

COMPTE RENDUE E5

AYOUB BELBACHIR



SOMMAIRE

COMPTE RENDUE E5	0
SOMMAIRE	1
Introduction	2
Tutoriel	4
Mise en place du firewall Pfsense :	4
Mise en place de l'Active Directory depuis le script menu PowerShell :	4
Mise en place du client RADIUS :	8
Configuration du point d'accès wifi TP Link :	10
Configuration de la 3 ^{ème} carte réseau de notre firewall Pfsense :	11
Déploiement du Portail captif :	12
Zabbix	14
Installation de notre Ubuntu server 20.04.....	14
Redirection Pfsense SSH.....	15
Installation de Zabbix	16





Introduction :

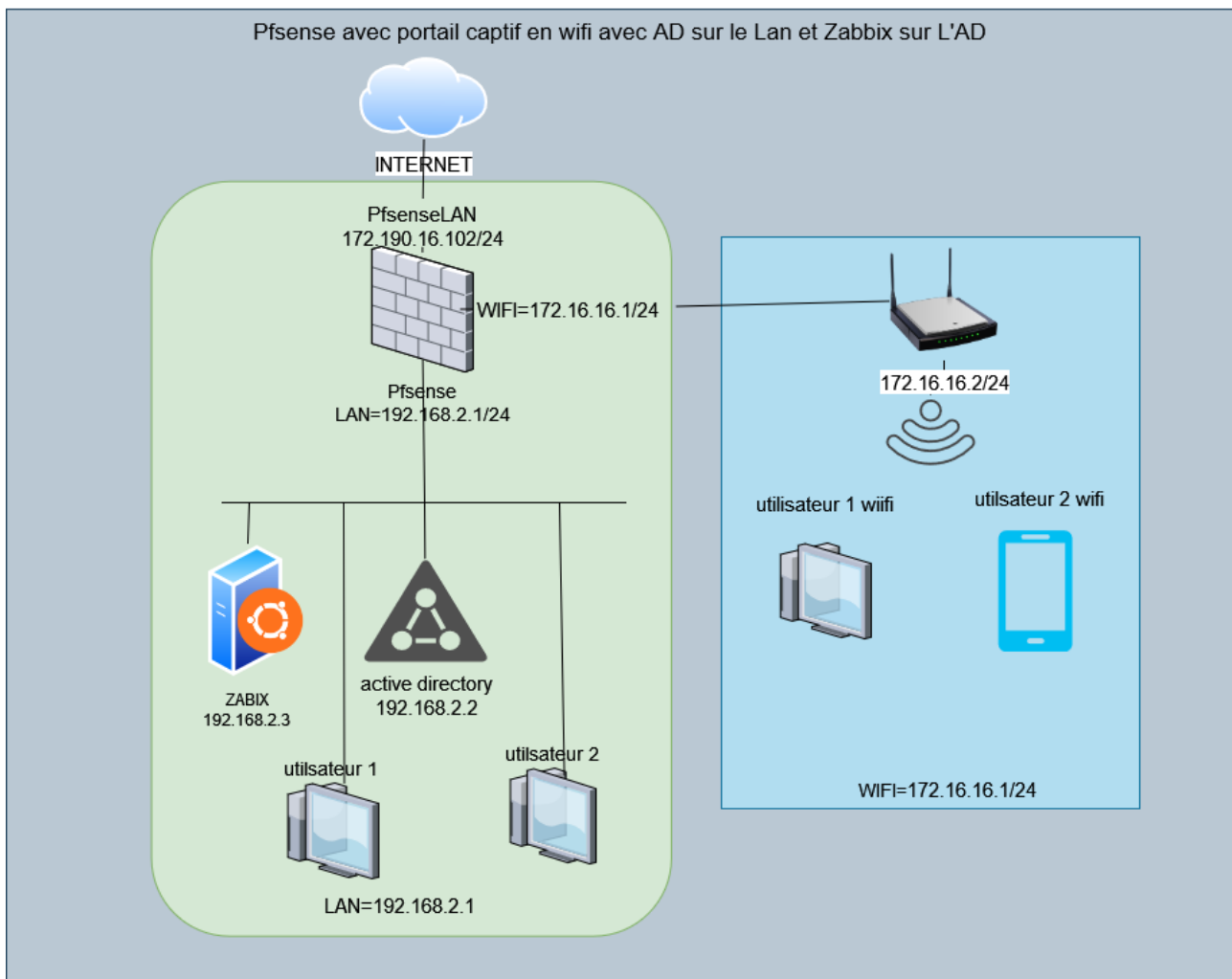
La Maison de Lignes de Lorraine (M2L) Cherche à diversifier et élargir ses domaines de compétences, elle ouvre alors un nouveau site qui se spécialisera par la suite sur la recherche en physique quantique

Besoin :

La direction voudrait que certains employés appartenant à ce site puisse accéder de manière sécurisée à une WIFI qui leur permettrait d'aller sur Internet mais aussi accéder à des fichiers concernant l'association stockés sur le réseau local. Elle voudrait aussi pouvoir monitorer leurs Nouvelles Active Directory

Schémas explicatifs :

M2L





Prérequis :

Script PowerShell permettant d'automatiser plusieurs paramètres comme ; attribuer une adresse IP statique, attribué un Hostname, créé un AD et une forêt, installer un DNS, création de OUs ; création d'utilisateur à partir d'un fichier .CSV qui doivent être déplacé dans les OUs selon leurs ID présent dans le .CSV disponible sur [mon GitHub](#)

