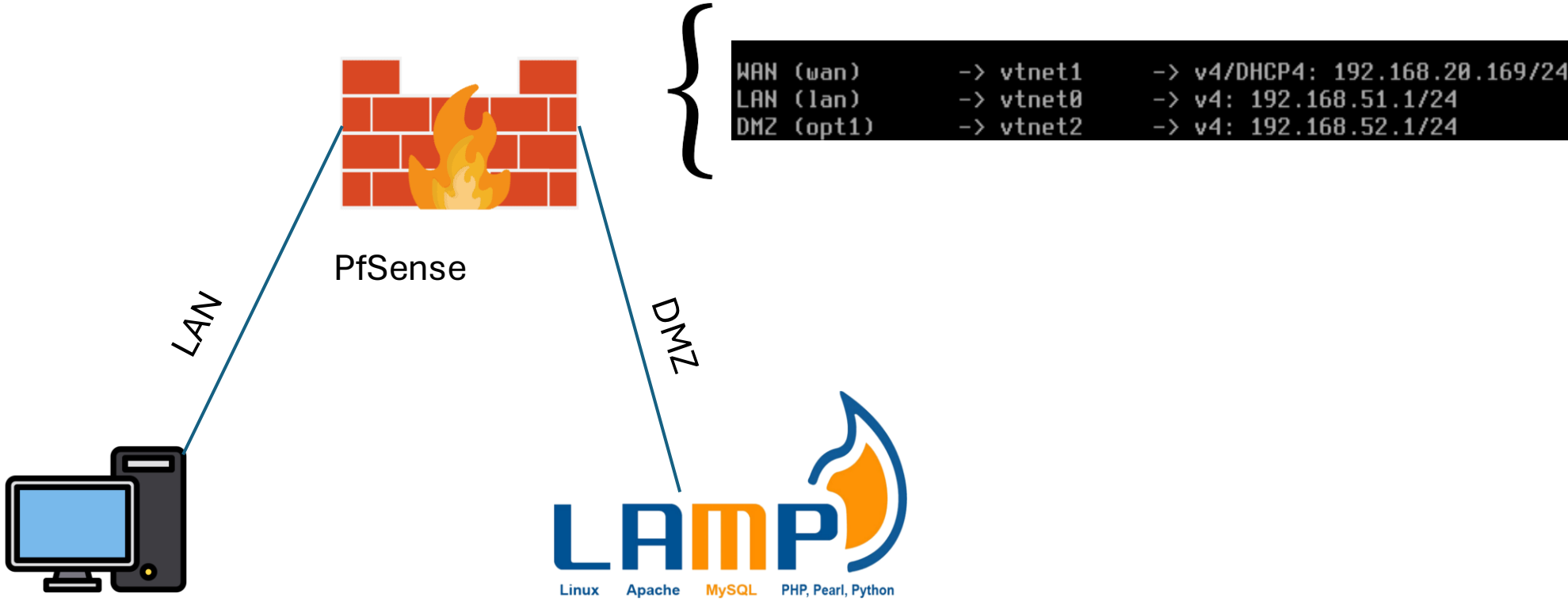
Belerge Jérémy BTS SIO 2

Mise en situation

La société Vikor désire installer un serveur Web au sein de son architecture réseau ,ce serveur doit être accessible depuis le LAN de l'entreprise ainsi que de « l'extérieur » ,à savoir internet.
Afin de sécuriser au maximum son réseau ,le choix de PfSense a été fait en raison de sa flexibilité et du nombre de fonctionnalités disponibles.

Sommaire

Schéma réseaux



Consignes:

-Le PFsense c'est quoi ?

