



N° Réf:.....

RAPPORT D'AVANCEMENT DE PROJET DE FIN D'ETUDE

Sujet

**Mise en place d'une solution sécurisée
pour le réseau TGR**

Réalisé par :

AJJA OUSSAMA

Trésorerie Générale de Royaume Rabat



Encadré par :

M. Said MOKHTARI (TGR Rabat)

Mme. Hind MESTOURI (ENSA Safi)

5^{ème} Année Génie Réseaux et Télécoms

Année Universitaire : 2018- 201

Introduction

La sécurité des systèmes d'information représente aujourd'hui une tâche de fond à prendre en compte par toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent et assurent la gouvernance de son système d'information. Les principales solutions de sécurité s'intègrent dans l'activité quotidienne informatique et permettent de surveiller, analyser, piloter en agissant directement après avoir reçu des alertes informant de potentielles anomalies. Ces alertes peuvent être remontées via des scripts, des mails, des fax, des appels vocaux ou bien par l'envoi de simple SMS d'alerte.

Pfsense est un pare-feu permet de surveiller une grande infrastructure contiennent de différents équipements de réseaux. Tout l'existant informatique et téléphonique de l'entreprise peut être concerné, le courant électrique, les disponibilités réseaux fibres, les serveurs, les imprimantes et autres éléments actifs constituant le réseau (hubs, switches, routeurs, etc.).

Pour gérer les failles du réseau, en suivant plusieurs étapes sous PFSense pour une meilleure sécurité des routeurs, cela sera bien citer dans le rapport.

1- Architecture proposée

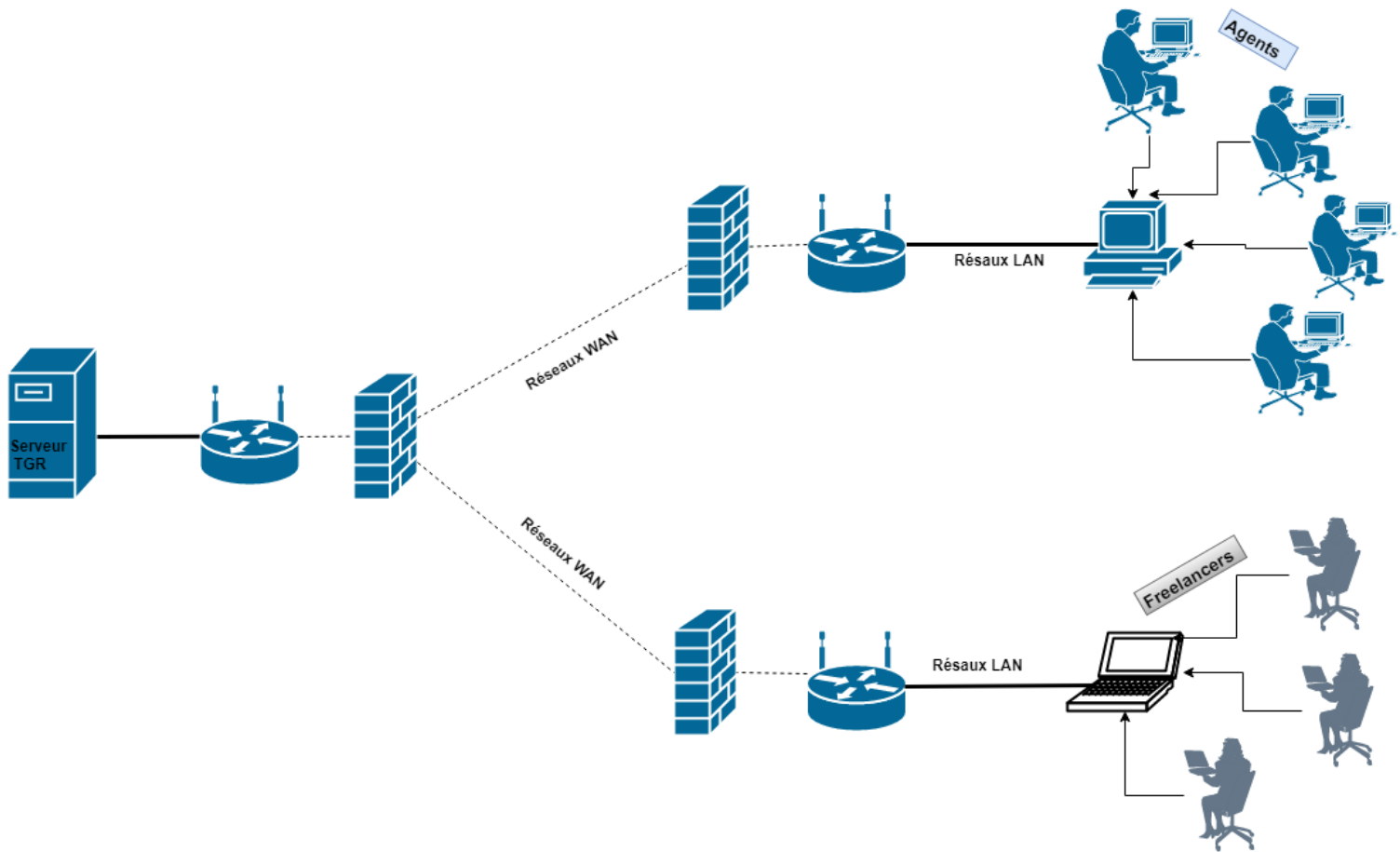


Figure 1: Architecture réseaux

Ce rapport est consacré à l'implémentation et au test de la solution pour la nouvelle architecture réseaux répondant aux exigences de sécurité de l'entreprise et pour évaluer cette architecture :

L'installation doit être faite dans un environnement virtuelle afin d'assurer la portabilité et l'indépendance de la plateforme physique.