1 Firewall Pfsense :

- + 1 GHz processeur ou plus
- + 3 cartes réseau
- + 15 Go d'espace libre sur le disque dur ou plus
- + 1 Go de mémoire RAM

1 Ubuntu Server 20.04 LTS (Zabbix) :

- + 1 GHz processeur ou plus
- + 10 Go d'espace libre sur le disque dur
- 1.5 Go de mémoire RAM

1 Windows server (Active directory)

- + Une RAM de 2 Go ou plus
- + Un espace disque disponible de 40 Go
- + 1,5 gigahertz (GHz) ou plus rapide
- + Domain=Ayoub.local
- + NetBIOS=Ayoub

1 Ubuntu Server 20.04 LTS (Zabbix) :

- + 1 GHz processeur ou plus
- + 10 Go d'espace libre sur le disque dur
- 1.5 Go de mémoire RAM





Ayoub Belbachir

Tutoriel :

Mise en place du firewall Pfsense :

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD

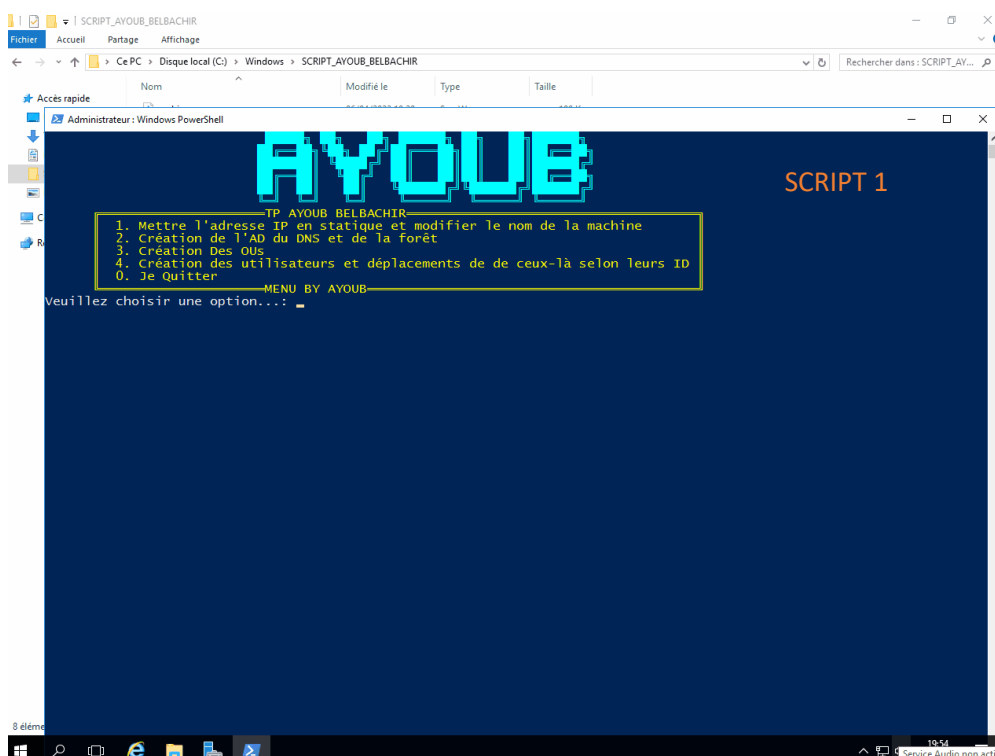
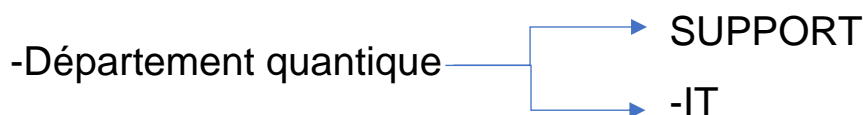
Nous allons assigner les interfaces réseau à notre Pfsense pour ce faire entrer l'option "1". Paramétrage de la vlan laisser par défaut taper "n" assigner ensuite les interface selon leurs noms pour nous : WAN=em0, LAN=em1 et OPT1(wifi)=em2 ensuite taper "y" Pfsense va démarrer différents services dans le pare-feu un DNS et un service DHCP

Paramétrage de l'adresse IP du LAN entrer l'option "2" puis l'option "2", Entrer l'adresse IP suivante 192.168.2.1 entrer ensuite le sous réseau qui lui correspond le CIDR (24) appuyer ensuite 2 fois sur entrer pour passer les étapes activer le DHCP, définir la plage d'adressage IP du DHCP (192.168.2.4 à 192.168.2.254), activer ensuite le protocole de configuration web.

Paramétrage de l'adresse IP de l'interface OPT1 entrer l'option "2" puis l'option "3", Entrer l'adresse IP suivante 172.16.16.1 entrer ensuite le sous réseau qui lui correspond le CIDR (24) appuyer ensuite 2 fois sur entrer pour passer les étapes activer le DHCP, définir la plage d'adressage IP du DHCP (172.16.16.2 à 172.16.16.254), activer ensuite le protocole de configuration web.