Pfsense est un OS transformant n'importe quel ordinateur en routeur/pare-feu. Basé sur FreeBSD, connu pour sa fiabilité et surtout sa sécurité, Pfsense est un produit OpenSource adapté à tout type d'entreprise.
Voici ses principales fonctionnalités :

- Gestion complète par interface web
- Pare-feu stateful avec gestion du NAT, NAT-T
- Gestion de multiples WAN
- DHCP server et relay
- Failover (possibilité de monter un cluster de pfsense)
- Load balancing
- VPN Ipsec, OpenVPN, L2TP
- Portail captif

Source: www.it-connect.fr

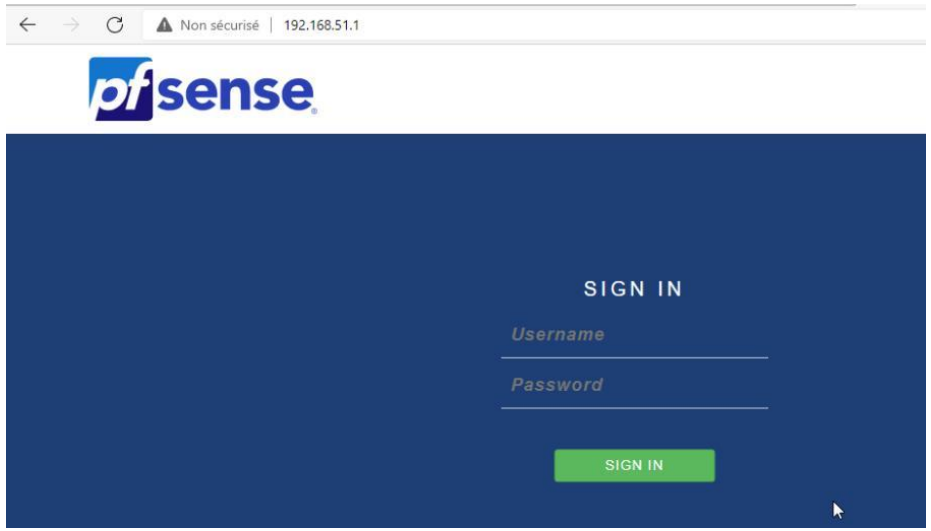
Pour résumer : pfSense est une solution logicielle libre qui transforme un matériel courant en un routeur/pare-feu professionnel et évolutif, idéale pour sécuriser, surveiller et contrôler l'ensemble des échanges d'un réseau informatique.

Consignes:

-Le PFsense comment on y accède ?

```
WAN (wan)       -> vtnet1     -> v4/DHCP4: 192.168.20.169/24
LAN (lan)       -> vtnet0     -> v4: 192.168.51.1/24
DMZ (opt1)      -> vtnet2     -> v4: 192.168.52.1/24
```

Voici la configuration du PFsense
Wan -> 192.168.20.169
LAN -> 192.168.51.1
DMZ -> 192.168.52.1



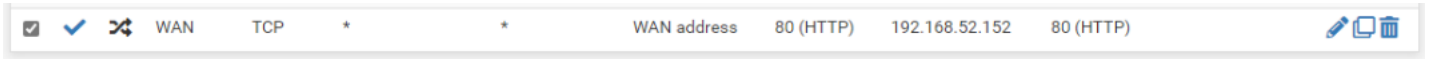
Depuis la machine dans la LAN , il nous faut rentrer l'ip entrer dans notre PFsense
(192.168.51.1)