- L'environnement virtuel qui a été choisi est la solution Oracle VM VirtualBox.

Solution proposé

La solution se compose de 3 **Pfsense** :

- **Pfsense Server** liée aux serveurs de Tgr
- **Pfsense 1** liée au département des agents
- **Pfsense 2** liée au département des Freelancer

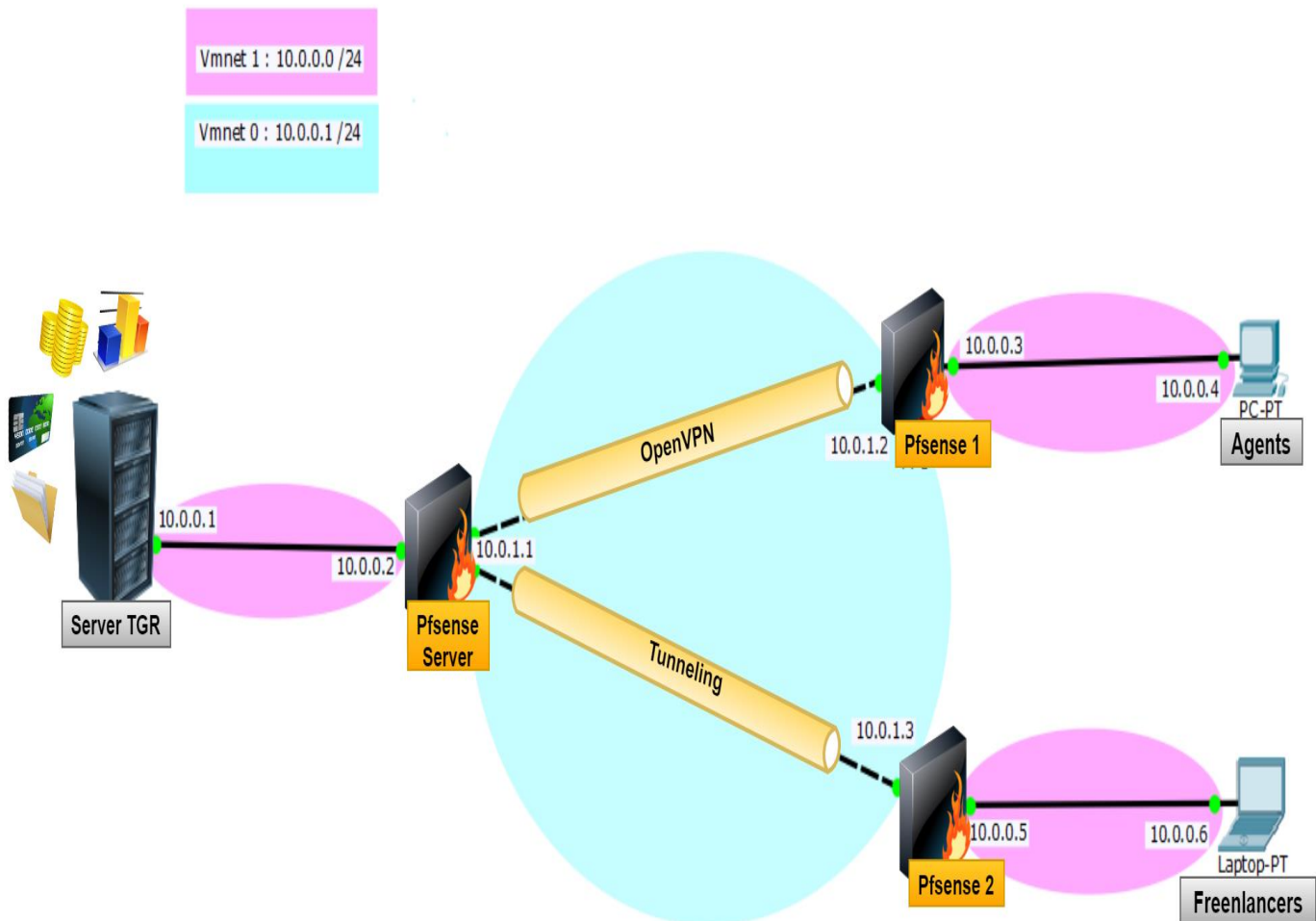


Figure 2: Solution d'architecture sécurisé

Environnement de travail