Mise en place de l'Active Directory depuis le script menu PowerShell :

Arborescence des OUs ;





Ayoub Belbachir

Le Script 1 permet :

- D'attribuer une adresse IP en statique au serveur
- De demander à l'utilisateur de saisir un hostname pour le serveur si non le hostname par défaut sera sélectionné pour renommer le serveur
- Le script vérifie si le hostname saisi est déjà le nom du serveur si c'est le cas l'ordinateur ne redémarrera pas car ce serait inutile

Le Script 2 permet :

- Installer l'active directory
- Installer le serveur NPS (RADIUS) pour notre futur portail captif
- Installer le module BurntToast qui permet d'afficher une notification à la fin de l'exécution des scripts 2, 3 et 4.
- Installation du gestionnaire de paquet CHOCO nécessaire pour l'installation de BurntToast
- Créer une forêt pour L'Active Directory

Le Script 3 permet :

- De vérifier si les OUs de l'Arborescence existent
- De vérifier si le groupe en relation avec notre portail captif existe
- De créer le groupe en relation avec notre portail
- De créer s'ils n'existent pas

Le Script 4 permet :

- De créer des utilisateurs depuis un fichier csv s'il n'existe pas
- D'attribuer des mots de passe à ces derniers
- De trier l'emplacement des utilisateurs selon leurs ID
- De leur permettre aux utilisateurs d'accéder au wifi selon leur ID
- D'assigner le groupe "portail captif" aux utilisateurs ayant droits

Le Script Menu permet :

- De sélectionner les scripts à exécuter dans l'ordre
- De jouer un son lors du lancement d'un script pour améliorer l'immersion de l'utilisateur
- De faire gagner du temps pour permettre d'automatiser les déploiements des paramètres

Script et information complémentaire disponible sur [mon GitHub](#)



Ayoub Belbachir

Exécution script 2 :

```
TP AYOUB BELBACHIR
1. Mettre l'adresse IP en statique et modifier le nom de la machine
2. Création de l'AD du DNS et de la forêt
3. Création des OUs
4. Création des utilisateurs et déplacements de de ceux-là selon leurs ID
0. Je Quitter
MENU BY AYOUB
Veuillez choisir une option...: 
```

Exécution script 2 :

```
TP AYOUB BELBACHIR
1. Mettre l'adresse IP en statique et modifier le nom de la machine
2. Création de l'AD du DNS et de la forêt
3. Création des OUs
4. Création des utilisateurs et déplacements de de ceux-là selon leurs ID
0. Je Quitter
MENU BY AYOUB
Veuillez choisir une option...: 
```



Ayoub Belbachir

Exécution script 3 :

Exécution script 4 :



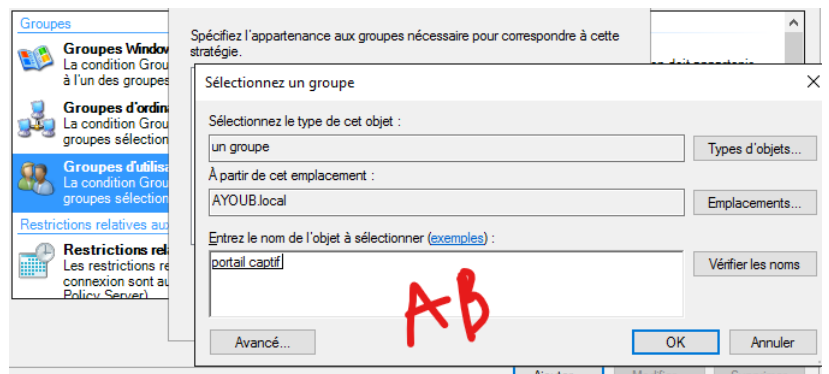
Ayoub Belbachir

Mise en place du client RADIUS :

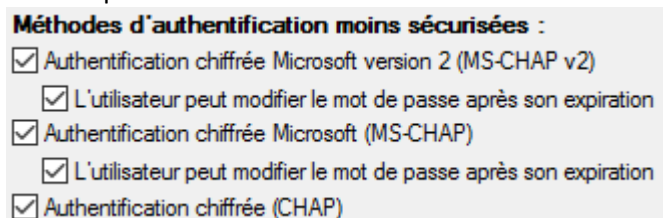
Le script 2 a déjà installé le serveur NPS il nous suffit donc de configurer le client Radius pour notre future portail captif et le script 3 s'est déjà chargé de créer le groupe que nous allons lier à notre client Radius.

Ouvrir le gestionnaire de serveur et aller dans le menu Outil > Serveur NPS (Network Policy Server), Effectuer un clic-droit sur NPS (Local)

- Cliquez sur Inscrire un serveur dans Active Directory
- Allez dans Client et serveurs RADIUS (sous NPS (Local))
- Effectuer un clic-droit sur Client RADIUS > Nouveau Nom convivial : po
- Adresse IP : 192.168.2.1 (IP de la Passerelle de notre active directory)
- Ajouter un secret partagé à retenir, cliquer ensuite sur ok
- Nous allons maintenant donner l'autorisation aux utilisateurs. Dans notre cas, il faut donc ajouter le groupe de sécurité portail et tous les utilisateurs appartenant à ce groupe auront l'autorisation :
- Allez dans Stratégies
- Effectuer un clic-droit sur Stratégies réseau > Nouveau
- Nom de la stratégie : portail captif
- Cliquez sur suivant
- Cliquez sur Ajouter...
- Sélectionnez Groupes d'utilisateur et cliquez sur Ajouter...
- Cliquez sur Ajouter des groupes...
- Tapez le nom de votre groupe :



- Cliquez sur Ok
- Cliquez ensuite sur Suivant
- Laissez par défaut : Accès accordé et cliquez sur Suivant
- Cocher les cases suivantes :



- Laissez tout le reste par défaut et cliquez sur suivant jusqu'à la fin.
- Cliquez sur Terminer.
- Effectuer un double clic sur le nom de la stratégie qu'on vient de créer (portail captif)
- Allez dans l'onglet Paramètres






