Introduction Générale

Chapitre 1 : Généralités

Les attaques informatiques

Présentation

Les types d'attaques

Dispositifs de protection

Pare-feu

Présentation

Principe de fonctionnement

Limites de pare-feu

Étude comparative et choix d'un firewall pour notre travail

Chapitre 2 : Analyse

Présentation du montage à réaliser

Chapitre 3 : Conception

Les logiciels utilisés

Présentation de VirtualBox

Présentation de serveur radius

Présentation de pfSense

Installation et configuration de pfsense sous virtualbox

Installation de pfsense

Configuration de pfsense

Translation d'adresses

Installation et configuration de serveur radius sous Windows server

Installation de serveur radius

Configuration et création d'utilisateur sur serveur radius

Chapitre 4 : Réalisation

Liste des tableaux

Liste des figures

Introduction générale

Le développement du réseau Internet, et de ses déclinaisons sous forme d'Intranets et d'Extranets, soulève des questions essentielles en matière de sécurité informatique. L'accroissement des trafics en télécommunication révèlent les besoins grandissants d'échanges privés et professionnels. Ces transmissions de données imposent une ouverture des systèmes d'information vers l'extérieur, notamment vers Internet. Celle-ci entraine une certaine dépendance des entreprises et des personnes vis-à-vis des services qu'offre Internet. Ainsi conjuguées, cette ouverture et cette dépendance rendent l'entreprise vulnérable aux risques. C'est pour cela que la sécurité Internet est devenue un sujet de recherche très intense. Ces recherches ont permis le développement de certains dispositifs de sécurité comme les pares-feux, les antivirus et les systèmes de cryptographie pour protéger les systèmes informatiques.

Vu l'importance et l'obligation de l'élaboration d'un pare-feu, chaque organisme doit établir un pare-feu pour la sécurité informatique afin d'identifier les sources de menace et ses dégâts informationnels.

C'est dans cette optique que s'inscrit notre travail : mise en place et déploiement d'un pare-feu

Un pare-feu, appelé aussi "coupe-feu", "garde-barrière" ou "firewall" en anglais, est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers ou externe (Internet). Ce système permettant de filtrer les paquets de données échangés avec le réseau. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivantes :

Une interface pour le réseau à protéger (réseau interne) et une interface pour le réseau externe.

Chapitre 1 : généralités

Chaque ordinateur connecté à Internet et d'une manière plus générale à n'importe quel réseau informatique, est susceptible d'être victime d'une attaque d'un pirate informatique. Ainsi, il est nécessaire de se protéger de ces attaques réseaux en installant un dispositif de protection.

I. Les attaques informatiques

1. Présentation

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une attaque est l'exploitation d'une faille (vulnérabilité ou brèche) d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plus part lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mieux s'y préparer.

Les motivations des attaques peuvent être de différentes sortes :

Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système,
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles,
- Glaner des informations personnelles sur un utilisateur,
- Récupérer des données bancaires,
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.),
- Troubler le bon fonctionnement d'un service,
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée, etc.

2. Les types d'attaques

Il est ainsi possible de catégoriser les risques de la manière suivante :

- Accès physique : il s'agit d'un cas où l'attaquant a accès aux locaux, éventuellement même aux machines :
  - ✓ Coupure de l'électricité,
  - ✓ Extinction manuelle de l'ordinateur,
  - ✓ Vandalisme,

- ✓ Ouverture du boîtier de l'ordinateur et vol de disque dur,
- ✓ Ecoute du trafic sur le réseau,
- ✓ Ajout d'éléments (clé USB, point d'accès Wifi……).

➢ Interception de communications :
- ✓ Vol de session,
- ✓ Usurpation d'identité,
- ✓ Détournement ou altération de messages.

➢ Dénis de service : il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
- ✓ Exploitation de faiblesses des protocoles TCP/IP,
- ✓ Exploitation de vulnérabilité des logiciels serveurs.

➢ Intrusions :
- ✓ Balayage de ports,
- ✓ Elévation de privilèges : ce type d'attaque consiste à exploiter une vulnérabilité d'une application,
- ✓ Maliciels : (virus, vers, et chevaux de Troie).

3. Dispositifs de protections

Il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou fibre optique, de se protéger des attaques réseaux en installant un dispositif de protection (Pares-feux, antivirus, réseaux privés virtuels, systèmes de détection d'intrusions, Proxys, etc.) permettant d'ajouter un niveau de sécurisation supplémentaire.

ll. Pare-feu

1. Présentation

Un **Pare-feu** (appelé aussi Coupe-feu, Garde-barrière ou **Firewall**), est un système permettant de protéger un ordinateur, ou un réseau d'ordinateurs, des intrusions provenant d'un réseau tiers (notamment Internet). Le Pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante
comportant au minimum les interfaces réseau (cartes réseau) suivantes :

➢ Une interface pour le réseau à protéger (réseau interne),
➢ Une interface pour le réseau externe (internet).

La configuration du Firewall est telle que les données arrivant sur l'une des cartes ne soient pas transmises directement sur l'autre mais de manière sélective, selon des critères de filtrage déterminés lors de sa configuration.
Le filtrage réalisé par le Pare-feu constitue le premier rempart de la protection du système d'information.

Selon la nature de l'analyse et de traitements effectués par un Firewall, différents types

de Firewalls existent. Ils se distinguent le plus souvent en fonction du niveau de filtrage des données auquel ils opèrent : niveau 3 (IP), niveau 4 (TCP, UDP) ou niveau 7 (FTP, HTTP,etc.) du modèle OSI. Dans le cas de la fonction du routeur (Firewall routeur), il analyse chaque paquet de données selon les informations contenant dans le paquet (adresses
IP, numéro de port, type de paquet).

2. Principe de fonctionnement

Un système Pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion [allow],
- De bloquer la connexion [deny],
- De rejeter la demande de connexion sans avertir l'émetteur [drop].

L'ensemble de ces règles permettent de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux
types de **politiques de sécurité** permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées : « tout ce qui n'est pas explicitement autorisé est interdit »,
- Soit d'empêcher les échanges qui ont été explicitement interdites.

3. Limite de pare-feu

Un système Pare-feu n'offre bien évidemment pas une sécurité absolue, bien au contraire. Les firewalls n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité. C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du
Pare-feu.

De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter fortement préjudice à la politique de sécurité globale.

Un Firewall ne peut pas protéger l'environnement à sécuriser contre des attaques ou des accès illicites qui ne passent pas par lui. Il n'est d'aucune efficacité en ce qui concerne des délits perpétrés à l'intérieur de l'entreprise,

Un Firewall n'est pas un anti-virus, il faut donc le protéger de manière complémentaire contre des infections virales.

Enfin, afin de garantir un niveau de protection maximal, il est nécessaire d'administrer

le Pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies. Par ailleurs, il est recommandé d'effectuer une **veille de sécurité** (en s'abonnant aux alertes de sécurité) afin de modifier le paramétrage de son dispositif en fonction de la publication des alertes.
La mise en place d'un Firewall doit donc se faire en accord avec une véritable politique de sécurité.

4. Étude comparative et choix d'un firewall pour notre travail

La façon de configurer un Firewall et de le gérer est tout aussi importante que les capacités intrinsèques qu'il possède.

4.1.Comparaison

L'analyse concurrentielle est une étape très importante pour le choix du pare-feu. Elle consiste à déterminer les principaux concurrents du pare-feu afin d'extraire leurs aspects positifs et négatifs. Pour cela nous avons choisi d'étudier deux pare-feu, qui sont PfSense et IPCOP.
Le tableau ci-dessous représente une étude comparative de PfSense et IPCOP

IPCOOP	PfSense
Basé sur Linux (Gratuit)	Basé sur Free BSD (Gratuit)
Caractéristiques: • DHCP (Dynamic Host Configuration Protocol) • DNS (Domain Name System) • NTP (Network Time Protocol) • NAT (Network address translation) • VPN : IPSec • QoS (traffic chapping) : Priorité selon • type de trafic, lissage de trafic (limitation) • Un serveur proxyWeb • Filtrage d'URL (SquidGuard) • Filtrage dynamique • Supervision de la bande passante.	Caractéristiques: • DHCP • DNS • NTP • NAT • VPN : IPSec, PPTP, L2TP • Load Balancing (Equilibrage de charge) • Multi-WAN • QoS (traffic chapping) : Priorité selon type • de trafic, lissage de trafic (limitation) • Un serveur proxyWeb (Squid) • Filtrage d'URL (SquidGurad) • Portail captif • Filtrage simple de paquet • Filtrage dynamique • Supervision de la bande passante (Ntop) • Mises à jour automatique

4.2. Choix du pare-feu

Au vu de ce comparatif, les deux solutions s'adaptant aux critères de sécurité dont nous avons besoin [Serveur proxy (filtrage applicatif), filtrage d'URL (SquidGuard), supervision de la bande passante]. Mais, il se trouve que PfSense possède plus de fonctionnalités que IPCOOP (mises à jour automatique, Portail captif, Load Balancing, Multi-WAN). Notre choix est ainsi porté sur le logiciel PfSense Open Source qui grâce à ses différentes fonctionnalités, apportera la sécurité nécessaire au réseau local de l'entreprise.

Chapitre 2 : Analyse

Notre réseau est un réseau d'une université. Nous avons pris le cas d'un UFR au sein de l'UNB (L'ESI)

Notre travail s'effectuera sur 3 réseaux différents

WAN : wireless area network qui est un reseau etendu generalement qualifié (d'internet)

LAN : local area network qui est un reseau local à la taille d'une entreprise

DMZ : **Zone démilitarisée** (notée **DMZ**, Demilitarised Zone) désigne
cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi
office de « zone tampon » entre le réseau à protéger et le réseau hostile.

Ains dans notre reseau LAN nous auront trois sous reseaux :

