Installation d’un serveur d’authentification

Sommaire:

I) Introduction.
II) Solution utilisée.
III) Mise en place de la solution
IV) Conclusion

I) Introduction:

En tant que prestataire gérant l’infrastructure réseau et matériel d’entreprises nous aurons ici comme mission de mettre en place un service d’authentification pour une association. Celle-ci met à disposition une salle informatique à libre disposition pour ses adhérents. Les adhérents uniquement doivent avoir accès au réseau qui leur est mit en place. Pour empêcher d’autres individus d’y avoir accès, en essayant de se brancher au prises avec un autre pc, par exemple, nous mettrons en place un portail captif avec authentification, celui-ci contiendra une liste d’utilisateurs qui seront autorisés à se connecter au réseau.

II) : Solution utilisée: pfSense

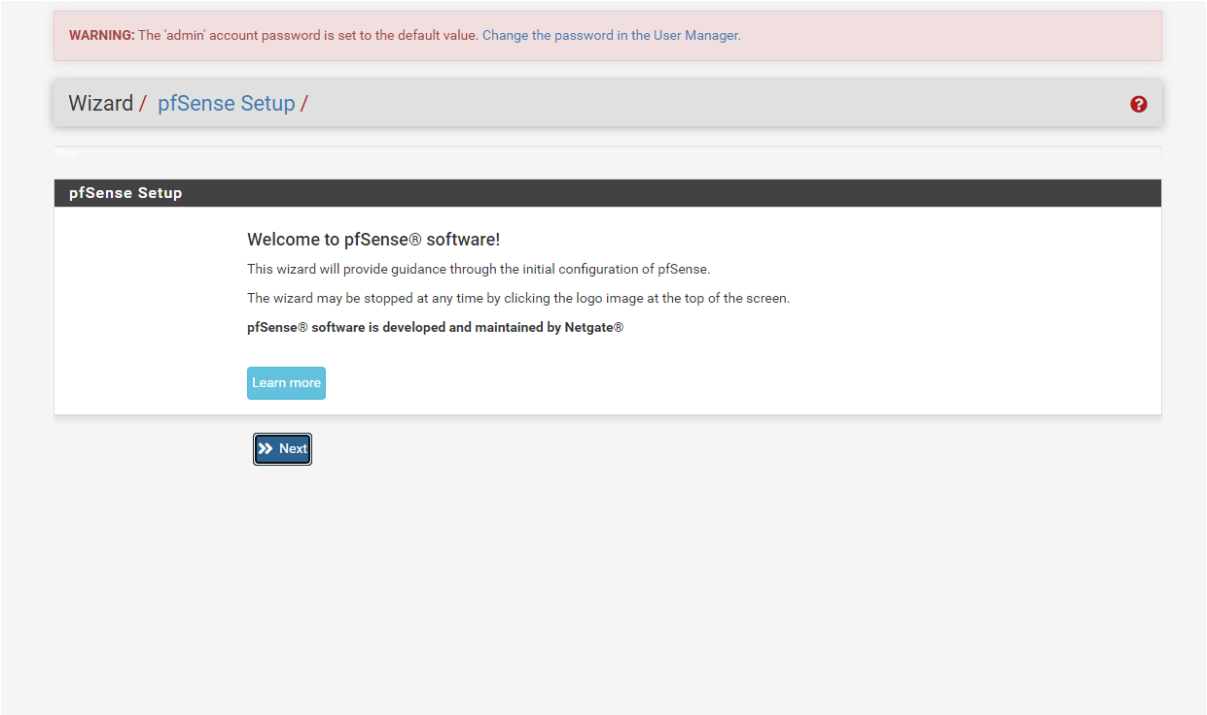
pfSense est un pare-feu open source basé sur FreeBSD. Nous pourrons y configurer un portail captif. Le portail captif force les clients d’un réseau à afficher une page Web d’authentification avant de pouvoir se connecter à Internet. Il est utilisé dans des réseaux qui assurent un accès public tels que les espaces d’accueil, établissement scolaire. Cette solution est parfaite dans notre situation.