Ayoub Belbachir

- Allez dans Chiffrement
- Décochez la case : Aucun chiffrement
- On désactive les 2 autre stratégie car elles ne sont pas utiles pour notre portail captif

Connectez-vous au WebUI de votre Pfsense avec un compte administrateur. Nous allons configurer un serveur d'authentification Radius :

- Allez dans le menu : Système > User Manager > Serveurs d'authentification
- Cliquez sur Ajouter
- ✓ Nom descriptif : portail captif
- ✓ Type : RADIUS
- ✓ Protocole : MS-CHAPv2
- ✓ Nom d'hôte ou adresse IP : 192.168.2.5 (Adresse du serveur RADIUS)
- ✓ Secret partagé : ce que vous avez mis lors de l'activation du client RADIUS sous Windows
- ✓ Services offered: Authentication and Accounting
- ✓ Port authentication: 1812
- ✓ Port de comptabilité : 1813
- ✓ Délai d'expiration de l'authentification : 5
- ✓ RADIUS NAS IP : LAN – 192.168.2.1
- Cliquez sur Save

Authentication Servers			
Server Name	Type	Host Name	Actions
portail captif	RADIUS	192.168.2.2	  
Local Database		pfSense	

AB

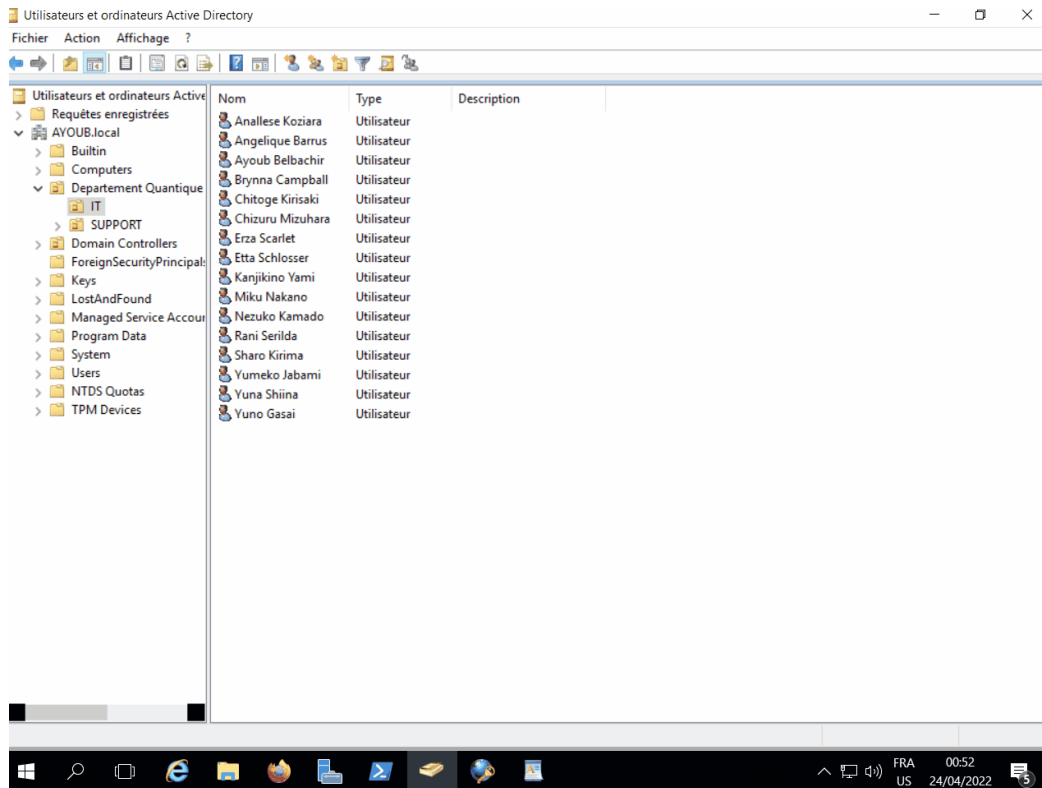
+ Add

Le serveur d'authentification est configuré, nous pouvons le tester l'authentification d'un utilisateur présent dans notre ad depuis l'interface web de notre Pfsense en nous rendant dans l'onglet Diagnostics > Authentification, sélectionner ensuite le serveur d'authentification que l'on vient de créer et saisissez ensuite le prénom et le nom (séparer d'un tiret) et les mots de passe d'un utilisateur utilisateurs ayant droits.



Ayoub Belbachir

Test d'authentification RADIUS depuis pfsense :



Configuration du point d'accès wifi TP Link :

Nous allons configurer le point d'accès wifi pour notre portail captif, il suffit de lui attribuer une adresse IP statique et de le brancher à la 3^{ème} carte réseau de notre firewall Pfsense nommé précédemment "WIFI" :

- Branchez votre point d'accès à une alimentation ne branchez pas encore le câble rj45 nous n'avons pas besoin d'internet pour le moment.
- Connecter vous ensuite au wifi émis par celui-ci le SSID et le mot de passe figure sur une étiqueté au dos de l'appareil.
- Depuis un navigateur accéder ensuite à l'interface web du point d'accès en entrant l'url de celui-ci "<http://tplinkap.net/> " (on peut la retrouver sur la même étiqueté observer à l'étape précédente)
- Entrer l'identifiant et le mot de passe "admin", "admin " suivez ensuite les étapes pour changer le mot de passe, changer le SSID pour "département quantique " et lui attribuer l'adresse IP 172.16.16.2 ainsi que le masque sous-réseau en /24 et désactiver le DHCP
- Branchez ensuite un câble rj45 de notre le point d'accès à la 3^{ème} carte réseau de notre firewall Pfsense
- Connectez ensuite un client au wifi de notre nouveau point d'accès