1- Architecture sous VMware

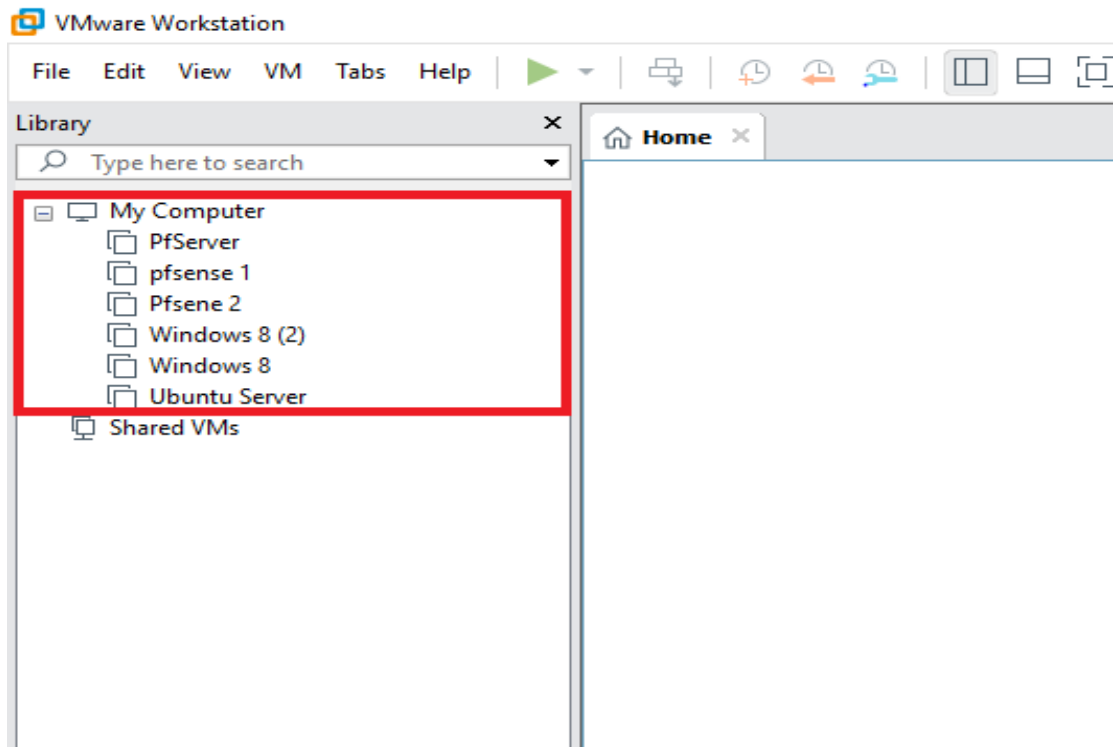


Figure 3: Architecture sous VMware

2 -VMnet

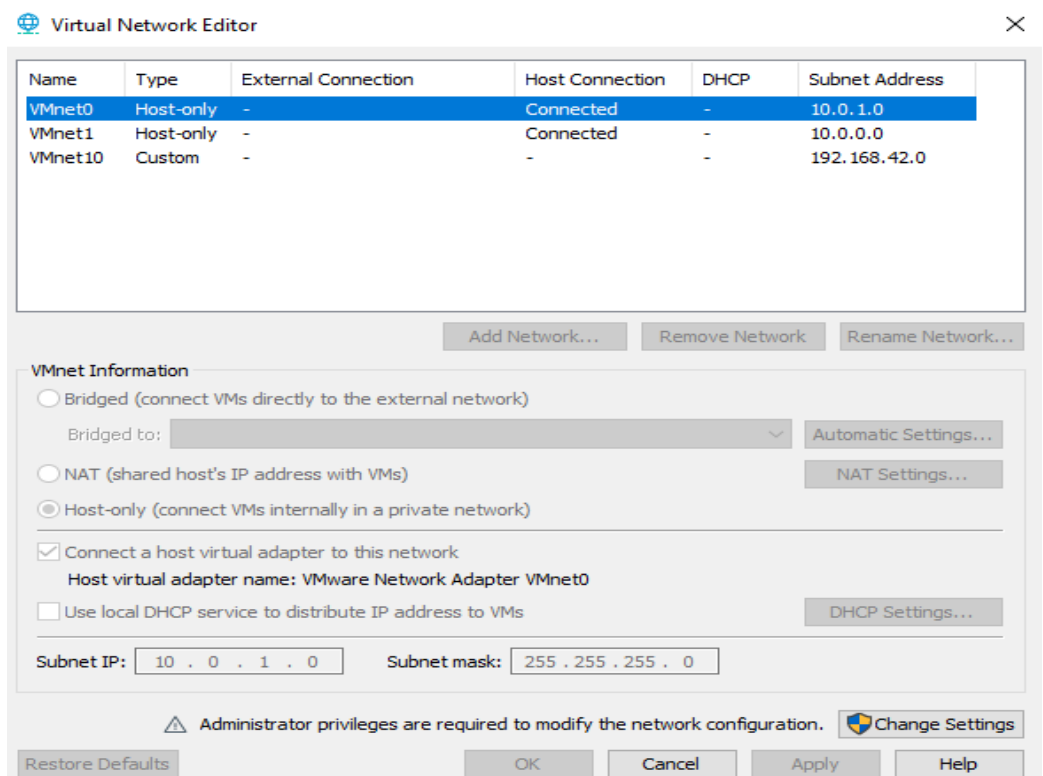


Figure 4: VMnet

Installation et configuration de Pfsense

1 Prérequis

L'installation est réalisée sur une machine virtuelle depuis VirtualBox, la procédure d'installation est la même si vous êtes sur une machine physique.