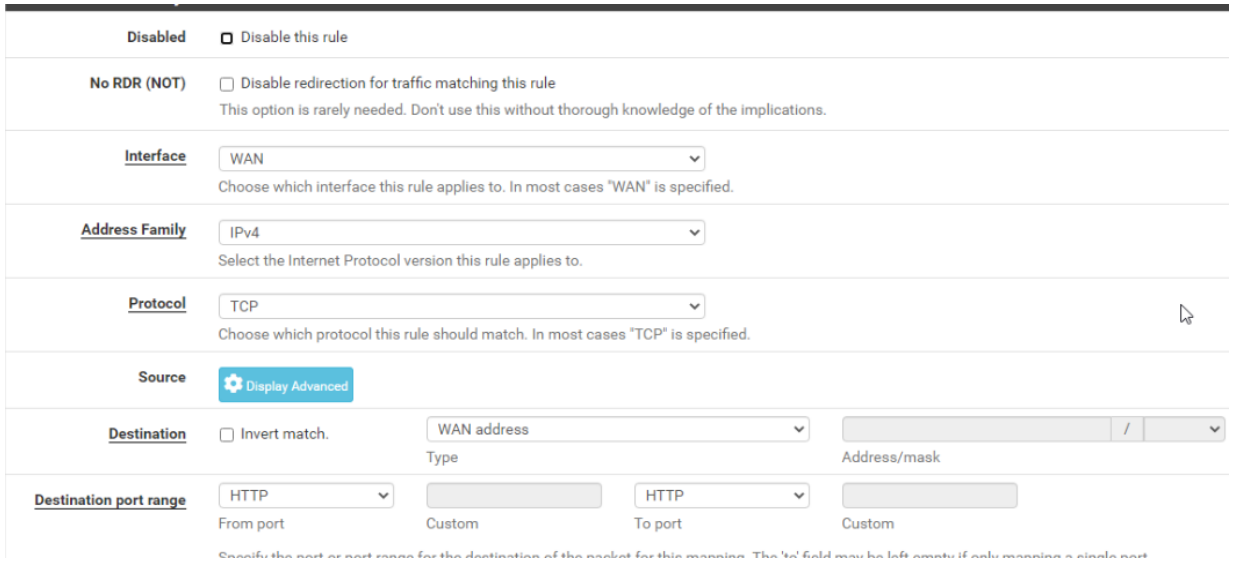
Utilisateur: admin
Password : pfsense

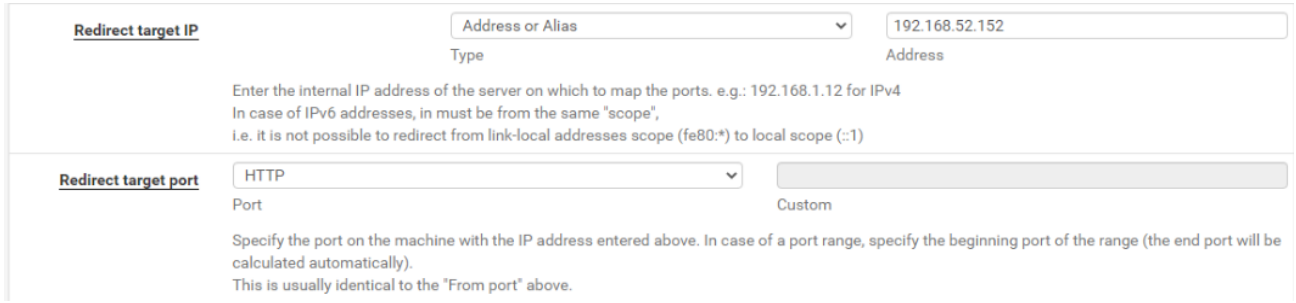
Consignes:

- WAN -> DMZ

Depuis Firewall -> NAT





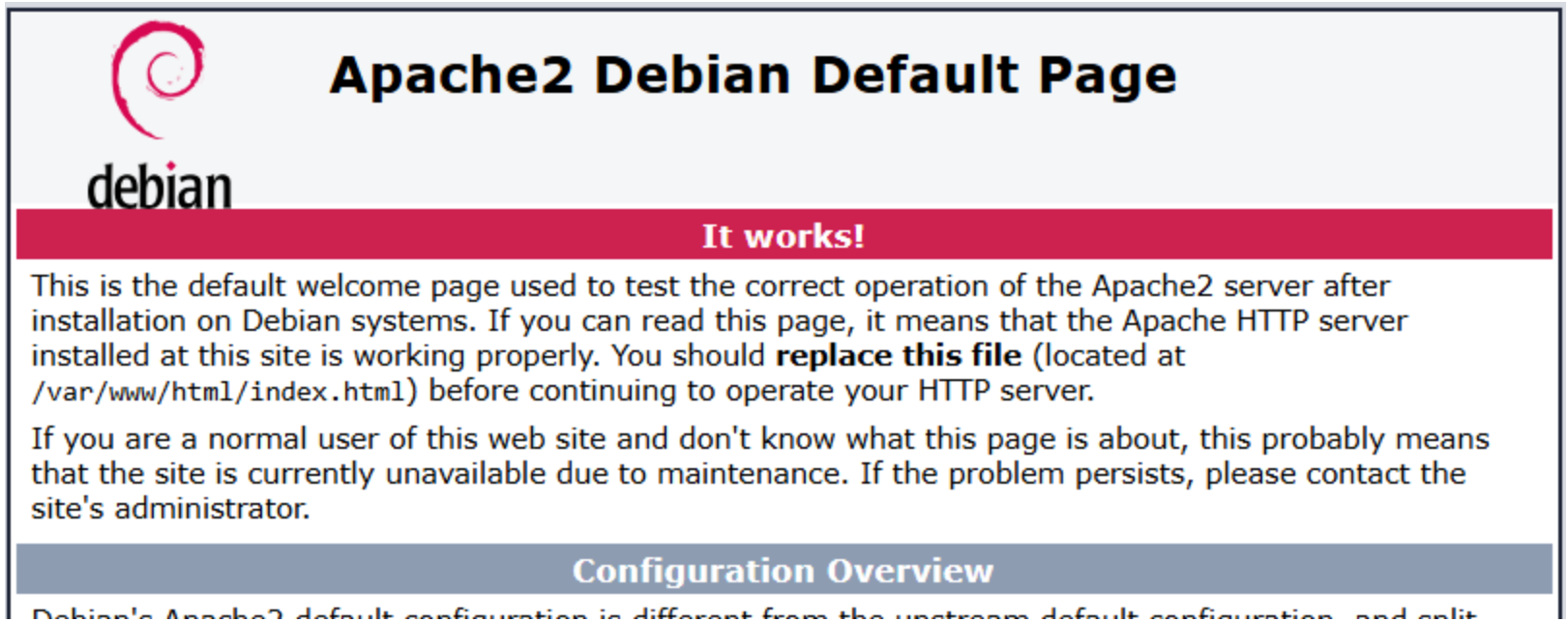


Cette règle va nous permettre d'avoir accès a notre page web depuis notre WAN. On rentre l'ip 192.168.52.152 (de notre LAMP) afin de pouvoir y acceder depuis notre WAN.

Consignes:

-Test

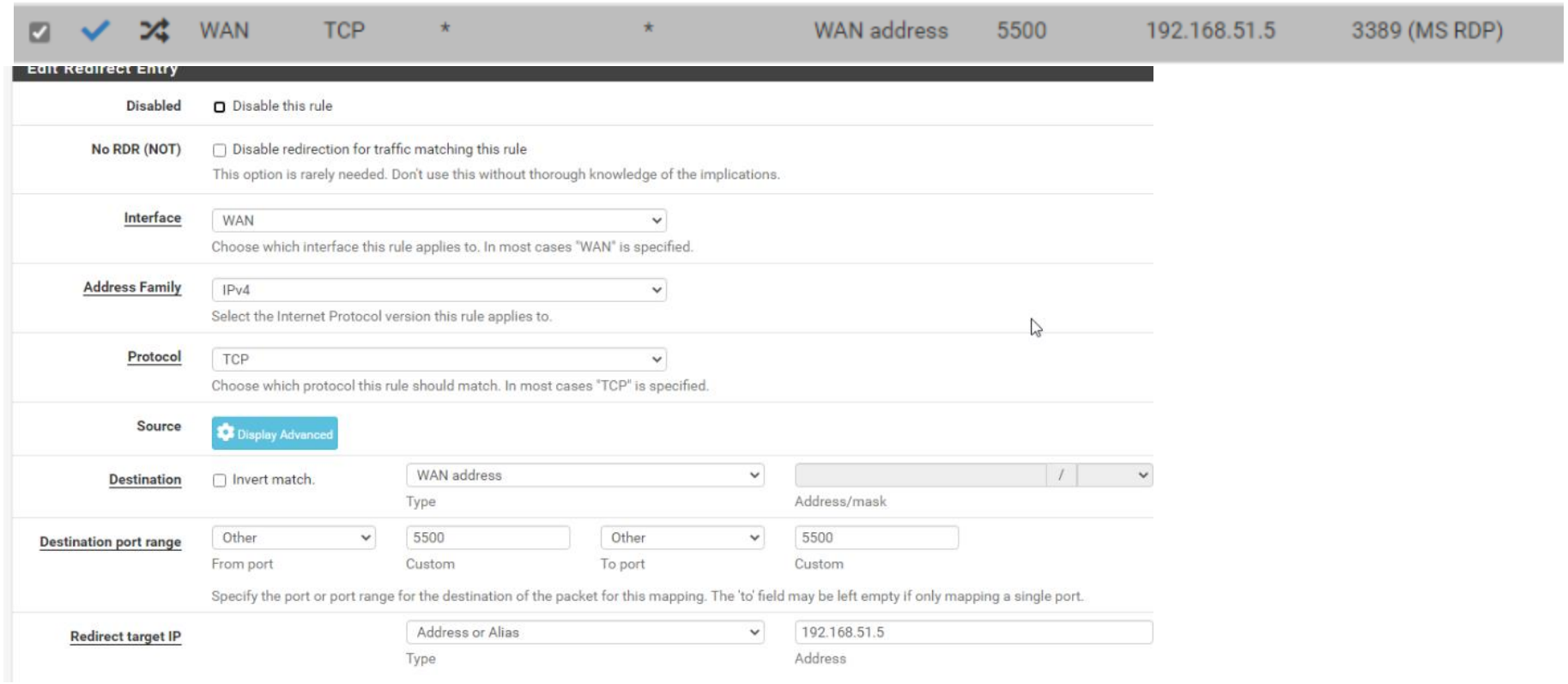
Résultat depuis notre WAN :



Consignes:

-RDP

Depuis Firewall -> NAT



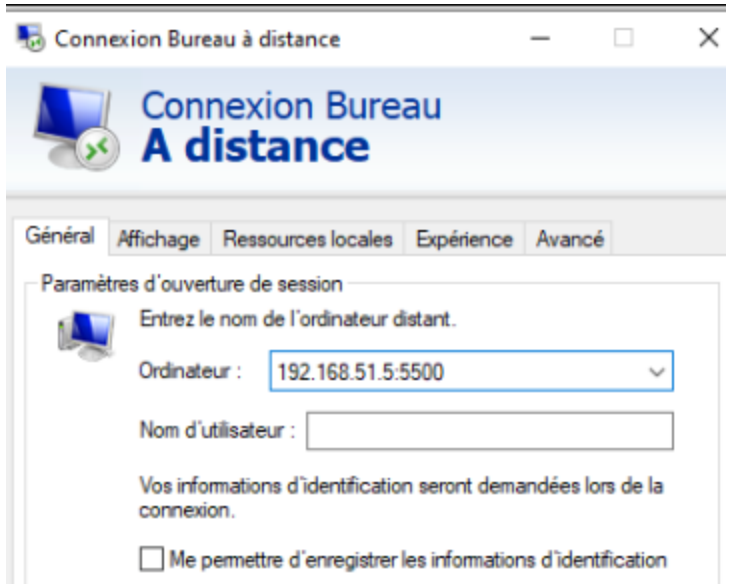
Cette regle va nous permettre de pouvoir autorisé le bureau a distance