Le sous reseau des etudiants

Le sous reseau du personnel

Le sous reseau des administrateurs

Le schema ci-dessous montre les différent element de notre reseau

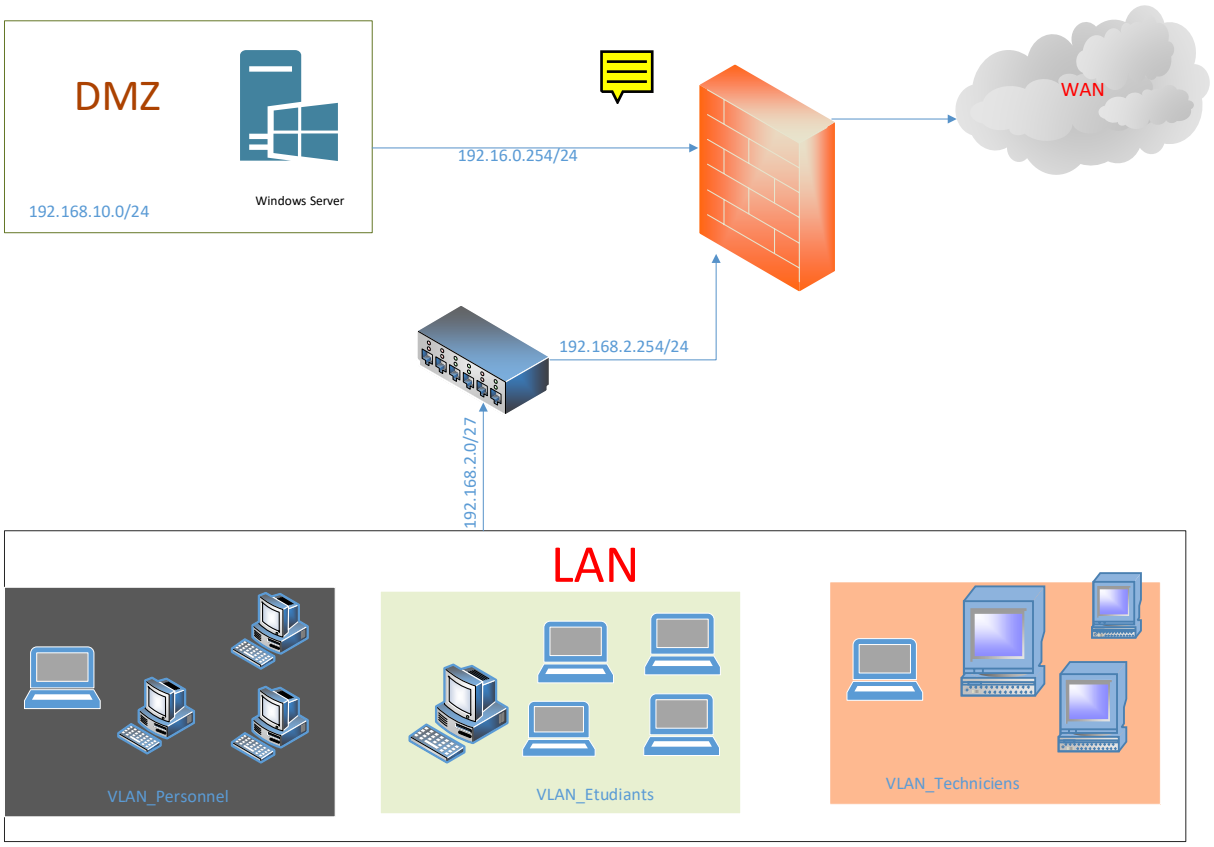


Figure : notre configuration reseau à réaliser

Chapitre 3 : Conception

- ✓ Les logiciels utilisés
  1. Les logiciels utilisés
     Virtualbox version 7.0.14
     Windows server
     Pfsense version 2.7.2
     Windows client

1.1 Presentation de virtualbox

Virtualbox permet la création d'une ou plusieurs
machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant
sur la même machine physique (machine existante réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte.

2.1 Presentation de pfsense

PfSense (distribution logicielle), ou ≪ **P**acket **F**ilter **Sense** ≫ est un routeur / pare-feu open source basé sur FreeBSD. Il date de 2004 à partir d'un fork de m0n0wall par Chris

Buechler et Scott Ullrich. PfSense peut être installé sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (*packet filter*), il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN (802.1q)
Les avantages principaux de PfSense sont les suivants :

- Il est adapté pour une utilisation en tant que pare-feu et routeur,
- Il comprend toutes les fonctionnalités des pare-feu coûteux commercialement,
- Il offre des options de firewalling /routage plus évolué qu'IPCOOP,
- Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres,
- Simplicité de l'activation / désactivation des modules de filtrage,
- Système très robuste basée sur un noyau FreeBSD,
- Des fonctionnalités réseaux avancées

Les services proposés :

- Portail captif
- Filtrage web
- Vlans virtuelles
- traffics shaper
- etc

1.3 Presentation de FreeBSD

FreeBSD est un système d'exploitation de type Unix librement disponible, largement utilisé par des fournisseurs d'accès à Internet, dans des solutions tout-en-un et des systèmes embarqués et partout où la fiabilité par rapport à un matériel informatique est primordiale.
FreeBSD est le résultat de presque trois décennies de développement continu, de recherche et de raffinement. L'histoire de FreeBSD commence en 1979, avec BSD.

1.4 Presentation de radius server

RADIUS (Remote Authentification Dial-In User Service) est un protocole client-serveur permettant de centraliser les données d'authentification. Le protocole RADIUS a été inventé et développé en 1991 par la société Livingston entreprise qui fabriquait des serveurs d'accès au réseau pour du matériel uniquement équipé d'interface série.

- ✓ Installation et configuration de pfsense sous virtualbox

1. installation

Création d'une machine virtuelle :

On crée une Machine Virtuelle sous Virtualbox avec les spécifications suivantes :

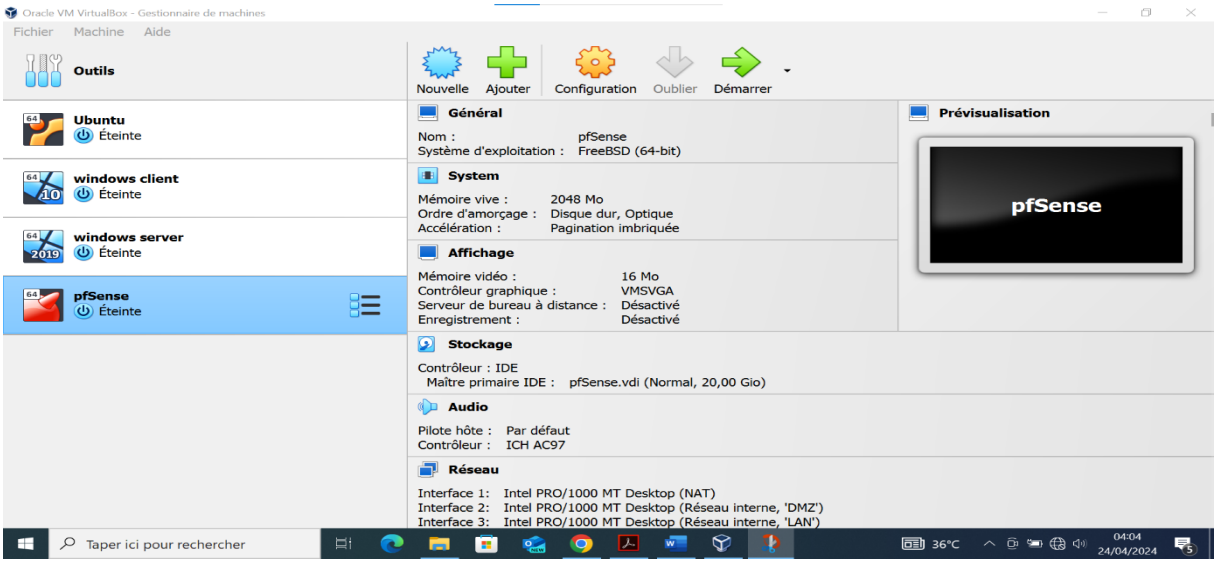


Figure : machine virtuelle

Avant de commencer l'installation, notre machine doit être équipée en minimum de trois cartes réseaux. Pour ce projet on va utiliser trois interfaces (3 cartes réseaux).
LAN : pour qu'on puisse communiquer localement avec le server
PfSence.
DMZ : **Zone démilitarisée** pour désigner cette zone isolée hébergeant des applications mises à disposition du public.
WAN : pour qu'on puisse se connecter à Internet.