En termes de configuration requise, nous faisons tourner Pfsense sur une machine virtuelle disposant d'un processeur, 512 Mo de RAM et 8Go de disque, ce qui est amplement suffisant pour Pfsense.

L'architecture se compose d'un serveur ou ordinateur disposant d'au moins deux cartes réseaux, une pour l'interface LAN (du côté du réseau local) et l'autre pour l'interface WAN (du côté du réseau relié à internet),

Le clavier français est en azerty, vous aurez donc besoin de connaître l'emplacement des touches du clavier anglais (qwerty) car lors de l'installation et la configuration via la ligne de commande le clavier est en qwerty. Et malheureusement même en modifiant les options lors de l'installation le clavier azerty n'est pas pris en compte.

2 Installation et configuration des interfaces de chaque Pfsense



Figure 5: Pfsense

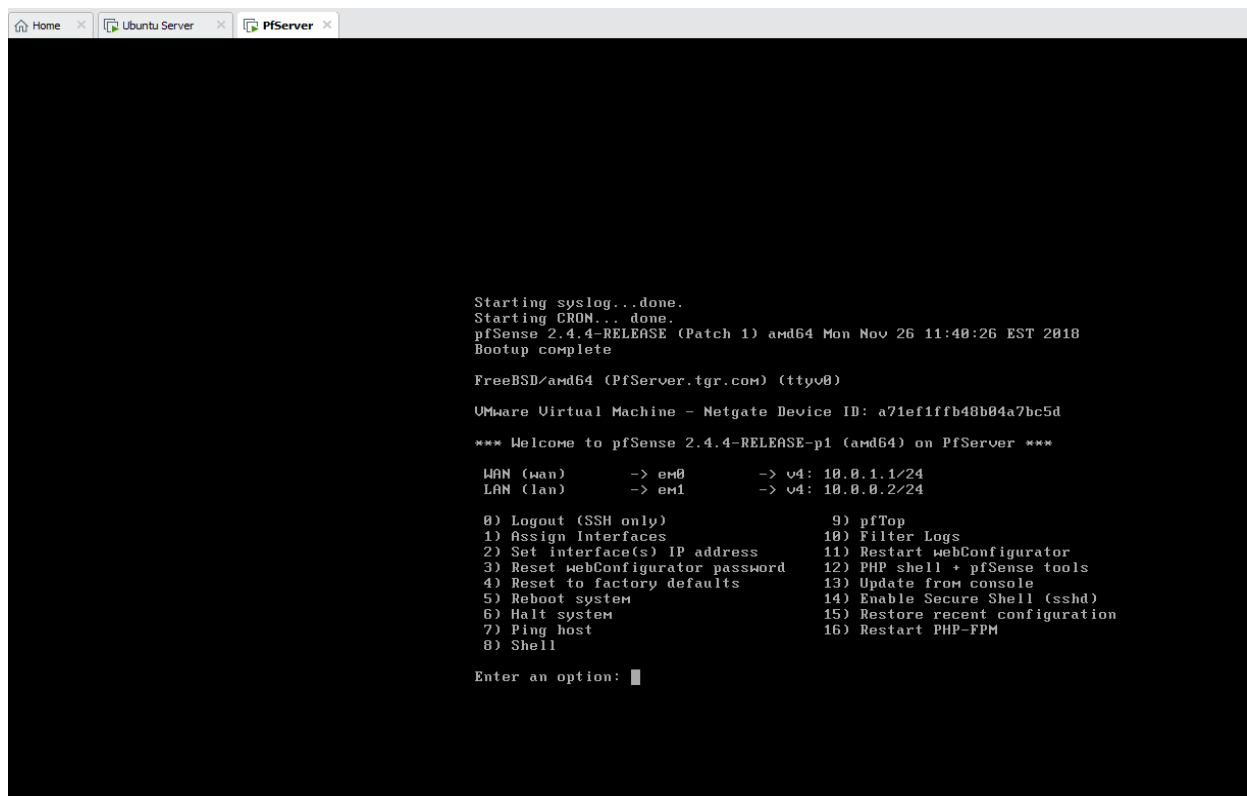


Figure 6: PfSense Server

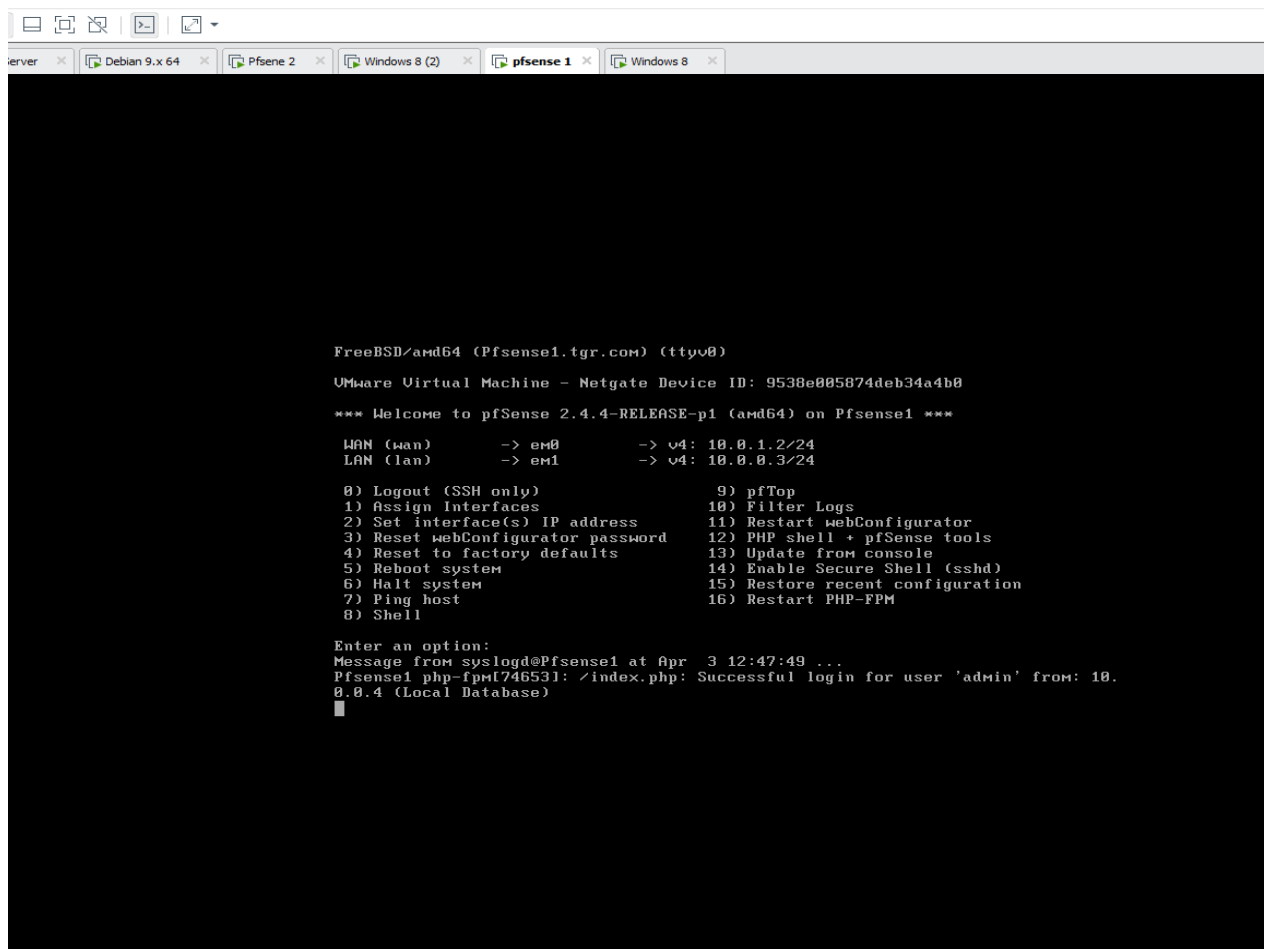


Figure 7: PfSense 1

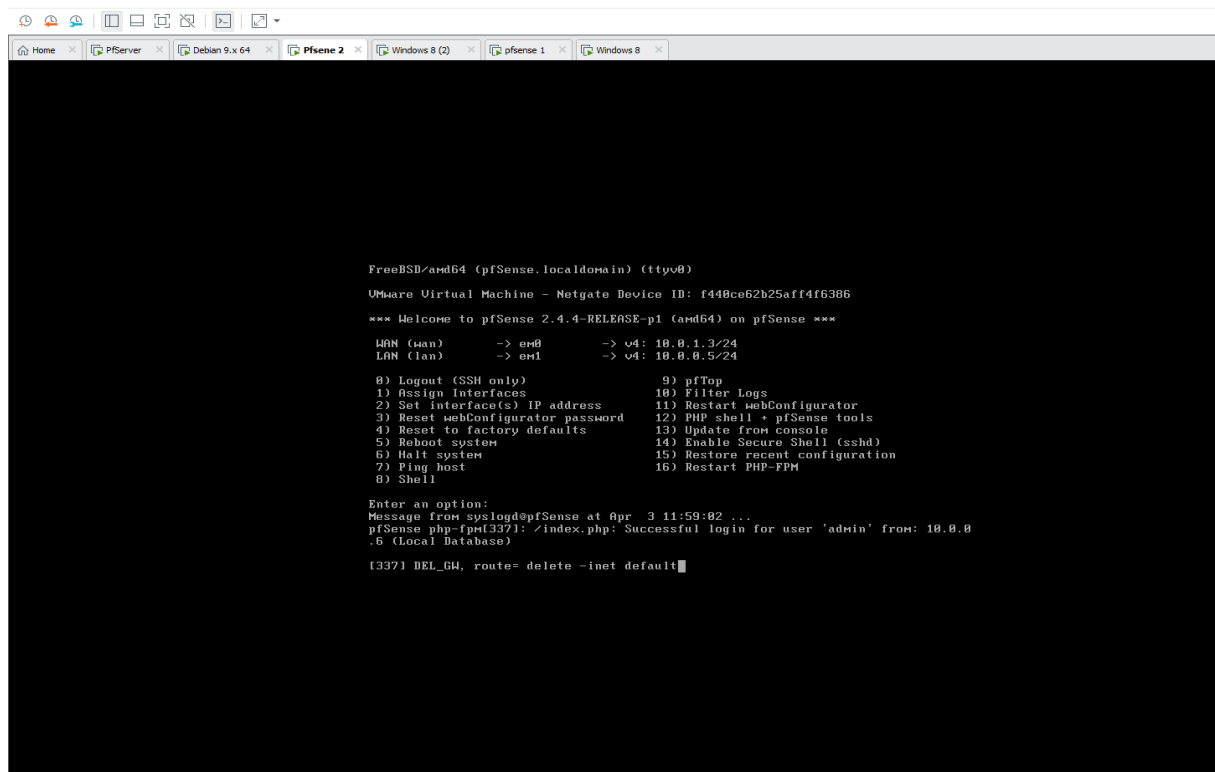


Figure 8: Pfsense 2

✚ Notre interface LAN & WAN sont maintenant configurées, alors nous pouvons accéder à l'interface Web de chaque **Pfsense** à partir de la machine qui se trouvant sur le réseau natif LAN du *pfSense*, par exemple l'interface web de Pfserver 10.0.0.2/24 on va l'accéder à partir Ubuntu (Server TGR) ayant l'adresse IP 10.0.0.1/24.