Ayoub Belbachir

Configuration de la 3^{ème} carte réseau de notre firewall Pfsense :

Nous allons configurer une règle sur notre firewall Pfsense pour que tout ce qui arrive d'Internet soit refusé et tout ce qui sort d'Internet depuis le réseau local soit autorisé, préalablement nommer "WIFI ":

Depuis notre navigateur dans le WebUI de Pfsense avec votre compte Administrateur

Rendez-vous dans l'onglet Firewall>Rules> WIFI add

Edit Firewall Rule			
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	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	OPT1		
	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	Any		
	Choose which IP protocol this rule should match.		
Source			
Source	<input type="checkbox"/> Invert match	OPT1 net	Source Address /
Destination			
Destination	<input type="checkbox"/> Invert match	any	Destination Address /

AB



Ayoub Belbachir

Déploiement du Portail captif :

Nous allons maintenant mettre en place le portail captif de Pfsense avec authentification serveur radius. Allez dans l'onglet Service > Portail Captif

Cliquez ensuite sur add remplir les champs en saisisant le nom de notre portail captif ainsi que la description de celui-ci,

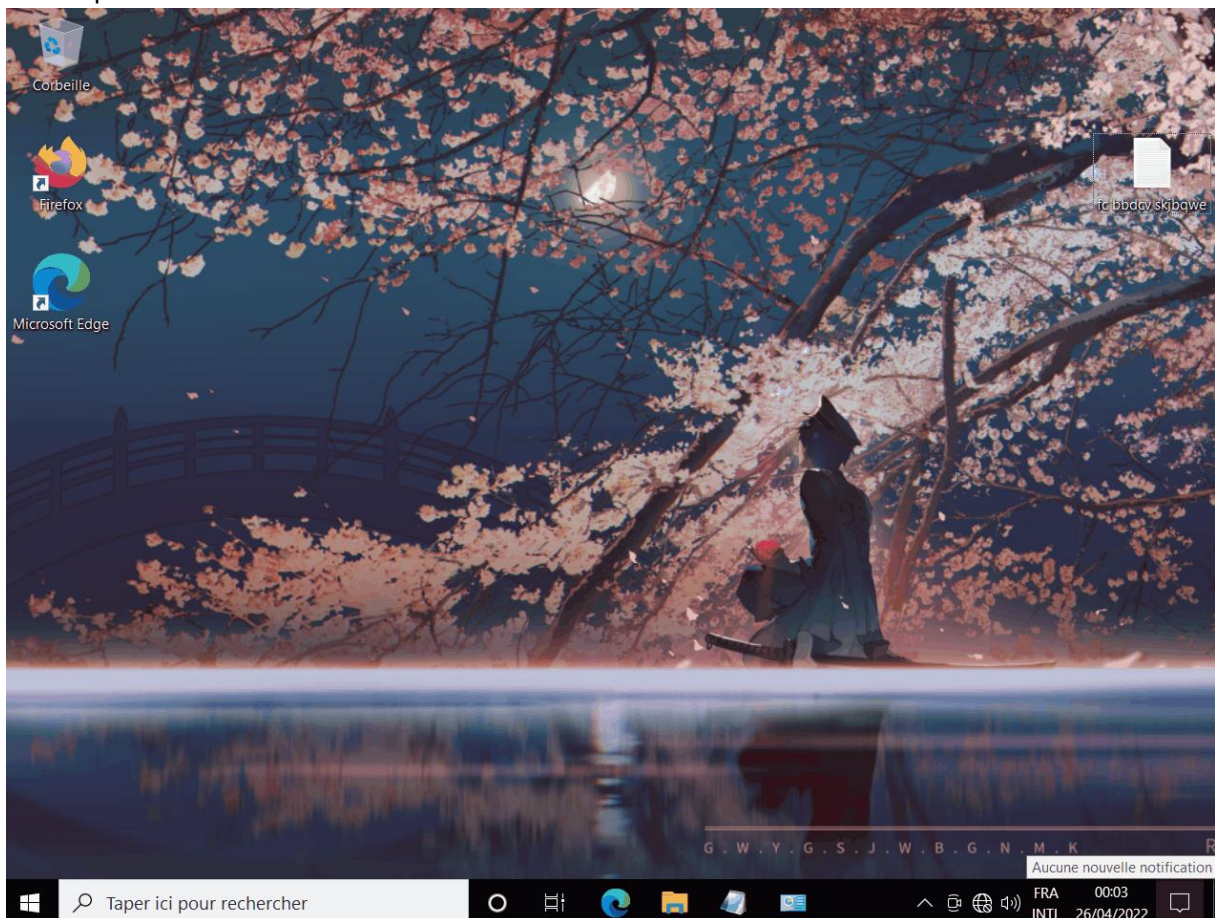
Cliquer sur Save puis nous cocherons la case "Enable Captive Portal", afin d'activer le portail puis sélectionnerons Wifi pour assigner le portail captif à notre 3^{ème} cartes réseaux nommer WIFI.

Optionnel : Nous pouvons choisir l'adresse de redirection apes avoir étaiit authentifier par le portail captif celui-ci nous enverra vers l'adresse de redirection inscrite par exemple <https://ayoubbelbachirsir.fr> , nous pouvons aussi personnaliser la page de connexion de notre portail captif en lui attribuant un arrière-plan et un logo dans l'onglet "Captive Portal Login Page".