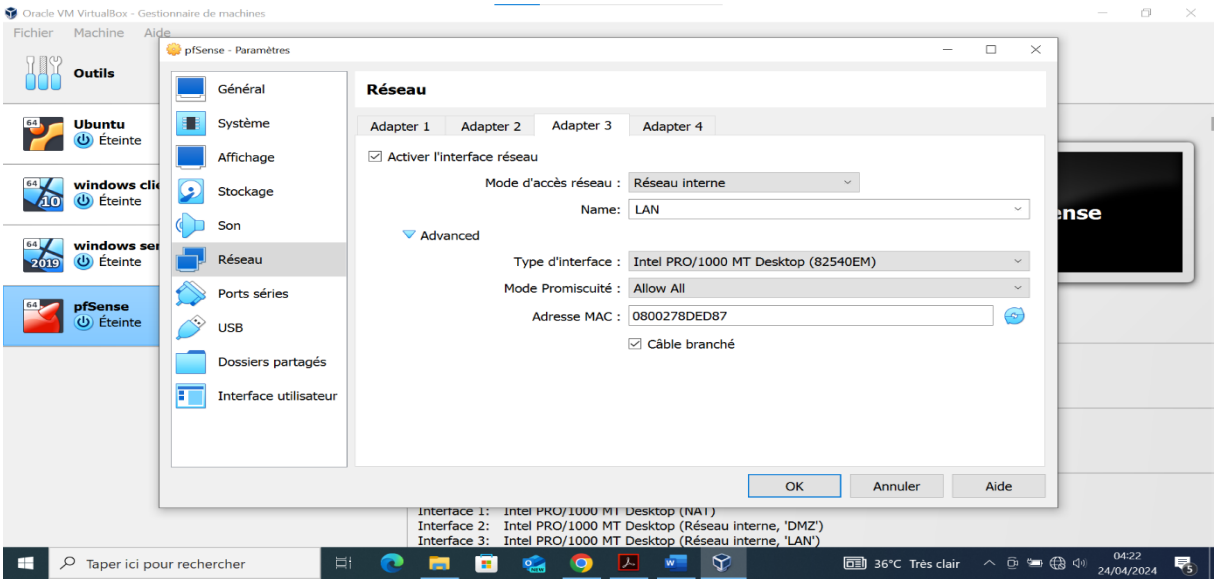


Figure : machine virtuelle : installation de la carte réseau LAN

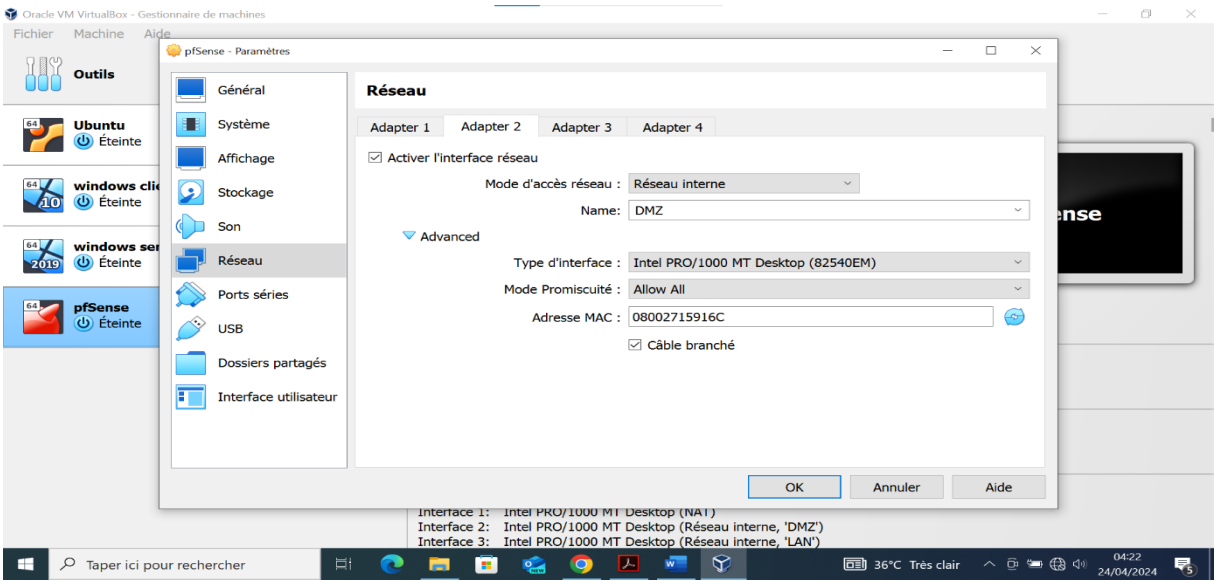


Figure : machine virtuelle : installation de la carte réseau DMZ

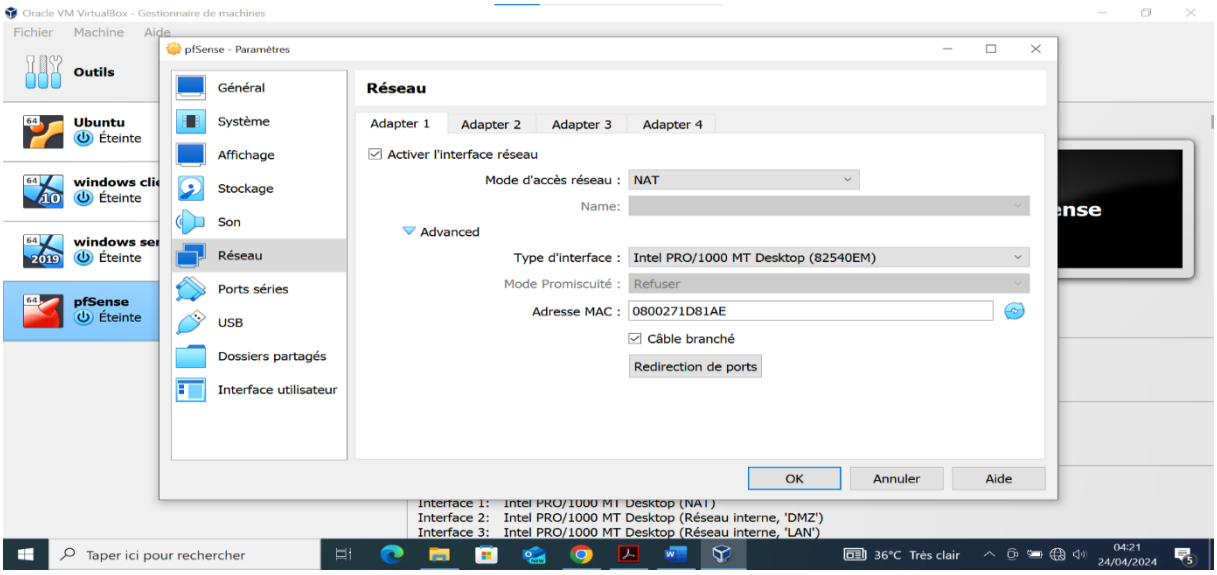


Figure : machine virtuelle : installation de la carte réseau WAN

On clique sur **Demarrer** pour commencer l'installation de PfSense.
La fenêtre suivante s'affiche :

Figure : pfsense : installation en mode demarrage

Ensuite sur la fenetre suivante on appuie sur ok pour commencer l'installation du systeme

Figure : pfsense : installation

Choisir select et cliquer sur entrer

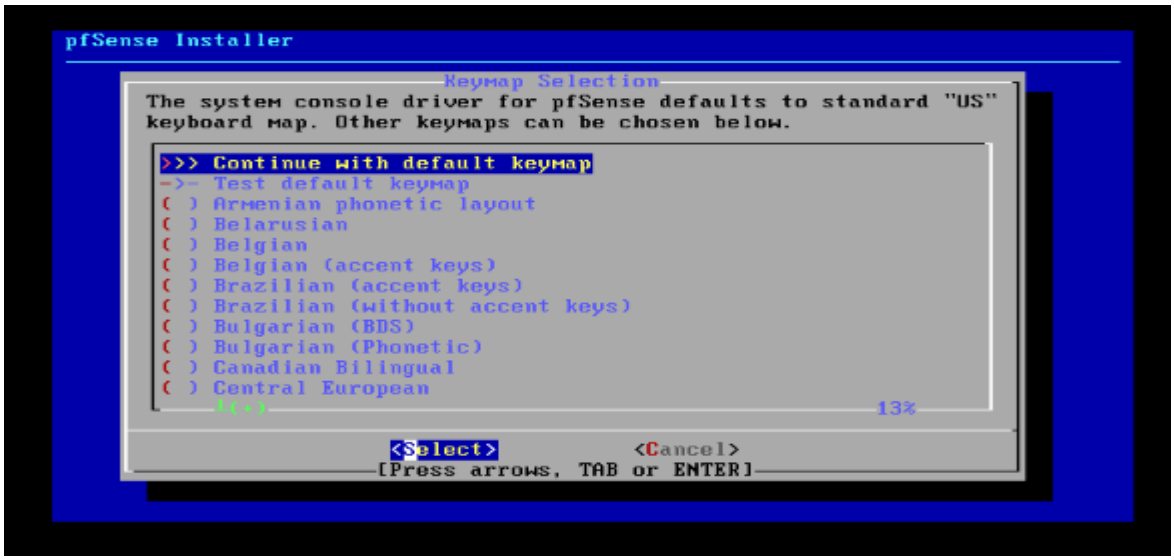


Figure : pfsense : installation

Cliquer sur Ok sur la fenetre suivante

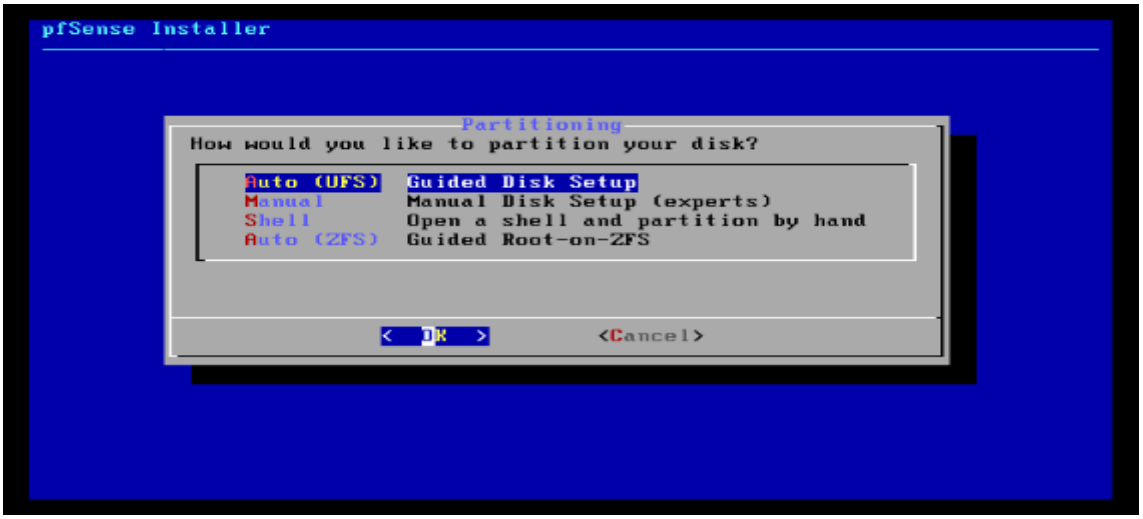


Figure : pfsense : installation

Cliquez sur reeboot pour redemarrer.

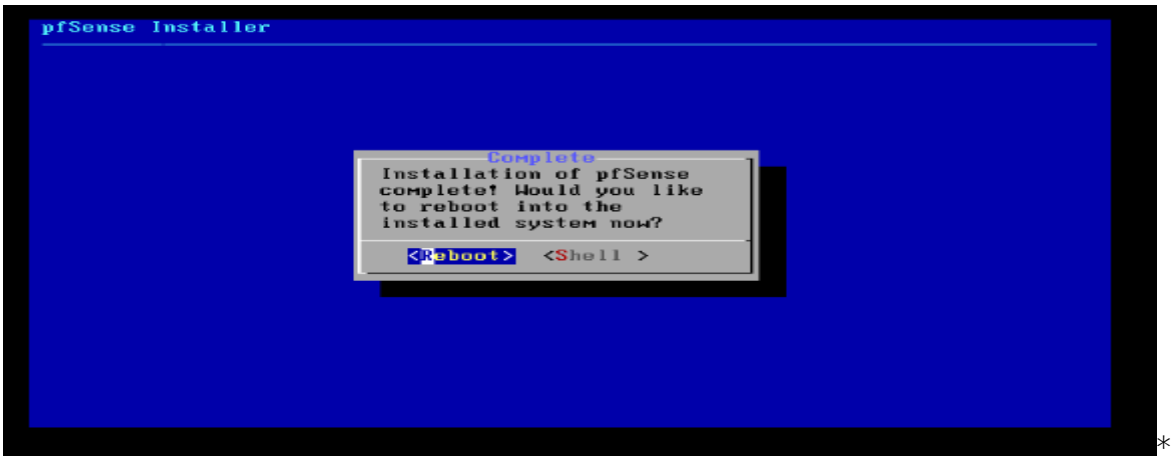


Figure : pfsense : installation terminer

Une fois la machine eteinte aller dans configuration sur virtualbox et supprimer le disque dans stockage pour eviter que la machine ne redemarre en voulant installer pfsense une 2e fois.

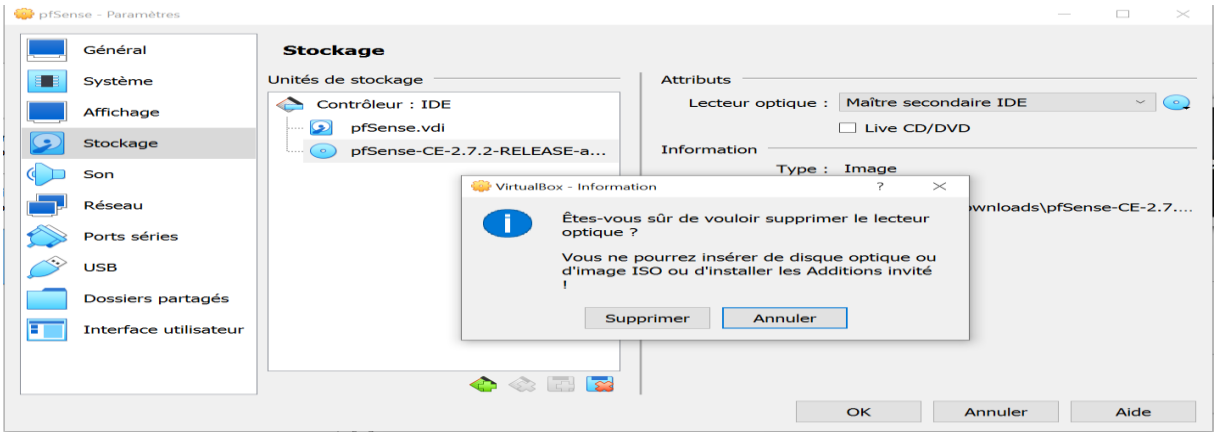


Figure : suppression du disque d'installation de pfsense dans le menu stockage de virtualbox

Les adresses IP des interfaces WAN et LAN sont attribuées par nous meme par le choix de l'option 2 (l'@ IP de WAN attribuée par le serveur DHCP, l'@ IP du LAN et du DMZ attribuée statiquement).