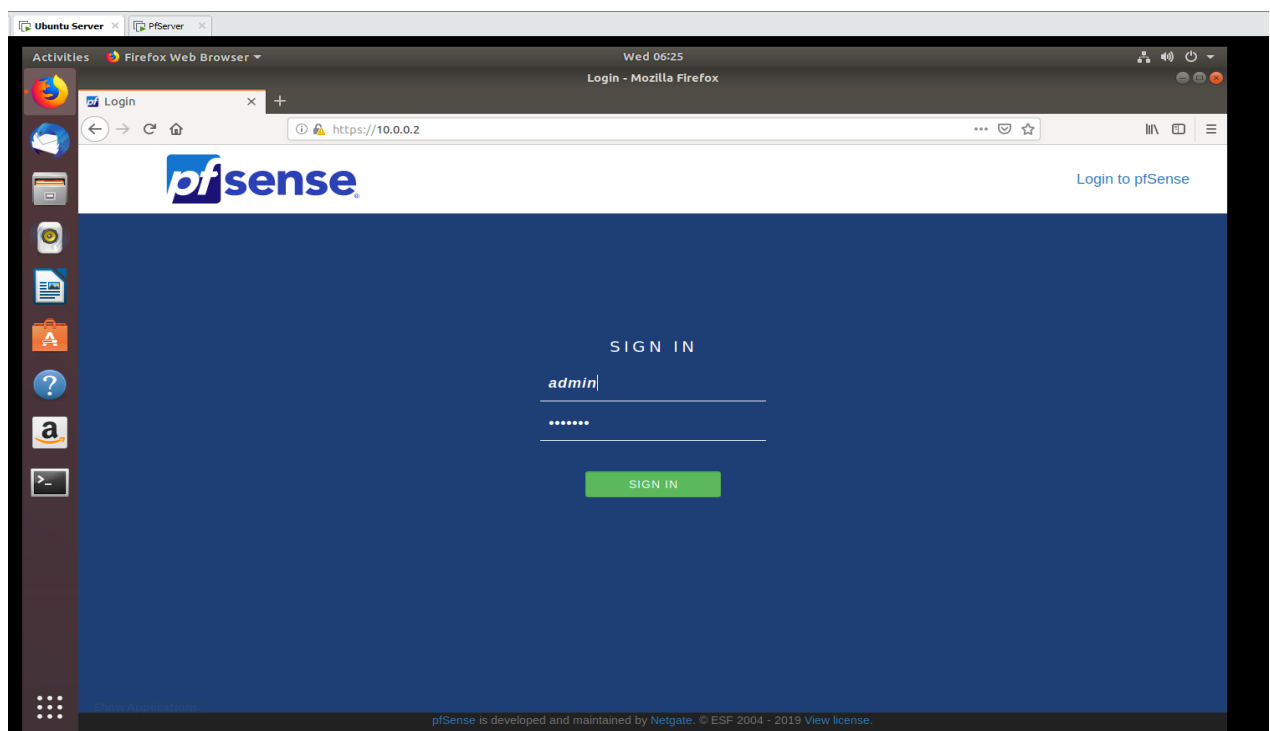


Figure 9: Login interface web

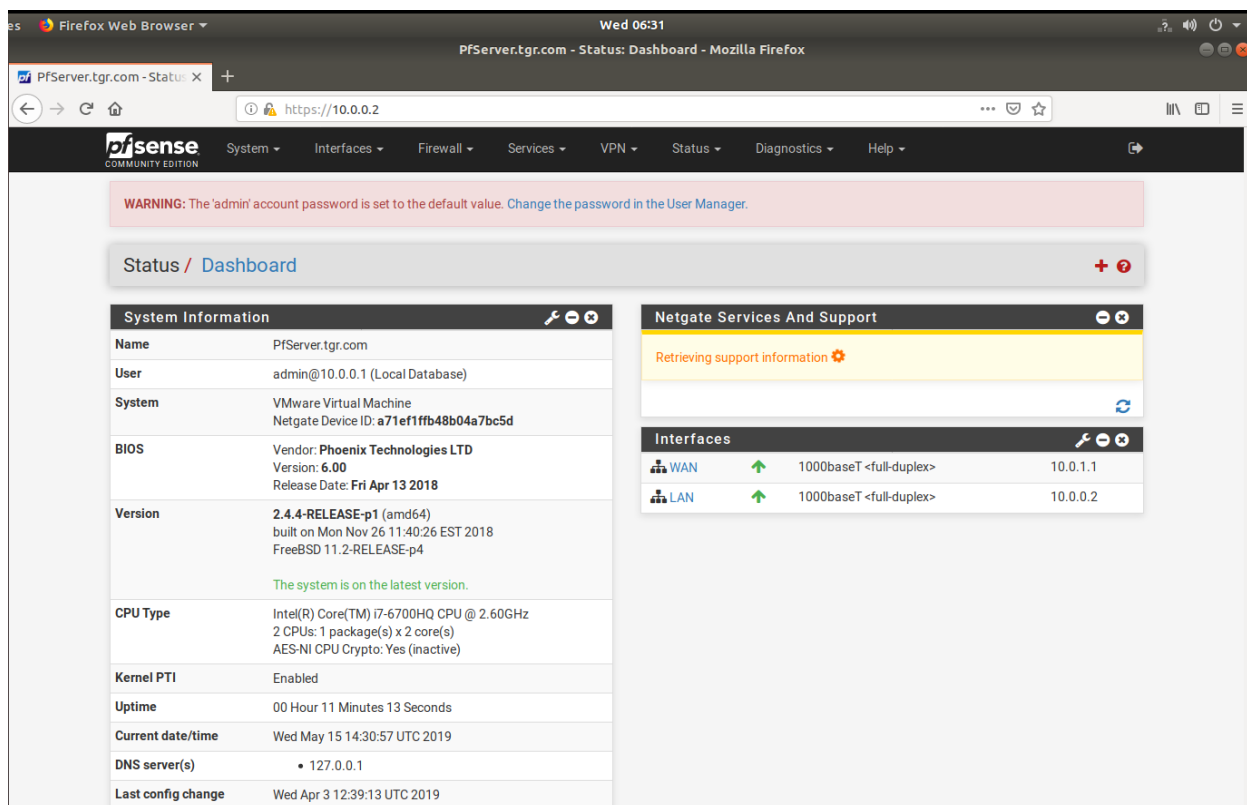


Figure 10: interface web

3- Configuration VPN site-to-site entre Server et client :