Dans la section "authentification" activer l'authentification backend ensuite sélection "Portal captif" cliquer sur Save

Rendez-vous ensuite sur votre une machine client accéder à votre navigateur, normalement une page du portail captif s'ouvre d'elle-même sinon accéder au lien
«[http://192.168.4.1:8002/index.php?zone=portail captif](http://192.168.4.1:8002/index.php?zone=portail%20captif)»

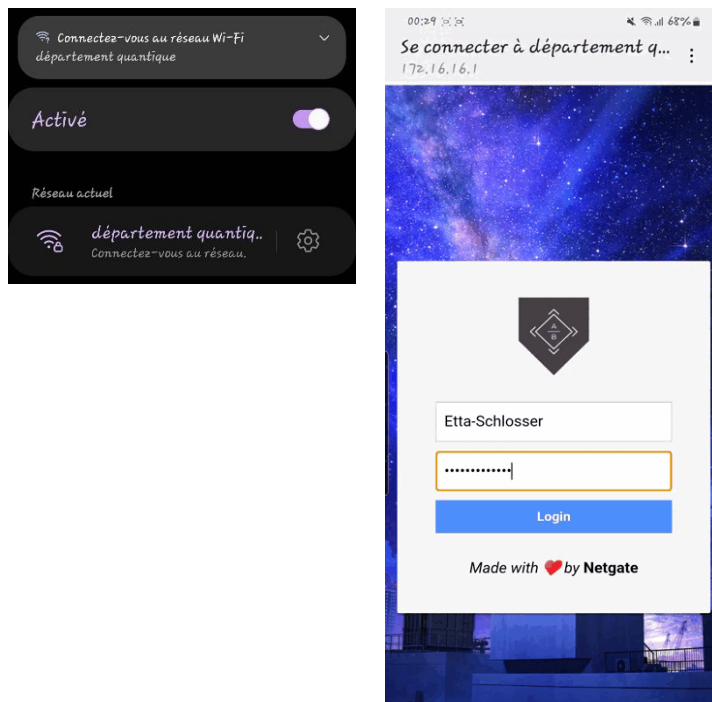
Test depuis un client Windows 10 :





Ayoub Belbachir

Test depuis un client Android :



Nous pouvons supervisée les clients connecter à notre portail captif

192.168.2.1/status_captiveportal.php

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Captive Portal / portail_captif

Users Logged In (2)

IP address	MAC address	Username	Session start	Actions
172.16.16.100	[REDACTED]	Etta-Schlosser	04/25/2022 22:24:46	[Trash icon]
172.16.16.101	[REDACTED]	Anallese-Koziara	04/25/2022 22:25:34	[Trash icon]

[+] Show Last Activity [Disconnect All Users]

AB

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.



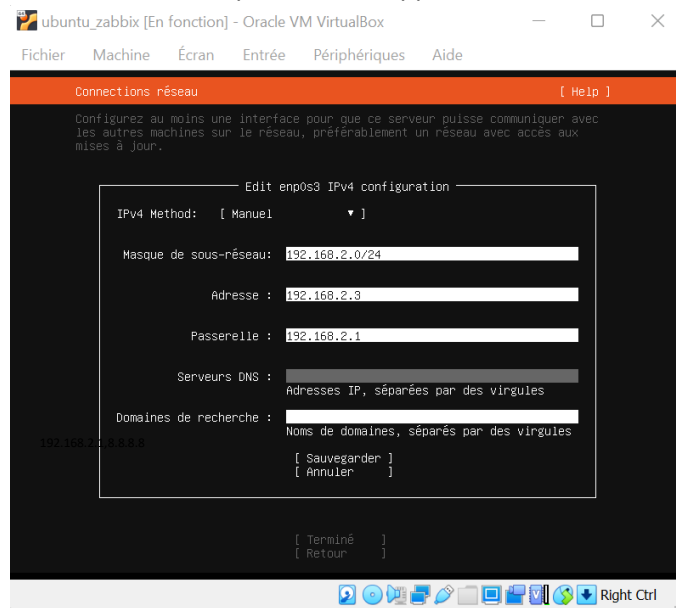
Ayoub Belbachir

Zabbix

Zabbix est un logiciel libre permettant de surveiller l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources. Ici Zabbix supervisera notre Windows server.

Installation de notre Ubuntu server 20.04

Lors de l'installation de Ubuntu nous pouvons désapprendre attribuer une adresse ip statique



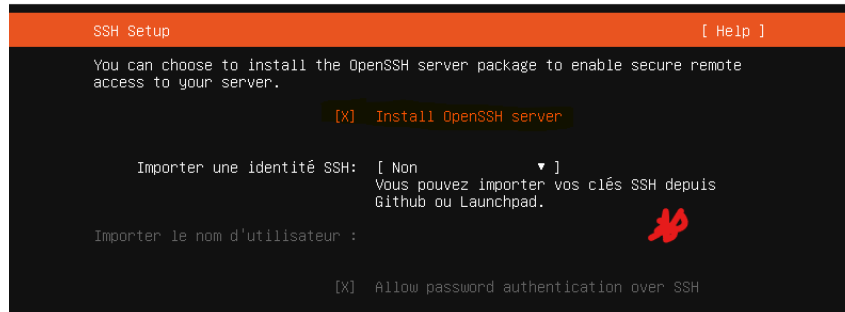
Si vous avez raté cette étape vous pouvez modifier le fichier `/etc/netplan/00-installer-config.yaml` via le SHELL, il suffit dit renseigner l'adresse ip voulu la passerelle de notre Ubuntu (LAN Pfsense) et un DNS ici le LAN de notre Pfsense le DNS de google ça donne donc :

```
GNU nano 4.8 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses:
        - 192.168.2.3/24
      gateway4: 192.168.2.1
      nameservers:
        addresses: [192.168.2.1, 8.8.8.8]
        search: []
  version: 2
```



Ayoub Belbachir

A la dernière étape de l'installation Ubuntu nous demande si nous souhaitons installer les paquets nécessaires pour installer un serveur SSH il suffit de cocher la case



Si vous avez raté cette étape vous pouvez installer un serveur SSH via le SHELL avec les commandes suivantes.