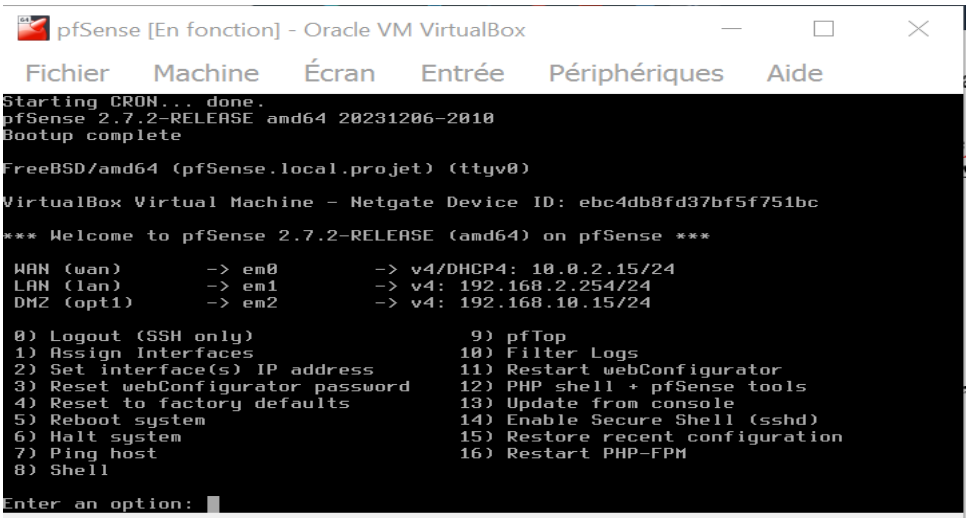


Figure : l'ecran d'acceuil de pfsense

Pour se connecter à l'interface web de configuration de PfSense on utilise l'adresse IP de l'interface LAN : http://192.168.10.15/ cette page s'affiche

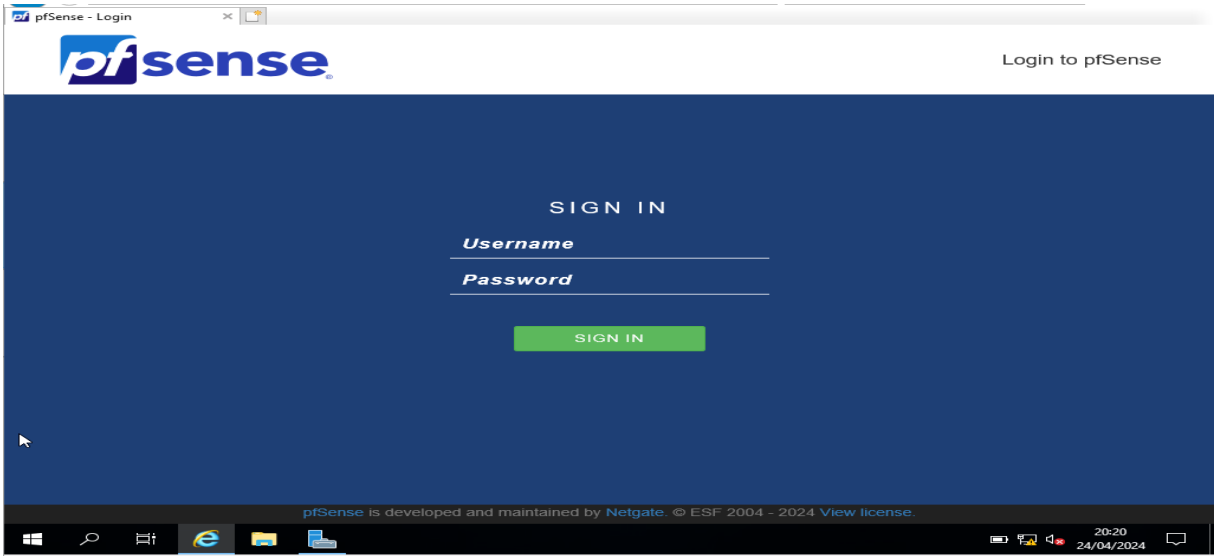


Figure : page d'identification pfsense

Le couple « Username/Password » par défaut est « admin/pfsense »

2. Configuration

Premiere configuration

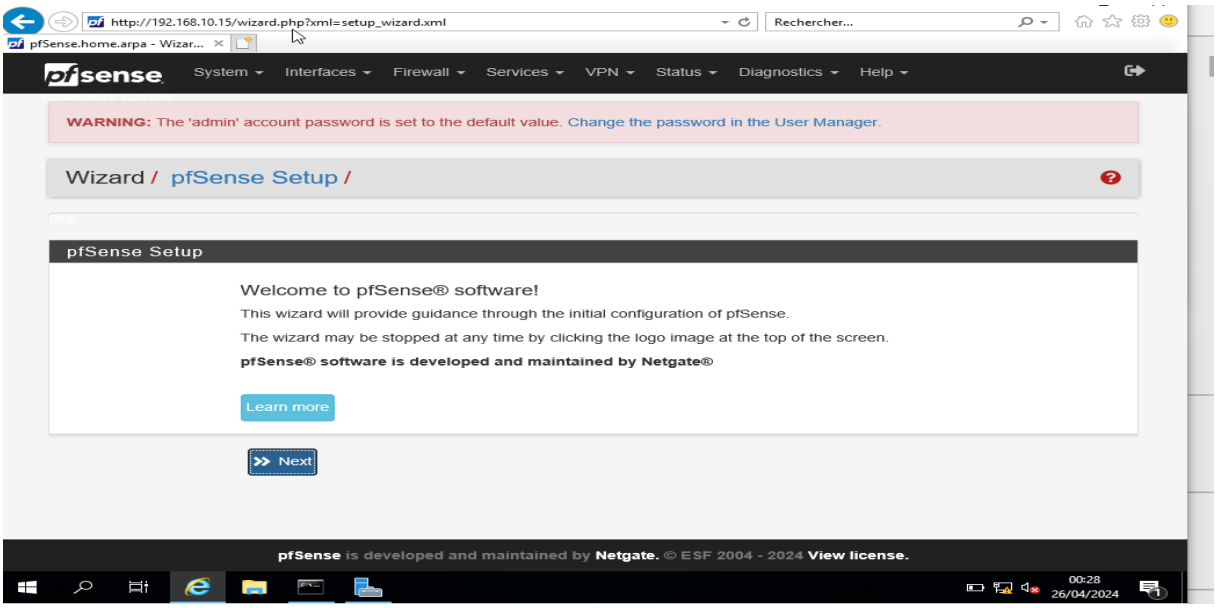


Figure : première configuration graphique

Apres confiuration de pfsense on obtient cette page :

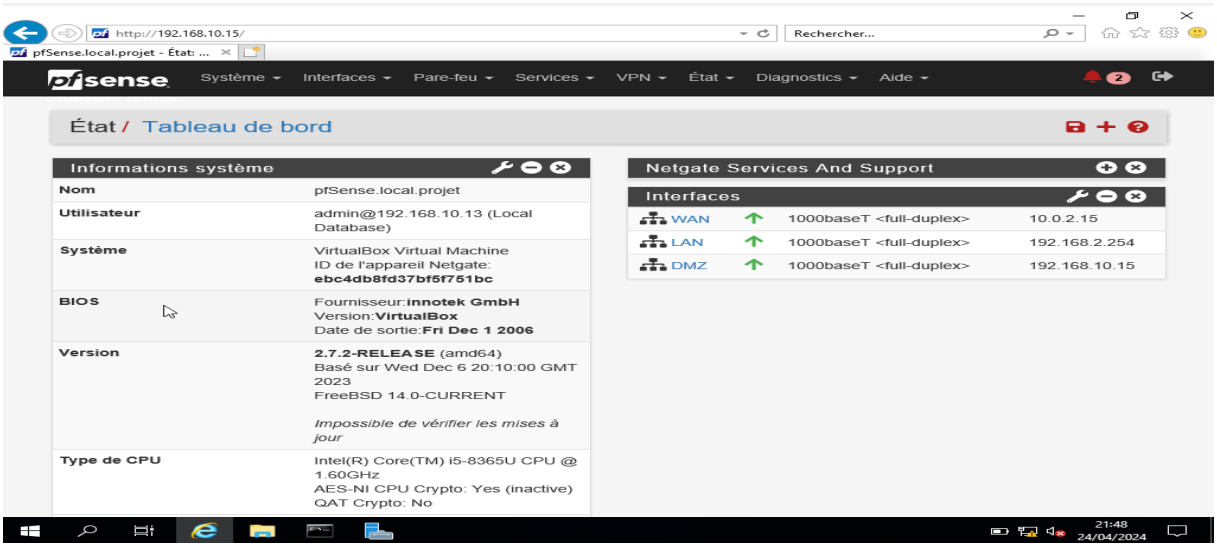


Figure : informations après configuration

Après avoir décrit l'analyse et à la conception du pare-feu PfSense mis en place, et expliciter les différentes étapes pour son installation et sa configuration basique, nous allons passer dans ce qui suit à la phase réalisation. Dans cette section, nous allons paramétrer également quelques paquets de firewall PfSense.

3. Translation d'adresse (NAT)

Son principe consiste à modifier l'adresse IP source ou destination, dans l'en-tête d'un datagramme IP lorsque le paquet transite dans le Pare-feu (Proxy) en fonction de l'adresse source ou destination et du port source ou destination.

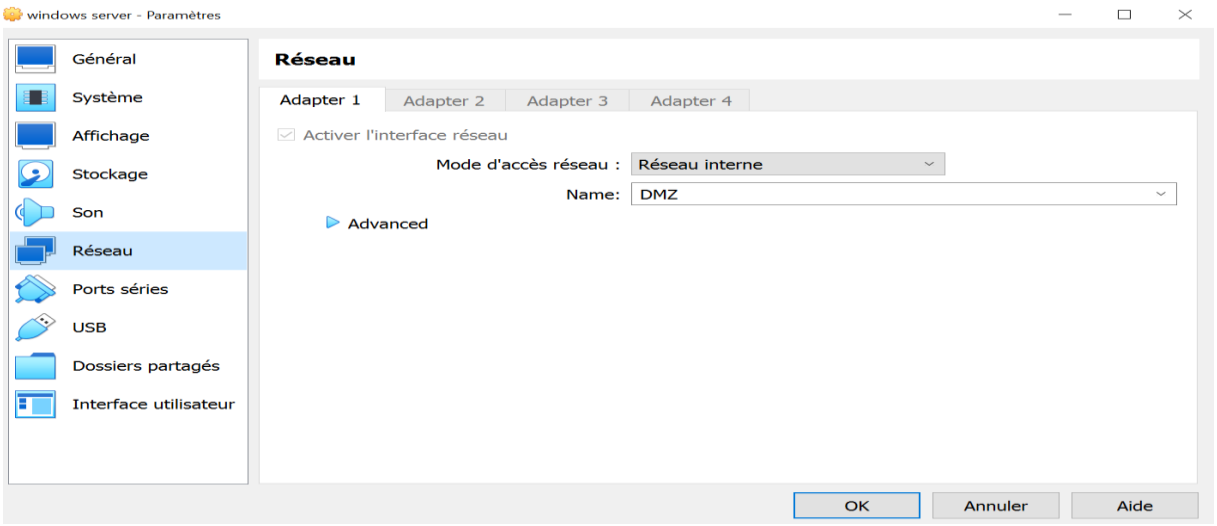
Lors de cette opération, le Pare-feu garde en mémoire l'information lui permettant d'appliquer la transformation inverse sur le paquet de retour. La traduction d'adresse permet de masquer le plan d'adressage interne (non routable) à l'entreprise par une ou plusieurs adresses routables sur le réseau externe ou sur Internet. Cette technologie permet donc de cacher le schéma d'adressage réseau présent dans une entreprise derrière un environnement protégé.

Translation statique
Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. La passerelle permet donc d'associer à une adresse IP privée (Par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

Translation dynamique
Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP

- ✓ Installation et configuration de serveur radius sous windows server

Windows server étant dans notre DMZ, alors son interface reseau sous virtualbox sera comme suit :



Ainsi sur windows server nous avons installer les roles :

Actives Directory avec le nom de domaine : projet.local

DNS , DHCP.