III): Mise en place de la solution.

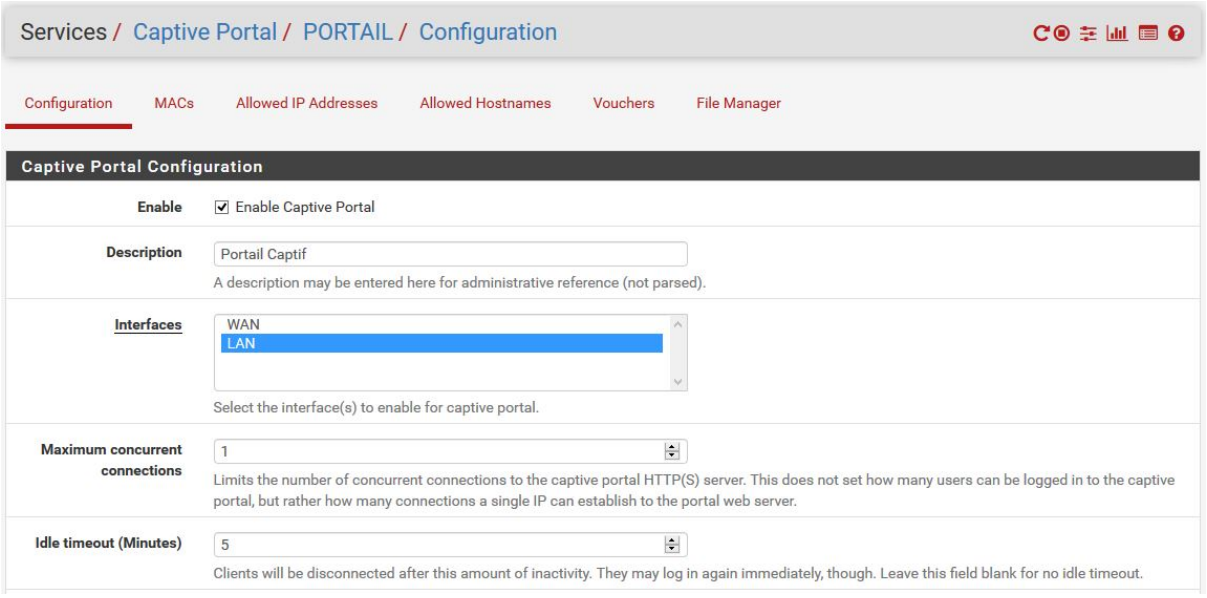
Dans notre cas, nous disposons de deux cartes internet. Une sera connectée au réseau de la salle avec une adresse en 192.168.x.x. L’autre sera relié à un switch qui simulera notre situation dans un réseau en 172.30.1.1 sur lequel le pare-feu sera configuré.

Nous installerons est paramétrons la machine virtuelle pfSense sur VirtualBox dont le commutateur sera donc relié à notre deuxième réseau en 172.30.1.0. Ici l'installation de pfSense sur VirtualBox ne présente aucunes difficultés particulières. Les interfaces WAN et LAN sont préconfigurées avec des adresses standards. On peut modifier les paramètres des deux interfaces depuis le shell ou définir nos propres adresses par exemple.
Il n'est pas conseillé de modifier les paramètres du réseau WAN car il est directement géré par VirtualBox.

Une fois la VM installée nous pouvons accéder au portail de web de configuration de pfSense via l'adresse WAN:



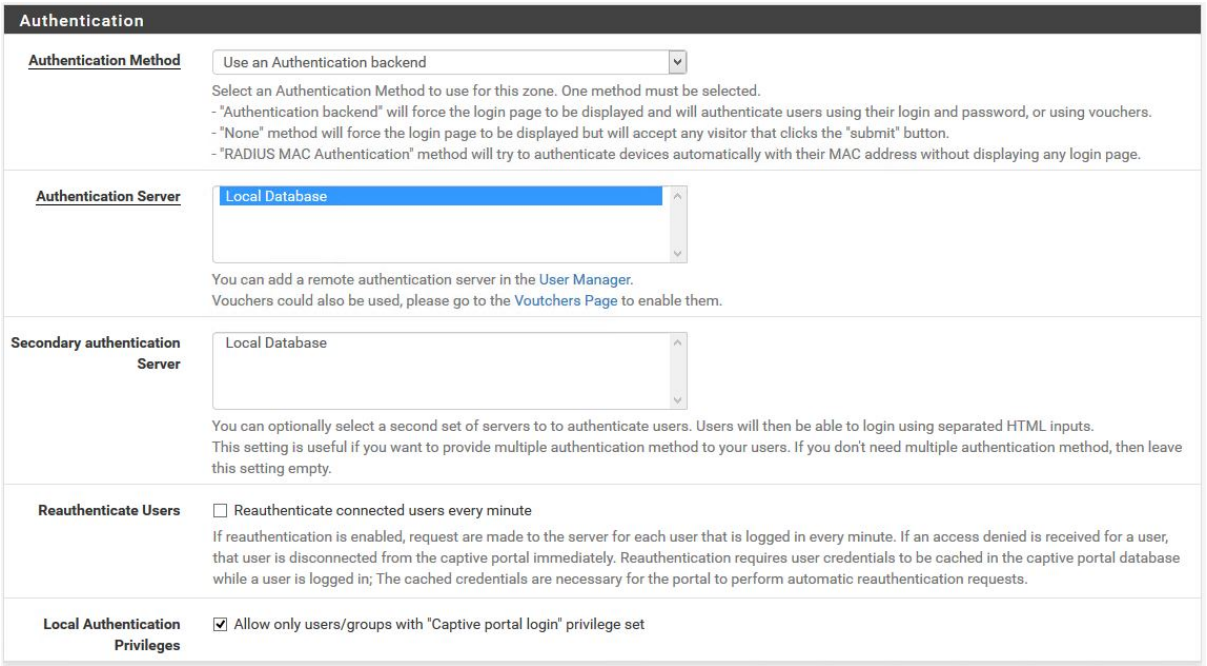
pfSense Setup vas nous faire passer sous quelques étapes de configuration, rien de capital pour la suite du projet.



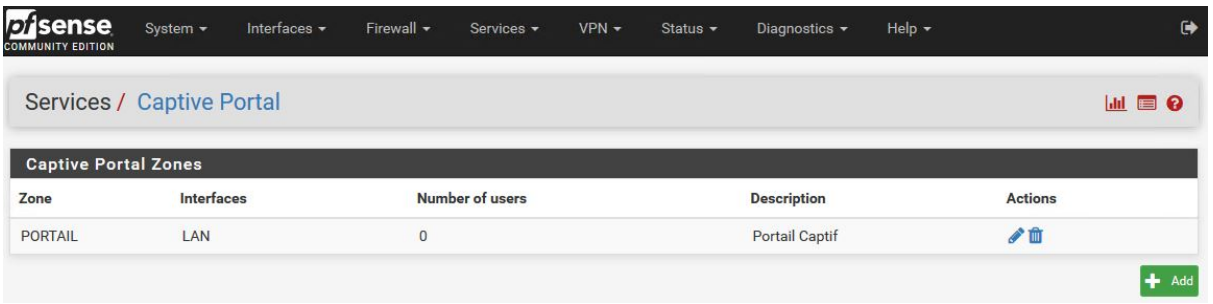
Activation du portail captif sous services/captive portal/portail/configuration: Bien choisir LAN!!

-Sélectionner « **Local Database** » pour « Authentication Server ». Mais ne pas sélectionner l'option pour l'authentification sur le serveur secondaire.