- **sudo** nous permet d'élever les droits d'écriture sur la machine
- **apt** quant à lui est le gestionnaire de paquets propre à Debian présent nativement dans les versions récentes d'Ubuntu

```
sudo apt install openssh-server
```

Redirection Pfsense SSH

L'installation de Zabbix se fera en SSH depuis une machine hôte présente sur le Wan de Pfsense, nous allons donc procéder à une application de règle de redirection sur notre Pfsense.

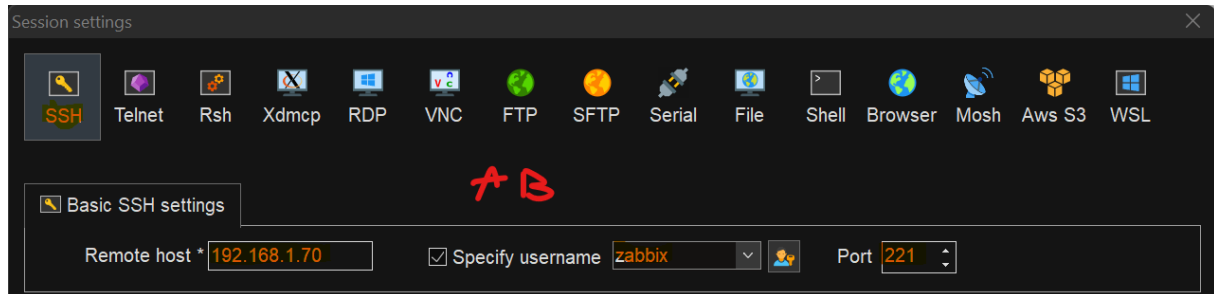
Depuis le WebUI de Pfsense rendez-vous dans l'onglet Firewall > NAT ajouter une nouvelle règle

Cette règle nous permet de rédiger les demandes du protocole SSH depuis notre Ubuntu server vers l'adresse WAN dans le port 221



Ayoub Belbachir

Depuis la machine hôte utiliser PuTTY ou MobaXtrem saisissez l'adresse ip Wan du Pfsense et le port que nous avons saisi lors de création de la règle NAT.



Installation de Zabbix

Nous devons premièrement télécharger les informations des packages source et mise à jour des paquets

```
≥ sudo apt-get update
≥ sudo apt-get upgrade
```

Nous devons installer un système de gestion de base de données, nous utiliserons MySQL

```
sudo apt install mysql-server
```

Pour les nouvelles installations de MySQL, vous devrez exécuter le script de sécurité inclus dans le SGBD. Ce script modifie certaines des options par défaut les moins sûres pour des choses comme les connexions root distantes et les samples users.

il suffit de suivre les étapes une fois la commande exécuter.

```
sudo mysql_secure_installation
```

Nous téléchargeons ensuite la dernière version de Zabbix à la racine de notre Ubuntu server

```
wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-1+ubuntu20.04_all.deb
```

Nous installons le fichier précédemment télécharger

```
dpkg -i zabbix-release_6.0-1+ubuntu20.04_all.deb
```

Nous devons télécharger les informations des packages source

```
sudo apt-get upgrade
```

Ensuite nous installons Zabbix server, frontend et l'agent

```
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

Nous créons la base de données pour Zabbix

```
mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'NOUVEAU_MOTS_DE_PASSE';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> quit;
```

Sur l'hôte du serveur Zabbix, importez le schéma et les données initiaux. Vous serez invité à entrer votre mot de passe nouvellement créé.