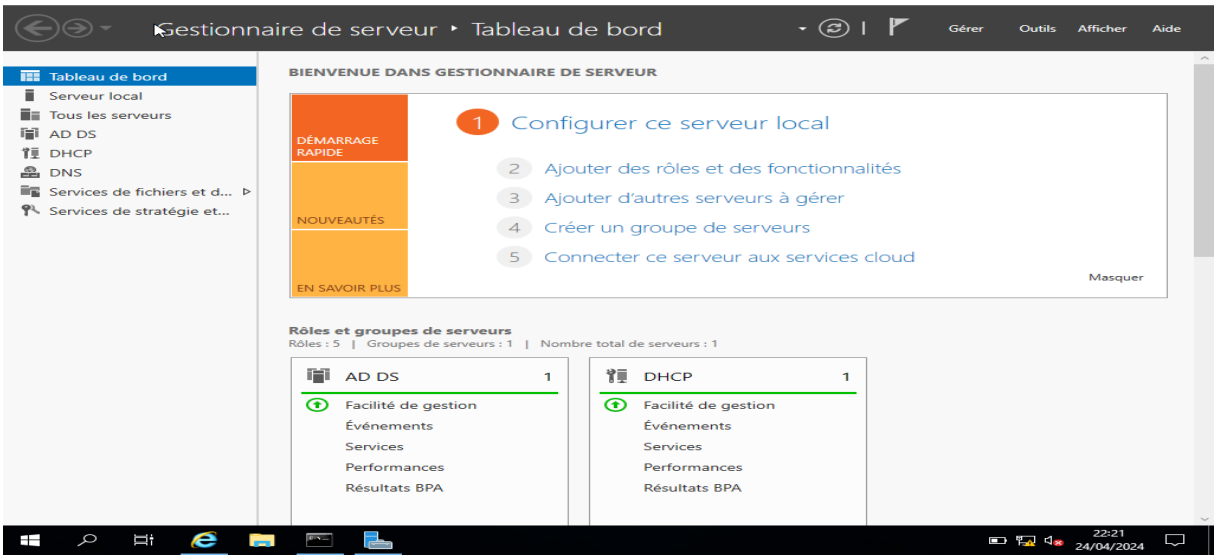


Figure : tableau de bord de l'outil de gestion de serveur

Connectez vous à votre compte puis allez dans le gestionnaire de serveur et cliquez sur **Outils > Utilisateurs et ordinateurs Active Directory**

- Cliquez sur votre domaine : **projet.local**
    - Allez dans **Users**
    - Effectuer un clic droit **Nouveau > Groupe**
    - Donner un nom à votre groupe

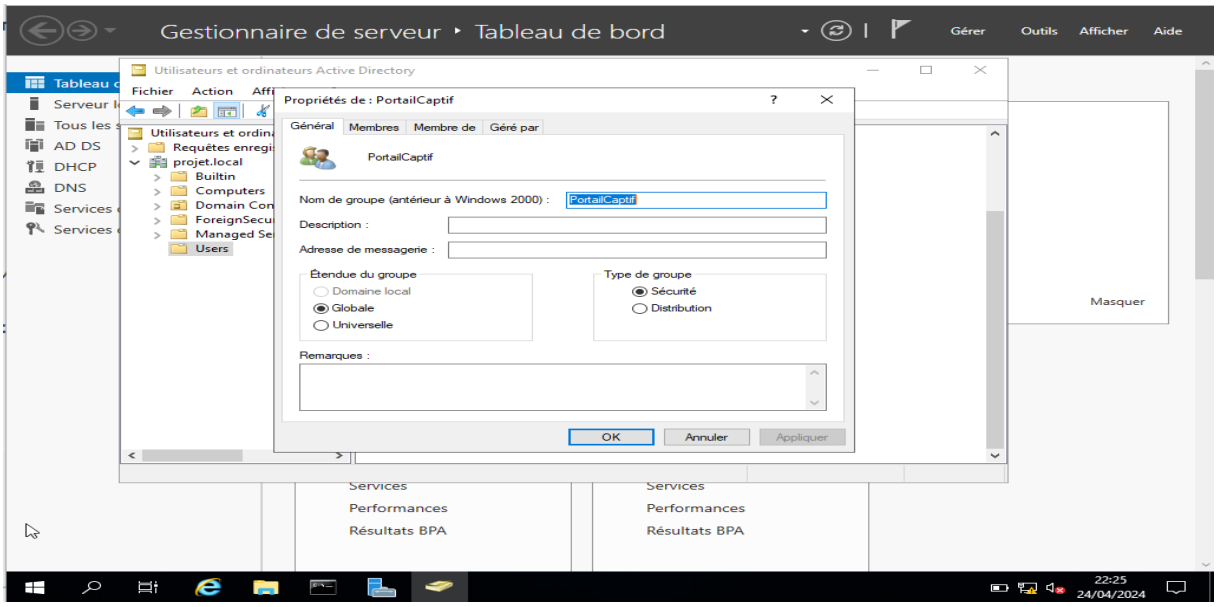


Figure : création de groupe

Créons ensuite un utilisateur et affectons le au groupe que nous venons de créer

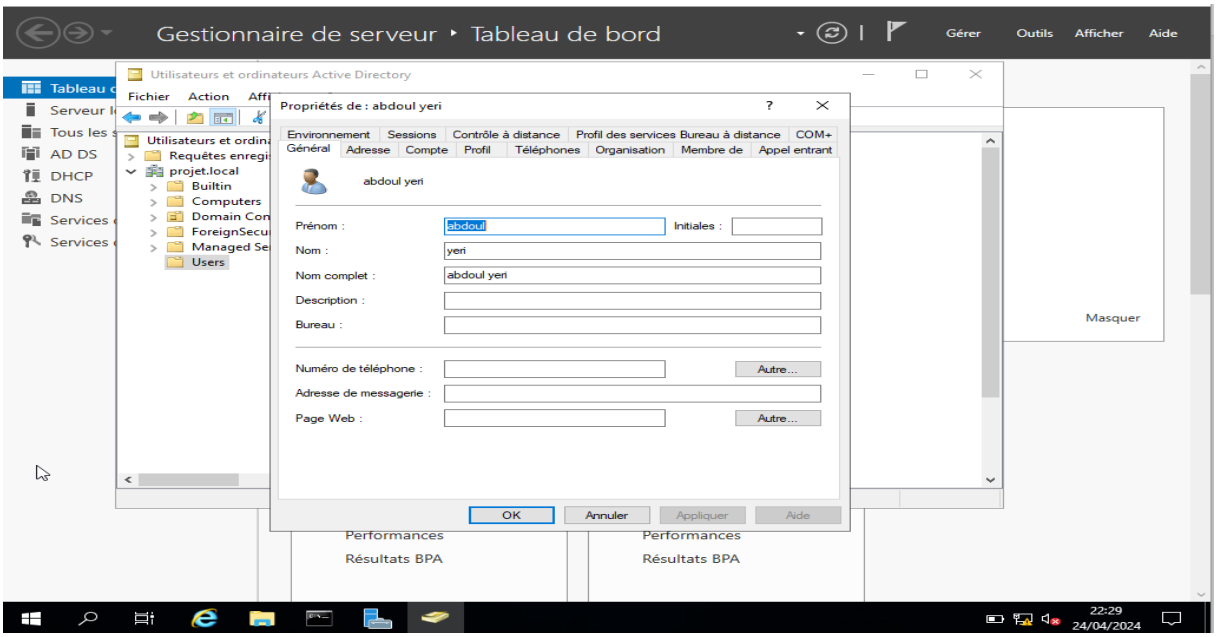


Figure : création utilisateurs et affectation au groupe

1. Installation

Nous allons maintenant installer le **rôle NPS** pour *Network Policy Server = Services de stratégie et d'accès réseau.*

- Ouvrir le gestionnaire de serveur et cliquez sur **Gérer > Ajout des rôles et fonctionnalités**
    - **Cliquez sur suivant x3**
    - Cochez le case : **Services de stratégie et d'accès réseau**
    - Une fenêtre apparaît, **cliquez sur ajoutés les fonctionnalités**

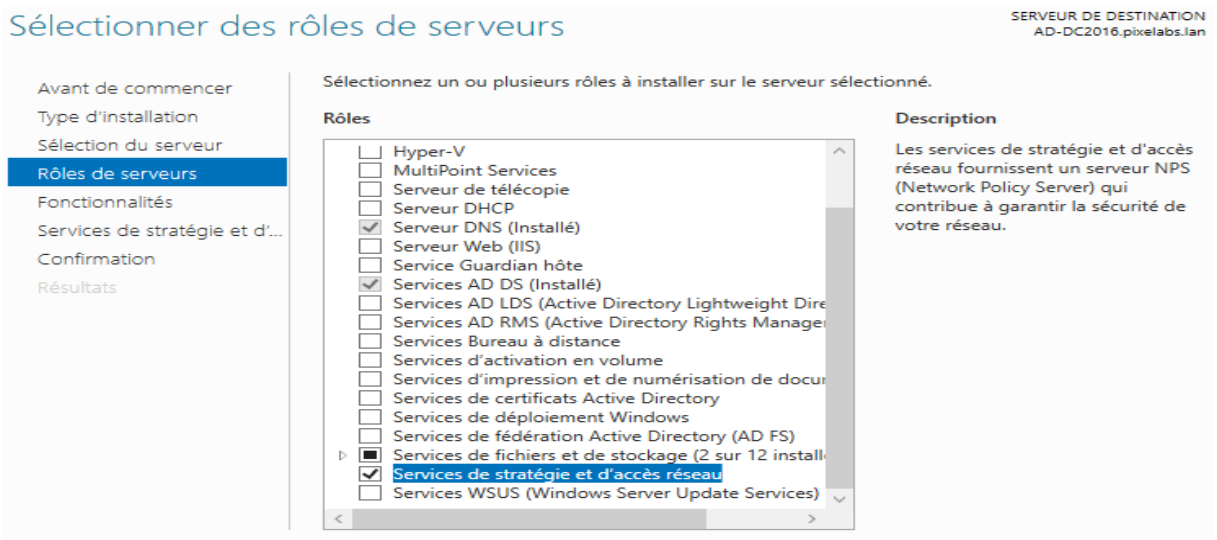


Figure : Installation

Ensuite **Cliquez sur suivant 3 fois et Cliquez sur Installer pour terminer**

2. Configuration Rôle Serveur RADIUS

Une fois l'installation du rôle terminé, lancez la console d'administration du serveur NPS.

- 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**

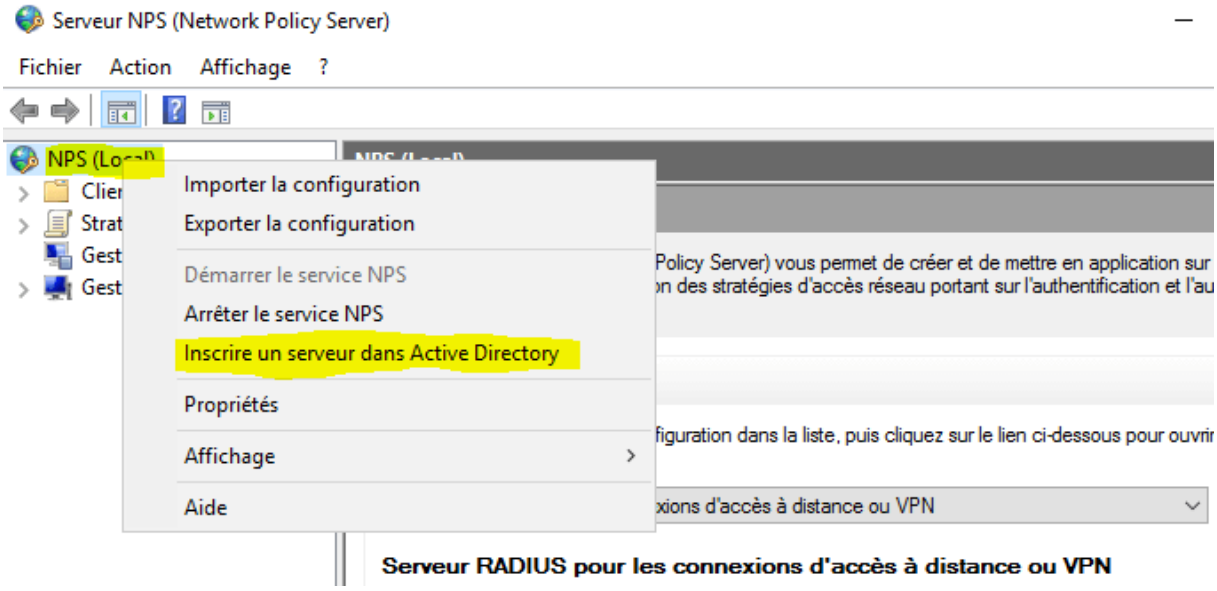


Figure : inscription du serveur dans active directory (Confirmer en cliquant sur **OK 2 fois**)
Nous allons commencer par mettre en place un nouveau client RADIUS.