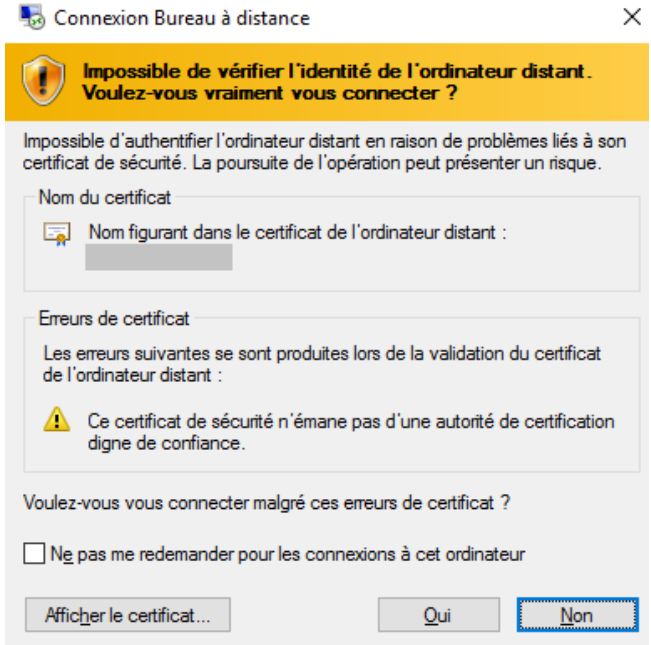
(Attention il ne faut pas oublier d'activé le bureau a distance sur vos machines windows)
Pour cela il faut suivre ce chemin : Parametre -> Système -> Bureau a distance

Consignes:

-Test

Afin de se connecter au Bureau a distance :





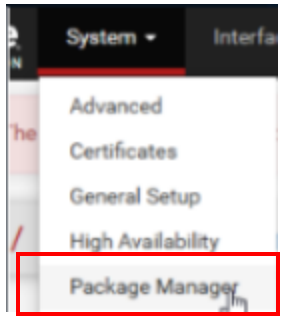
Sur la deuxième machine il faudra alors rentrer l'ip de notre machine cible , ainsi que le port qui est renseigné dans notre règle (ici 5500)

Si le message apparait c'est normal , c'est car le certificat n'est pas officiel

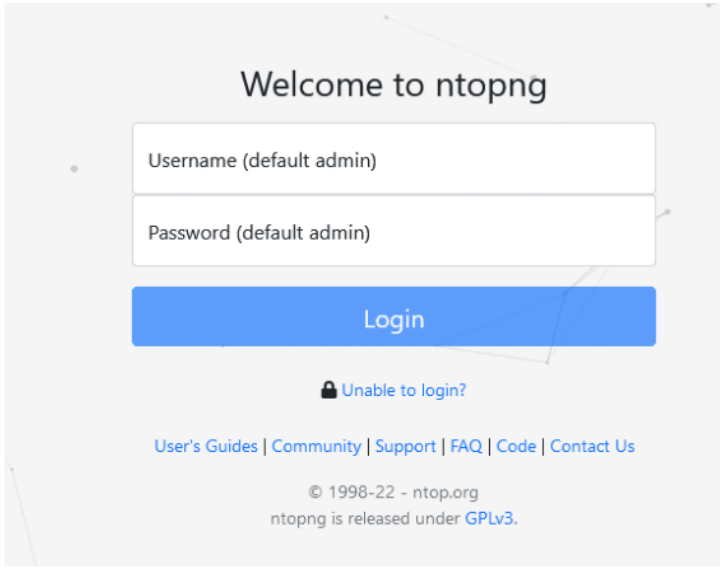
Consignes:

-Monitoring | NtopNG

Pour installer le package, connectez-vous à l'interface web, ouvrez l'onglet **System**, puis sélectionnez **Package Manager**. Recherchez le package **ntopng** et cliquez sur **Installer** pour démarrer l'installation



Une fois l'installation terminée, accédez à **Diagnostic → ntopng Settings** pour effectuer la configuration. Activez l'option **Enable ntopng** afin d'activer le service, puis enregistrez les modifications. Puis afin d'acceder a l'interface il faudra noter 192.168.51.1:3000



Consignes:

-Monitoring | NtopNG

L’outil permet une surveillance en temps réel du trafic réseau à travers différents modules. Le **tableau de bord** fournit une vue globale du débit, du volume de paquets échangés et des protocoles utilisés. La section **Hosts** répertorie les appareils connectés ainsi que leur consommation de bande passante, tandis que **Flows** présente les connexions actives entre ces hôtes. Enfin, l’analyse du trafic propose des **graphiques** détaillant l’utilisation des protocoles et l’évolution du trafic au fil du temps.