```
zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix
```



Ayoub Belbachir

Afin de configurer la base de données précédemment créée modifier le fichier **/etc/zabbix/zabbix_server.conf** décommenter la ligne la ligne figurant « DBPassword= » et insérer le mot de passe de notre base de données.

Nous allons ensuite changer la langue du WebUI de Zabbix pour ce faire nous devons installer un nouveau langage sur le serveur Zabbix.

Exécuter la commande `sudo dpkg-reconfigure`

Et sélectionner la langue française en appuyant sur la touche espace `fr FR ISO-8859-1`

Faire la touche « TAB » puis « entres »

Redémarrer enfin le service apache `service apache2 restart`

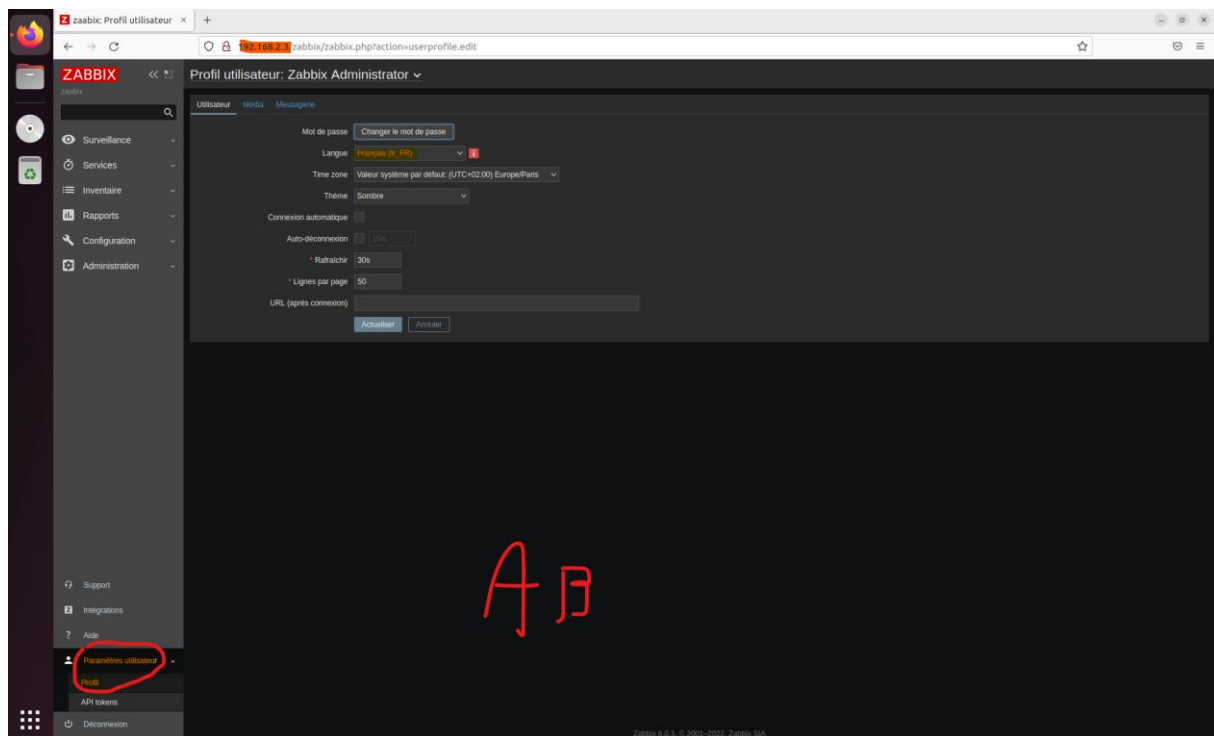
Depuis un navigateur rendez vous sur l'URL suivante qui varie selon l'adresse IP attribuer à notre Ubuntu server.

Sur l'écran de connexion, utilisez le nom d'utilisateur et le mot de passe par défaut.

- Nom d'utilisateur par défaut : Admin
- Mot de passe par défaut : zabbix

Dans la partie inférieure droite de l'écran, accédez aux paramètres du profil utilisateur.

Sur l'écran du profil utilisateur, sélectionnez la langue souhaitée et cliquez sur le bouton Mettre à jour.

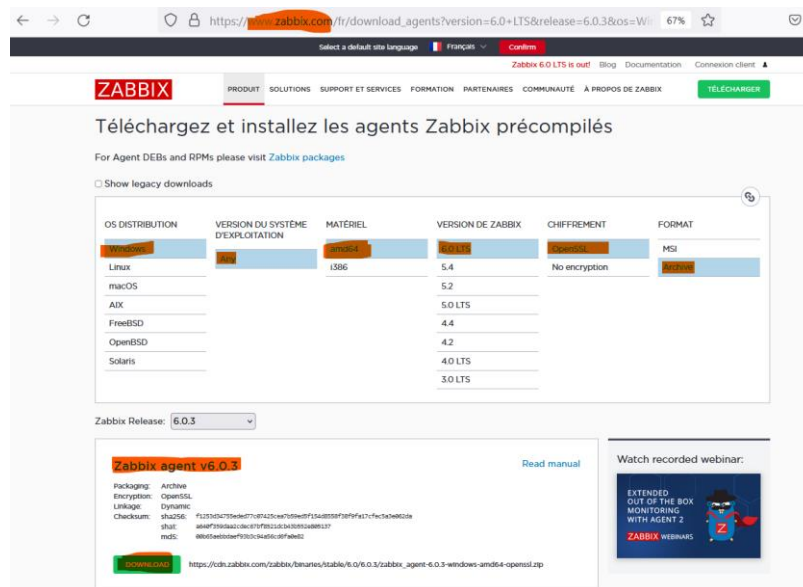




Ayoub Belbachir

Afin de superviser notre Windows server nous allons installer l'agent de zabbix sur notre windows server :

Commençons par télécharger l'agent de Zabbix sous format .zip sur le site officiel de Zabbix depuis notre Windows server.



Décompresser le dossier et modifier le fichier « **zabbix_agentd.conf** » avec un éditeur de texte

Changer la ligne « **Server=127.0.0.1** » en remplaçant l'adresse ip local par l'adresse ip de notre server Zabbix « **Server=192.168.2.3** » sauvegarder le fichier et copier le dans le dossier bin présent dans le dossier précédemment décompresser.

Rendez-vous dans l'invite de commande de notre Windows server, a l'aide de la commande « **cd** »

rendez-vous dans le bin `cd C:\Users\Administrateur\Downloads\zabbix_agent-6.0.3-windows-amd64-openssl\bin`

Puis exécuter la commande suivante pour installer l'agents avec notre configuration

```
zabbix_agentd.exe -c c:\zabbix\zabbix_agentd.conf -i
```

Le résultat devrait être le suivant



Ayoub Belbachir

Maintenons-nous allons créer un nouvel hôte dans le WebUI de Zabbix

Rendez-vous dans l'onglet Surveillance > Hôtes puis cliquer sur

Créer un hôte

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	192.168.2.2		IP	DNS	10050

L'agent Zabbix étant fin mis en place vous pouvez personnaliser le tableau de bord du WebUI de Zabbix