- Allez dans Client et serveurs **RADIUS** (sous NPS (Local))
    - Effectuer un clic-droit sur **Client RADIUS > Nouveau**
    - Nom convivial : **CaptivePortal**
    - Adresse IP : **192.168.10.15** *(Adresse IP de l'interface DMZ de pfSense)*

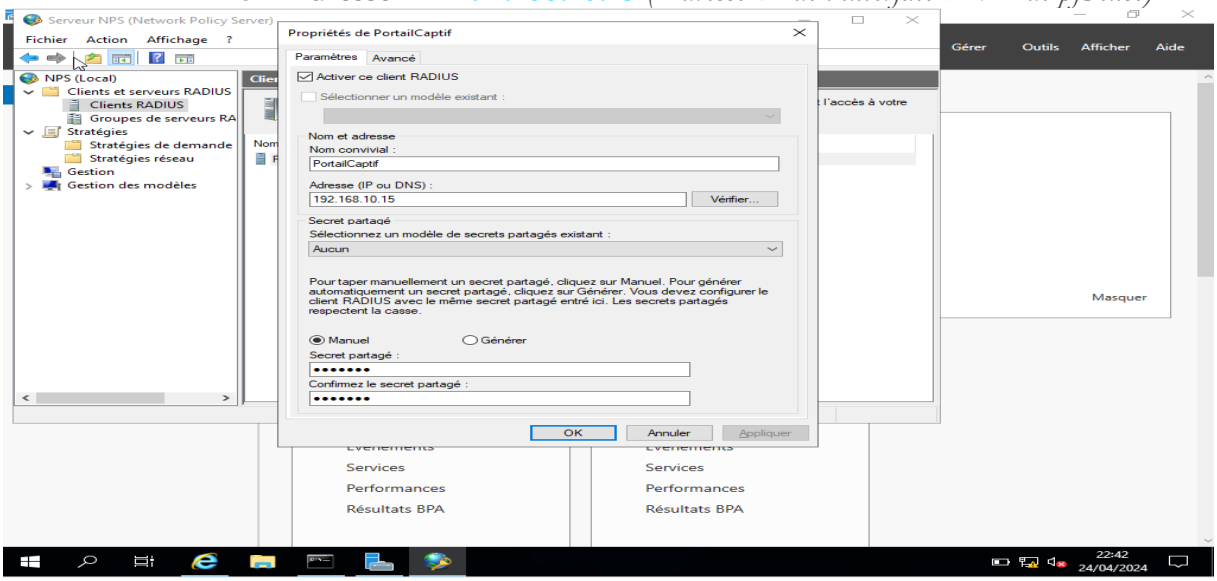


Figure : creation d'un client radius

- Ajouter un **secret partagé (à retenir)**

Nous allons maintenant donner l'autorisation aux utilisateurs. Dans notre cas, il faut donc ajouter le groupe de sécurité **PortailCaptif** et tous les utilisateurs appartenant à ce groupe auront l'autorisation.

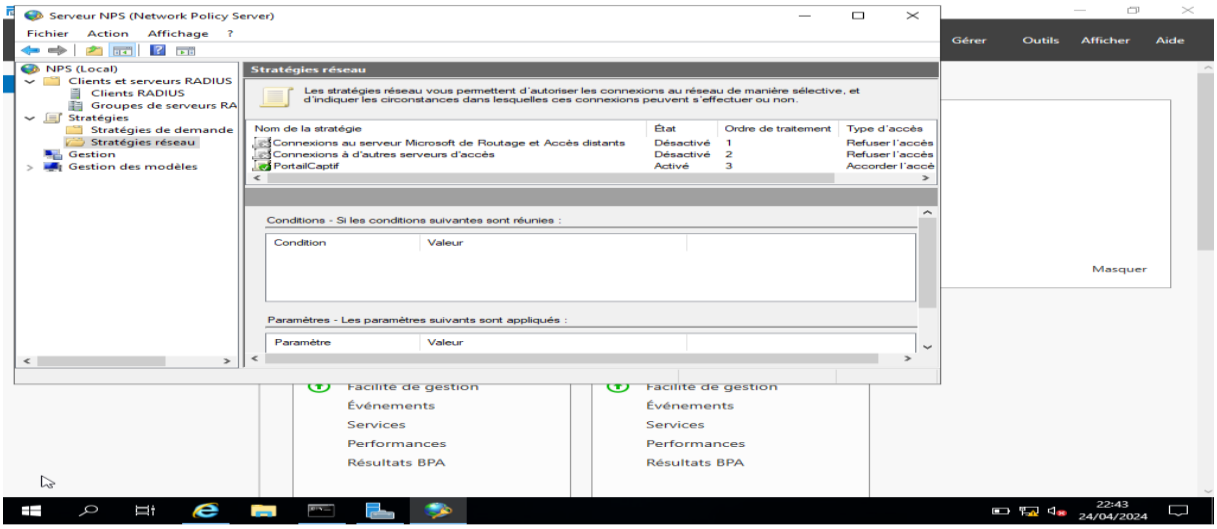


Figure : configuration de la stratégie réseau

Chapitre 4 : Réalisation

- ✓ Portail captif pfsense avec authentification radius

Un portail captif : est une structure permettant un accès rapide à Internet. Lorsqu'un utilisateur cherche à accéder à une page Web pour la première fois, le portail captif capture la demande de connexion par un routage interne et propose à l'utilisateur de s'identifier afin de pouvoir recevoir son accès. Cette demande d'authentification se fait via une page Web stockée localement sur le portail captif grâce à un serveur HTTP. Ceci permet à tout ordinateur équiper d'un navigateur HTML et d'un accès Wifi de se voir proposer un accès à Internet. Les identifiants de connexion (identifiant, mot de passe) de chaque utilisateur sont stockés dans une base de données qui est hébergée localement ou sur un serveur distant.
Une fois l'utilisateur authentifié, les règles du Firewall le concernant sont modifiées et

celui-ci se voit alors autorisé à utiliser son accès pour une durée limitée fixée par l'administrateur. A la fin de la durée définie, l'utilisateur se verra redemander ses identifiants de connexion afin d'ouvrir une nouvelle session.

Pour la mise en place du portail captif, nous irons sur pfsense

Activer le DNS Resolver

Allez dans le menu **Services > Résolveur DNS > Paramètres généraux**

- ☑ **Activer les résolutions DNS**
  - Interface réseau : **Tout**
  - Interfaces réseau sortantes : **Tout**
  - ☑ Activer le support DNSSEC
  - ☑ Enregistrer les bails DHCP dans le résolveur DNS
  - ☑ Enregistrez les mappages statiques DHCP dans le Résolveur DNS
- Tout le reste est par défaut.
- Cliquez sur **Enregistrer et Appliquer les paramètres**
-

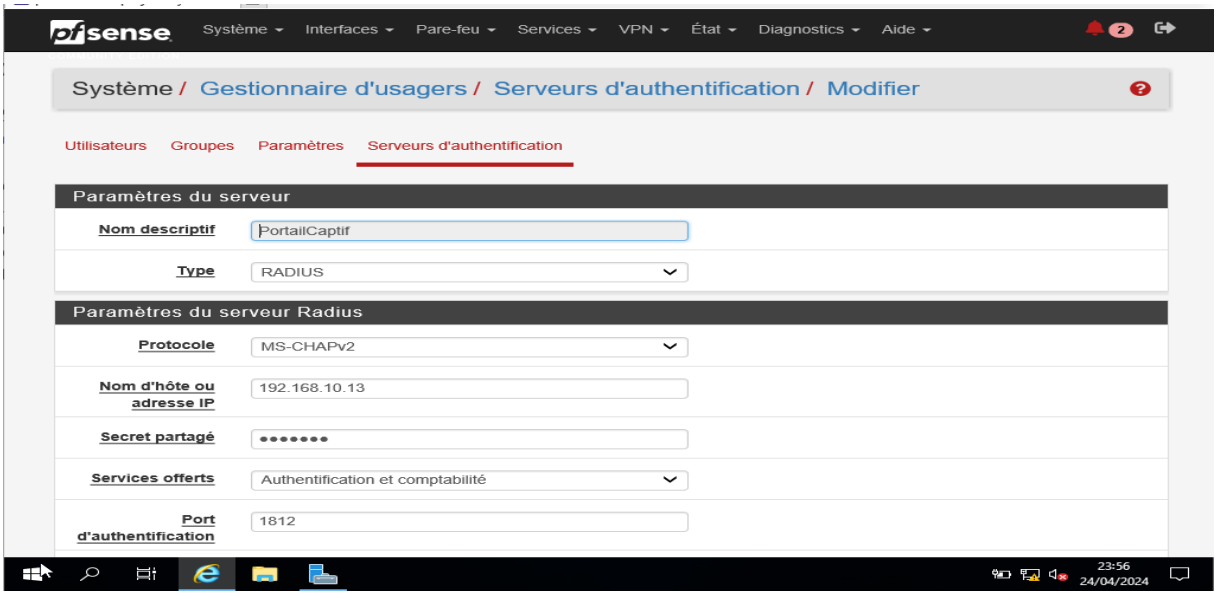
Figure :

Configuration Serveur d'Auth RADIUS

Allez dans le menu : **Système > Gestionnaire d'usagers > Serveurs d'authentification**

- Cliquez sur Ajouter
  - Nom descriptif : **PortailCaptif**
  - Type : **RADIUS**
  - Protocole : **MS-CHAPv2**
  - Nom d'hôte ou adresse IP : **192.168.10.13** *(Adresse du serveur RADIUS, c'est-à-dire Windows Server 2019)*
  - Secret partagé : *ce que vous avez mis lors de l'activation du client RADIUS sous Windows*
  - Service offerts : **Authentification et comptabilité**

- Port d'authentification : **1812**
- Port de comptabilité : **1813**
- Délai d'expiration de l'authentification : *par défaut c'est 5 secondes*
- **Attribut IP RADIUS NAS : LAN – 192.168.10.15**



Figure

Configuration Portail Captif

Allez dans le menu **Services > Portail Captif > Ajouter**

- **Nom de la zone : PortailCaptif**
- **Description de zone : PortailCaptif**
- **Enregistrer et poursuivre**

☑ **Activer le Portail Captif**

- Interfaces : **LAN**
- ☑ **Activer la fenêtre de dialogue de fermeture de session**