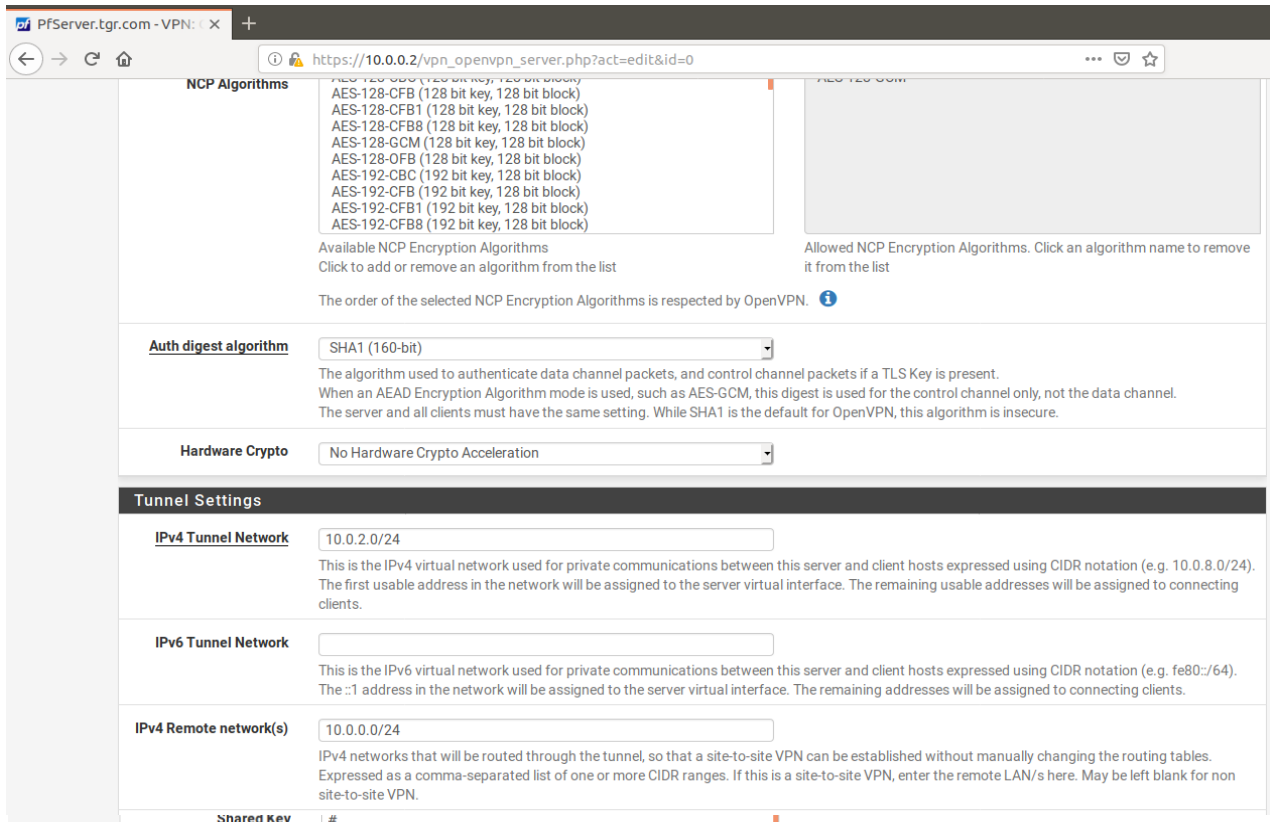


Figure 11: Configuration de Tunnel OpenVpn pour Les Agents

🚦 Même méthode pour La configuration de 2éme Tunnel pour Les Freelancers, après on va passer à la configuration des Rôles de pare-feu pour activer les statuts des Tunnels

The screenshot displays the pfSense Firewall Rules configuration interface. The top section is titled 'Edit Firewall Rule' and contains the following fields:

- Action:** Pass (Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.)
- Disabled:** ☐ Disable this rule (Set this option to disable this rule without removing it from the list.)
- Interface:** WAN (Choose the interface from which packets must come to match this rule.)
- Address Family:** IPv4 (Select the Internet Protocol version this rule applies to.)
- Protocol:** UDP (Choose which IP protocol this rule should match.)