- Allez dans la partie **Comptabilité**
  - ☑ **Send RADIUS accounting packets.**
  - Accounting Server : **CaptivePortal**
  - Send accounting updates : **Aucune mise à jour**

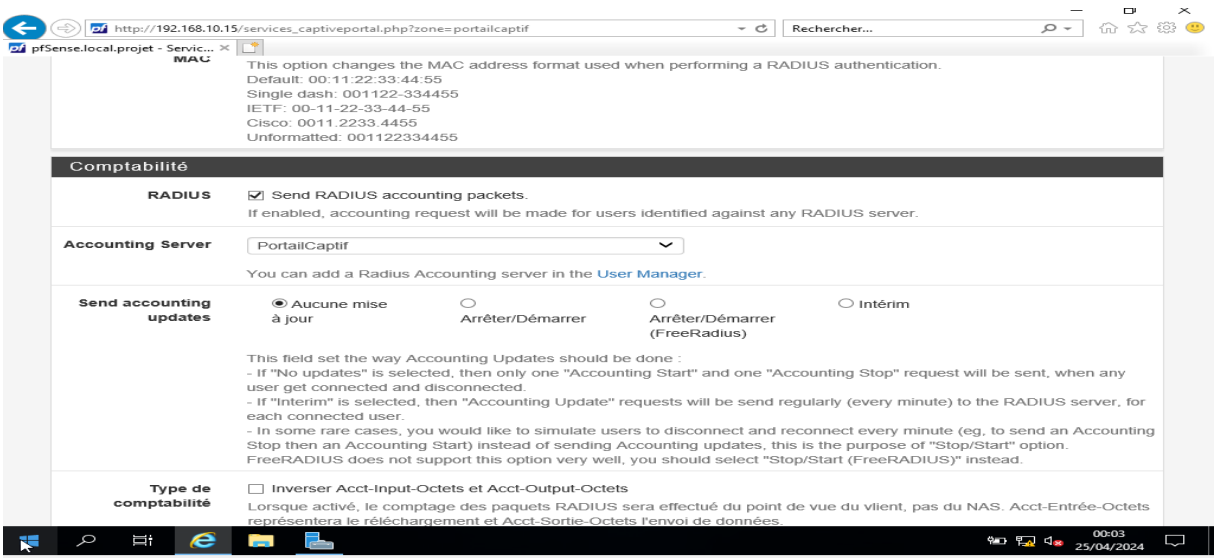


Figure :

Enfin appuyer sur enregistrer.

Test portail captif

Voici la configuration de notre Virtual Machine de test Windows 10 *(considérée comme un smartphone/ tablette ou un PC portable).*

- **Elle est connectée sur l'interface du portail captif (LAN)**
- **Configuration réseau manuelle sur la meme plage d'adresse que pfSense.**
- **Elle ne fait pas partie du domaine AD**

il suffit juste de taper https://tiktok.com dans votre navigateur et vous serez rediriger vers la page d'authentification du portail captif

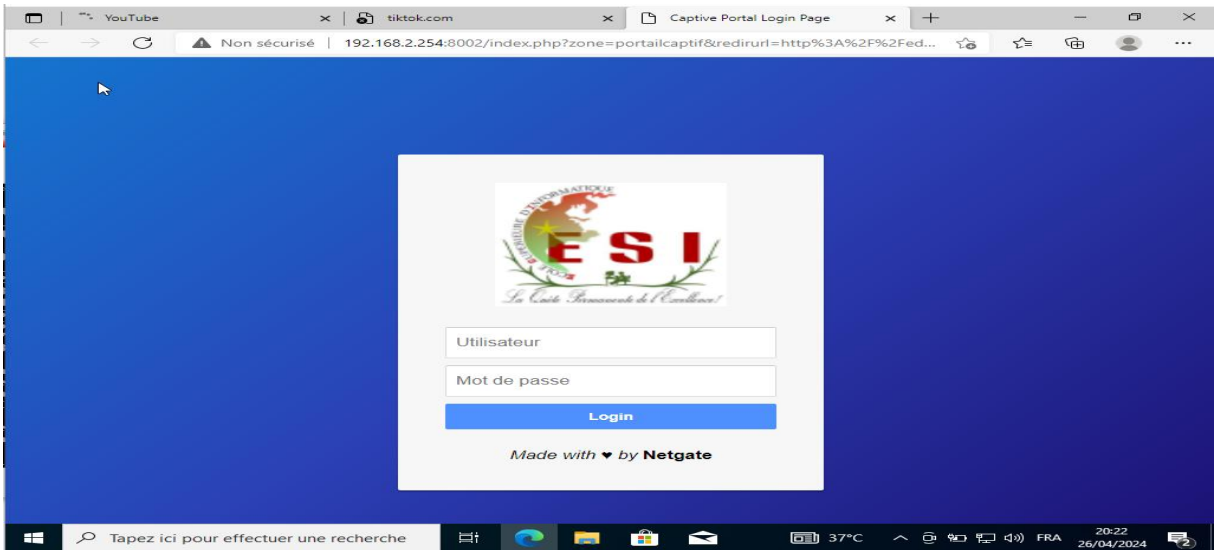


Figure : portail captif

Après authentification grace au identifiants crées sur radius server, on se connecte et on a la possibilité d'aller vers notre recherche

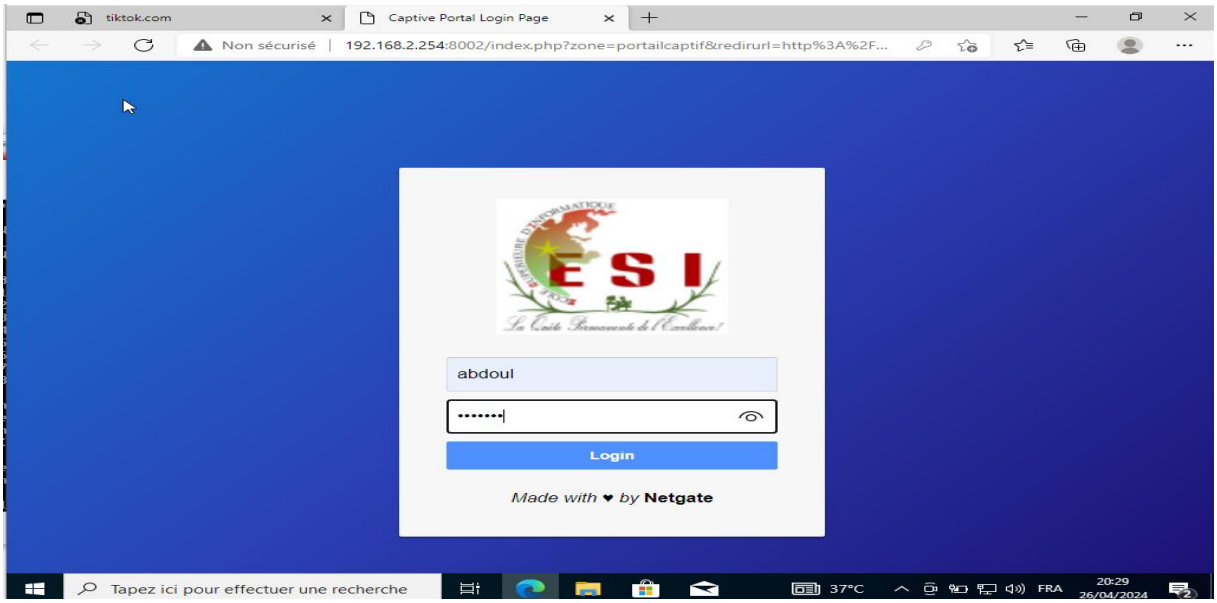


Figure : remplissage des identifiants

Enfin l'utilisateur pourra se rendre sur internet et effectuer ses recherches.

- ✓ **Filtrage**

D'autre part, grâce à l'utilisation d'un Pare-feu, il est possible d'assurer un suivi des connections via la constitution des journaux d'activités (logs) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.
Il est ainsi possible de **filtrer les connexions** à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs.
Le filtrage basé sur l'adresse des ressources consultées est appelé **filtrage d'URL.**
Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de **liste blanche**, lorsqu'il s'agit d'une liste de sites interdits on parle de **liste noire**.
En fin l'analyse des réponses des serveurs conformément à une liste de critères (motsclés….) est appelée **filtrage de contenu.**

Ainsi nous allons créer des allias avec une liste de site à bloquer (nom de domaine et adresses IP) et les différents VLANs (étudiants, Personnels et Techniciens)
Pour cela nous allons au niveau de l'onglet règle de l'interface de pfsense et selectionner allias dans le menu déroulant pour la création des allias.

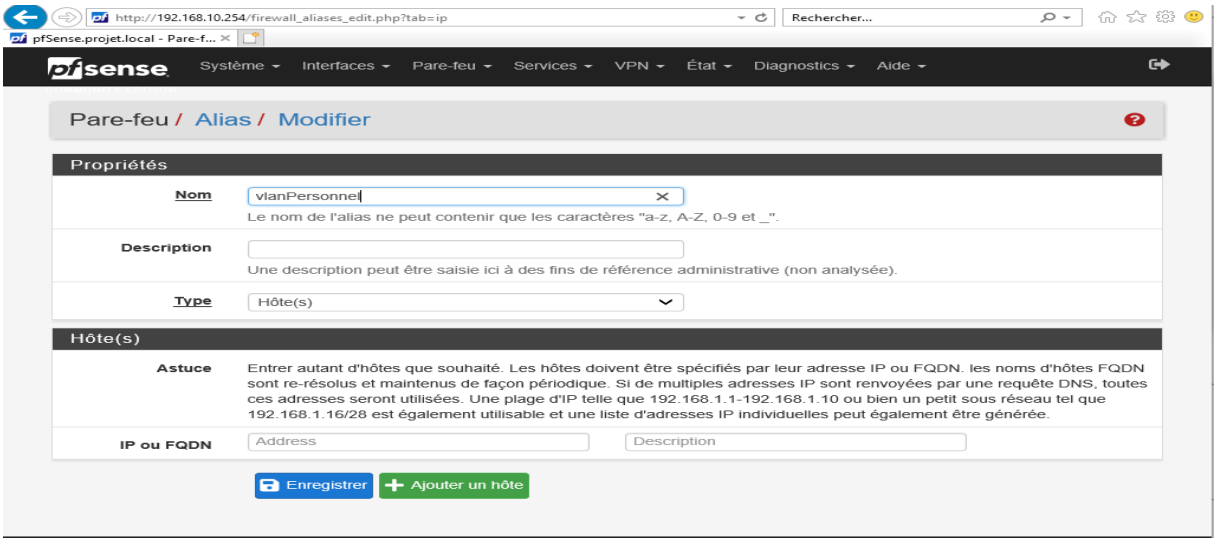


Figure : creation de vlans

Attribution des adresses ip à chaque vlan puis application des resultats

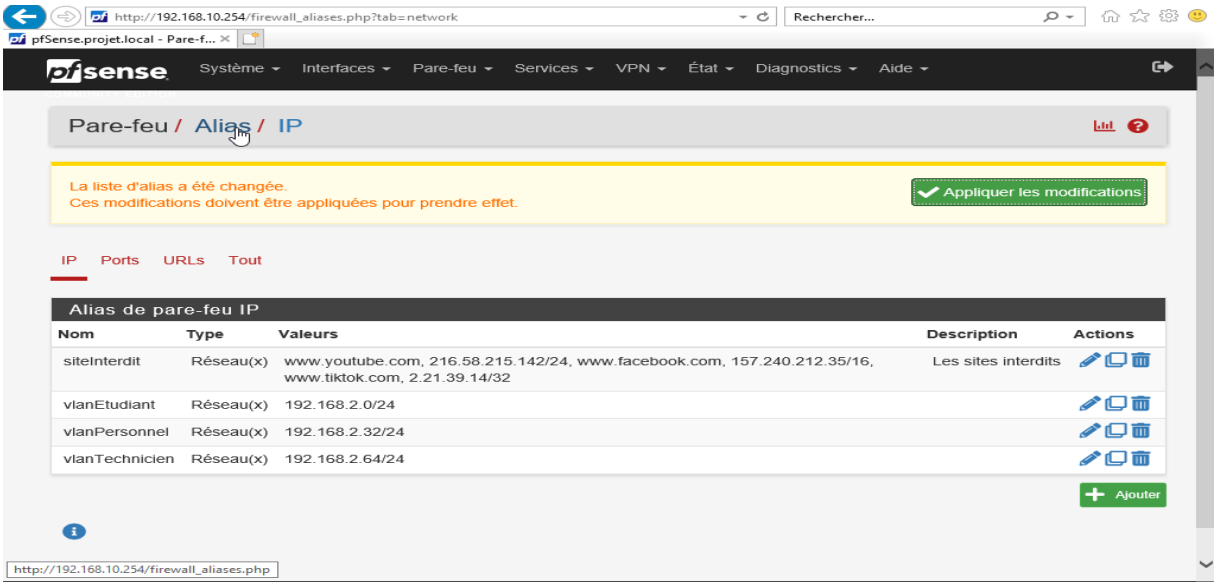
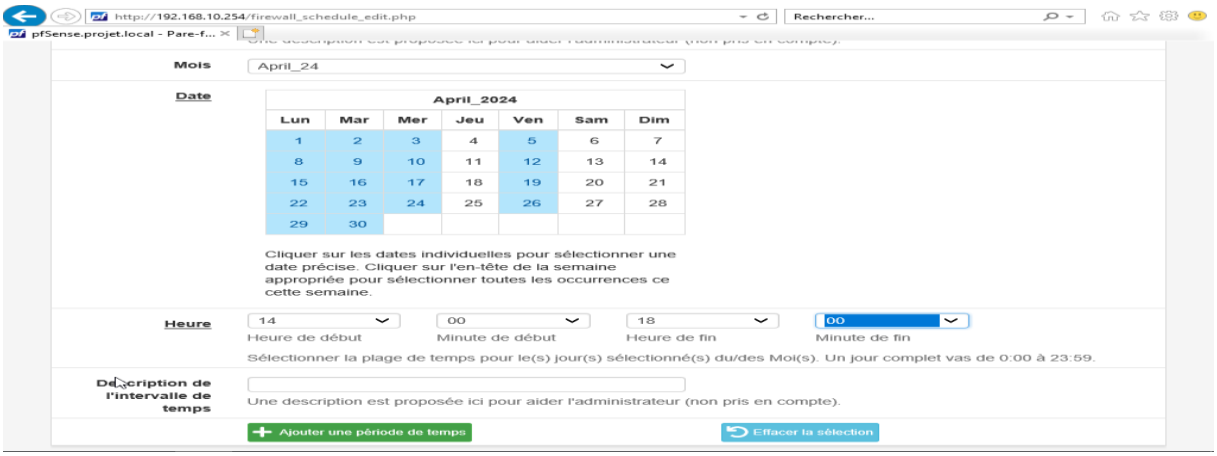


Figure : recapitulatif des allias

A travers le planning nous allons mettre en places les heures et jours où les etudiants n'auront pas accès à ses sites que nous voudrons bloquer



Figures : planning des horaires de blocage

Nous allons par la suite créer des règles en utilisant ces allias

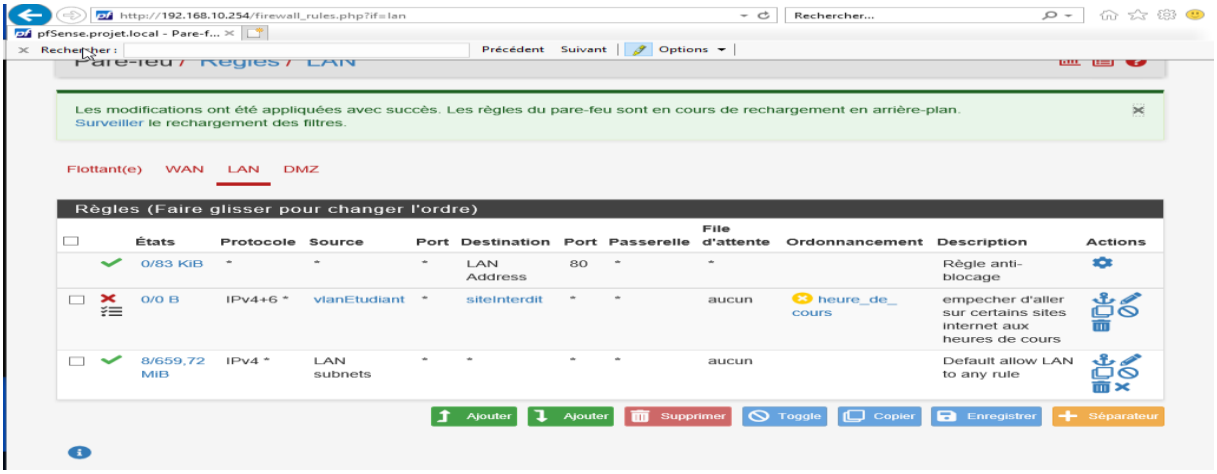


Figure : mise en place de filtrage web

Test filtrage

Enfin nous allons tester cela sur notre vlan etudiant. La machine windows cliente a été configurer sur la meme plage d'adresse que celui du vlan Etudiant

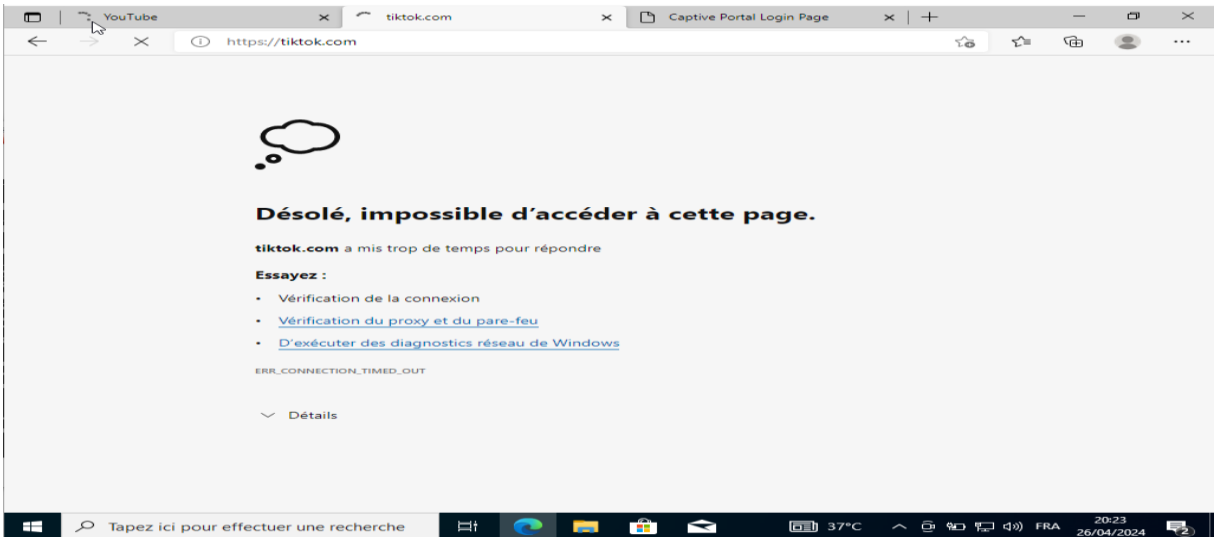


Figure : connexion impossible

Apres authentification, une requete venant du vlan etudiant vers www.tiktok.com ou www.facebook.com ou www.youtube.com aux heures de cours ne passeront pas.

Nous avons verifier le bloquage à travers à l'aide de la journalisation système sur pfsense dans le menu état.

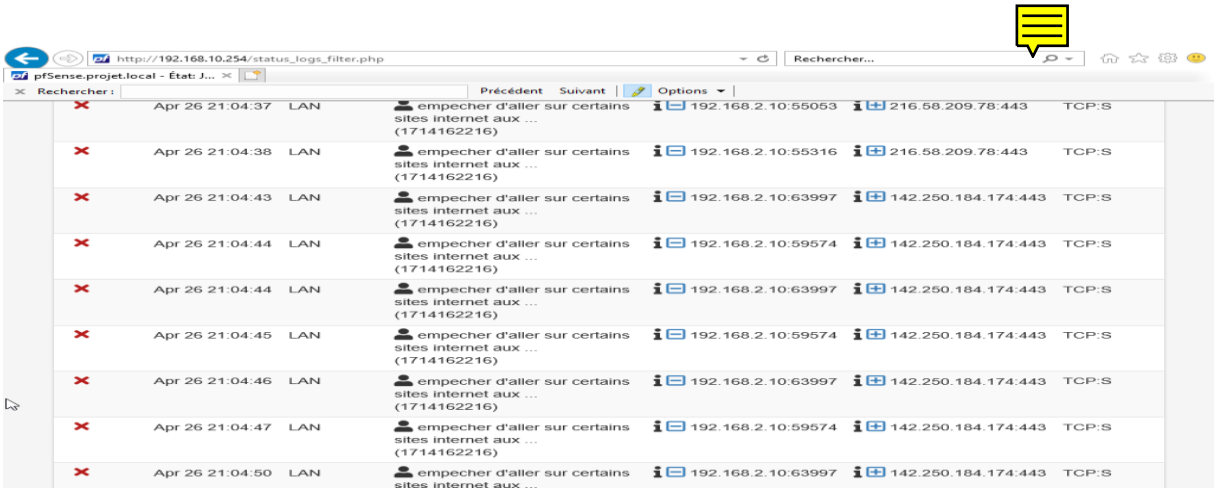


Figure : requete provenant du lan vers youtube bloqué

Perspectives futurs

D'autres fonctionnalités avec le rajout des packages (exp: le paquet SNORT pour la détection et la prévention d'intrusion réseaux),
Configuration d'autres services (exp: vlans virtuelles, traffics shaper),
Ce travail gagnerait davantage une fois le pare-feu testé sur des réseaux réels.

Conclusion

Un pare-feu donc a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés ou interdits.

Les recherches pour faire évoluer les technologies de filtrage sont nées du besoin de sécuriser les échanges réseaux. Pour améliorer ce filtrage il a été nécessaire de remonter dans les couches OSI, ce qui a été rendu possible grâce à une technologie logicielle et matérielle de plus en plus rapide.

Comme on peut le constater, les firewalls possèdent de multiples capacités qui peuvent différer en fonction de leurs types. Cette multitude de solutions impose donc une étude rigoureuse de la sécurité devant être mise en place.

Dans notre travail dont le thème était **mise en place et deploiement d'un pare-feu**, nous avons mis en place un firewall open source « PfSense »
sous Virtualbox qui permet de faire office de firewall et de routeur. Au delà de ça, il offre beaucoup de fonctionnalités très poussées comme : le NAT, le DHCP etc. De plus, l'ajout de packages (Paquets) permet à PfSense d'être totalement modulable et d'agrandir encore plus son panel de fonctionnalités. Dans notre projet nous avons ajouté (installer et configurer) le serveur radius pour l'authentification des utilisateurs au niveau du portail Captif , les allias et règle afin de permettre le **filtrage d'URL**.