The **Source** section includes:

- Source:** ☐ Invert match. any (Source Address)
- Display Advanced:** The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

The **Destination** section includes:

- Destination:** ☐ Invert match. This firewall (self) (Destination Address)
- Destination Port Range:** OpenVPN (1194) (OpenVPN (1194))

The bottom section shows the 'Rules (Drag to Change Order)' table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 UDP	*	This Firewall	1194 (OpenVPN)	*	none			Anchor Edit Delete
<input type="checkbox"/>	0/0 B	IPv4 UDP	*	This Firewall	1195	*	none			Anchor Edit Delete

At the bottom of the table, there are buttons for 'Add', 'Add', 'Delete', 'Save', and 'Separator'.

Figure 12: Rules Firewall

Status OpenVPN :

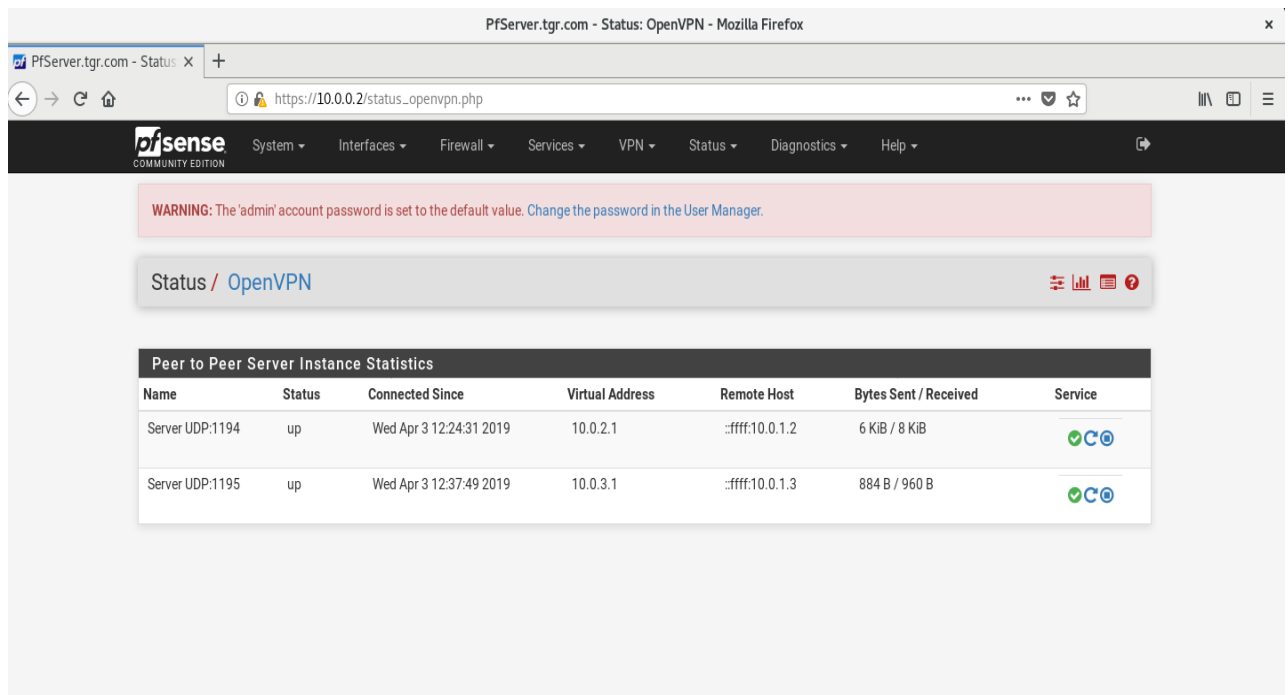


Figure 13: Status OpenVPN