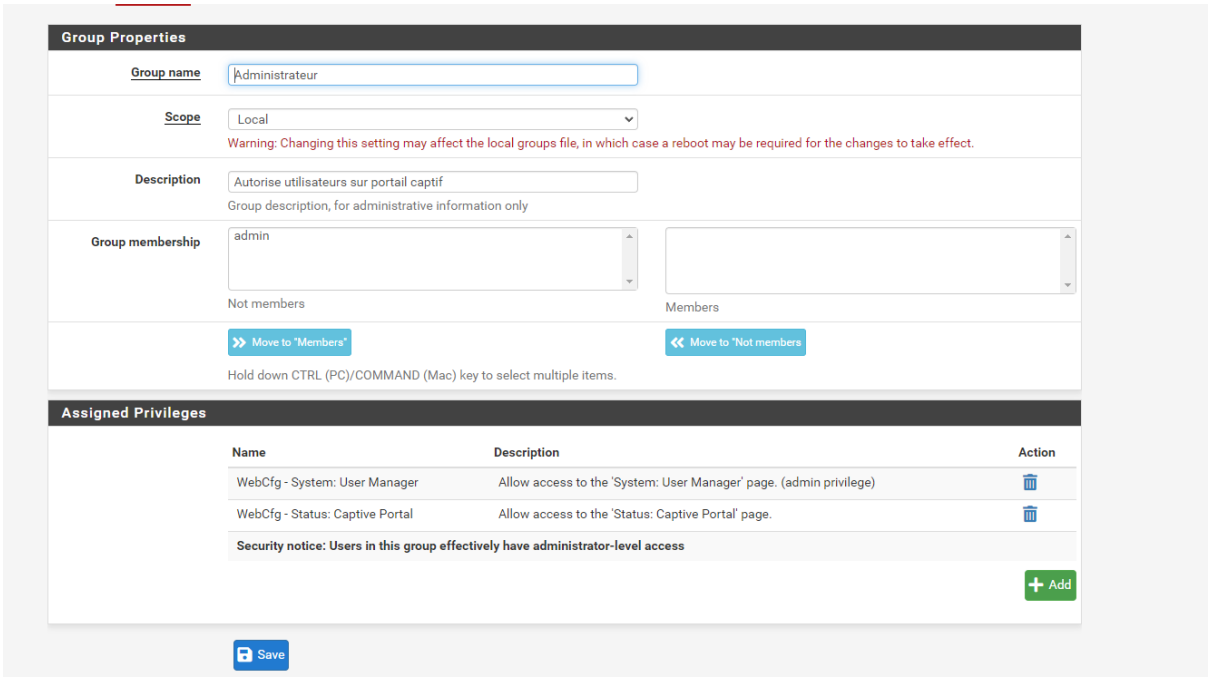
-Sélectionner « **Use an Authentication backend**«



Notre portail est créé:

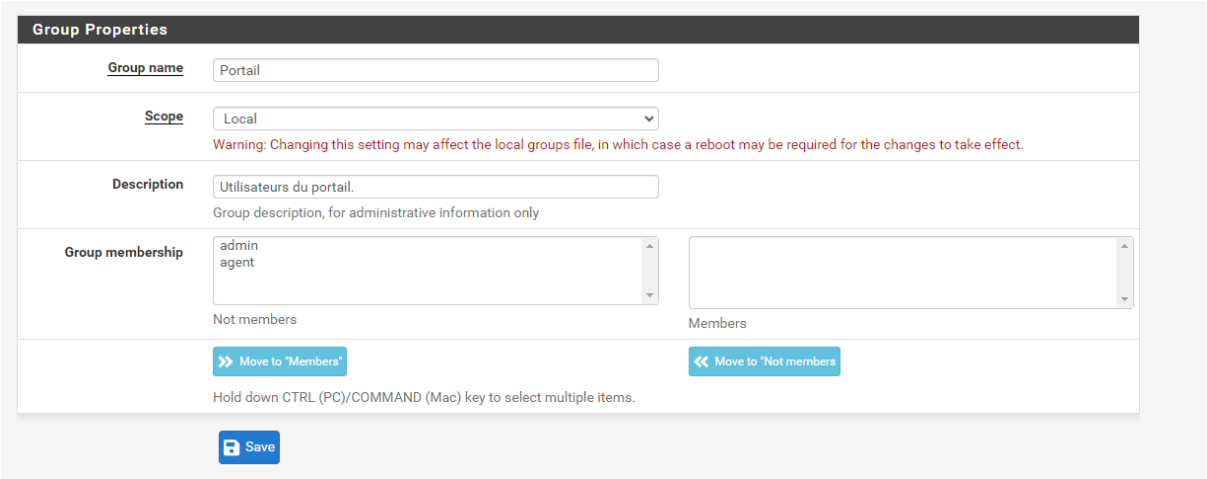


Nous créerons un groupe d'administrateurs qui pourra gérer les utilisateurs du portails et ses différents paramètres:

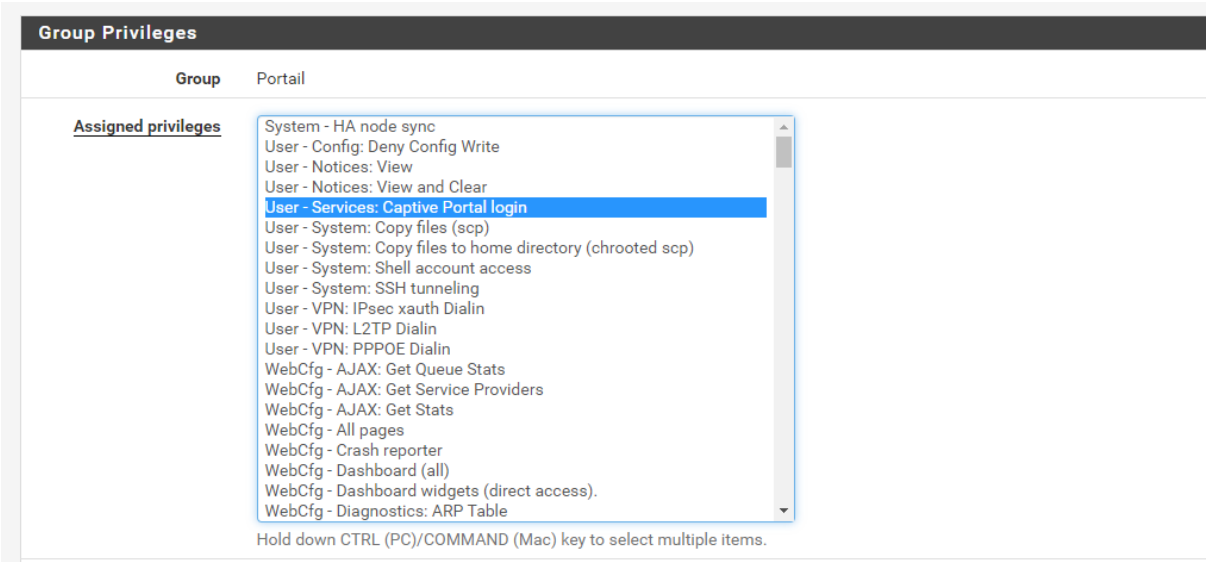


Configuration du Groupe et des Utilisateurs autorisés a se connecter au Portail Captif:

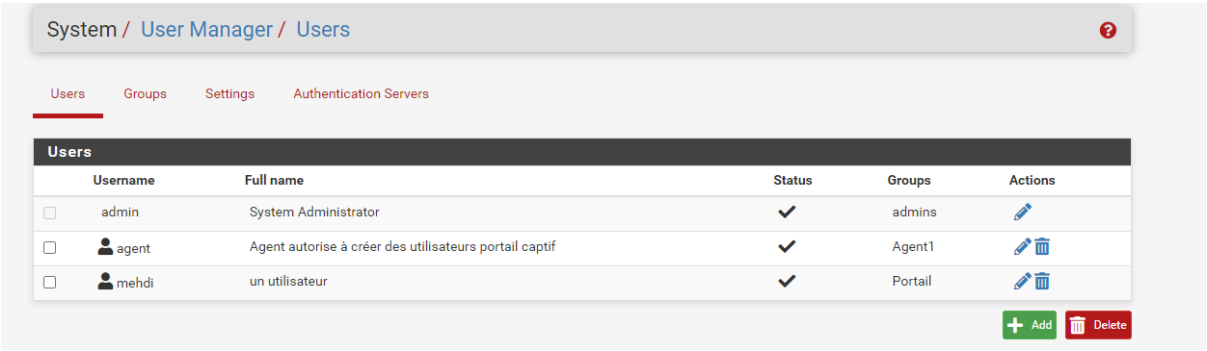
Nous allons ensuite créer le GROUPE du portail captif:



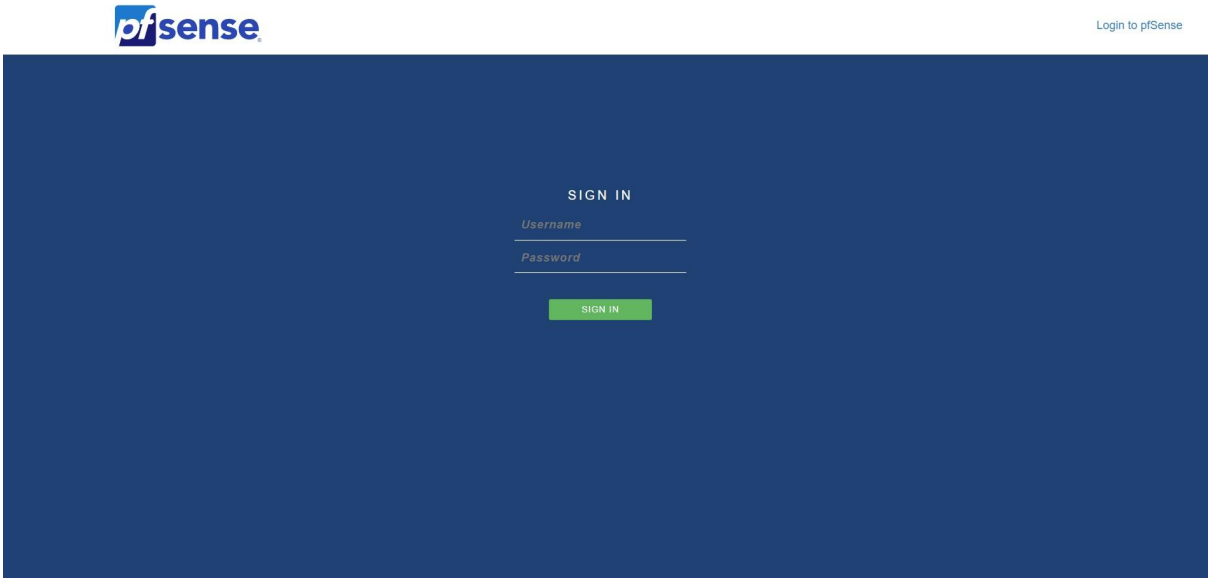
Nous y installerons le service de portail captif:



Nous avons créé un utilisateur (mehdi+mot de passe) qui fera bien parti du groupe portail:



L'utilisateur admin par exemple pourra se connecter via cette interface web réservé au administrateurs:



Pour qu’un utilisateur lambda se connecte, il lui suffira d'ouvrire une page web (sur le réseau LAN) et un portail captif de connexion devrait apparaître. Si il a été ajouté précédemment par un administrateur au groupe portail, il devrait pouvoir alors accéder au réseau de la salle.

IV)Conclusion:

Je n’ai malheureusement pas réussi à me connecter au portail pour les utilisateurs, malgré le fait d'être bien sur le réseau LAN avec une bonne adresse, un dhcp activé qui distribue de bonnes adresses. Après vérification, les connexions aux différents ports ethernet et prises sont également correctes.. Le portail captif n’est donc pas achevé, il nous manque cette dernière étape d’apparition de la page web.

Allag
Mehdi,

Les règles à admirer pour mettre en place un réseau public sont les suivantes
 Les établissements accueillant des enfants de moins de 3 ans sont interdits de mettre en place un
 wifi public.
 Il est nécessaire de déclarer l'ouverture du réseau à l'ARCEP conformément à l'art.L.32 de la loi sur les postes et les
et des envois électroniques. L'ARCEP est une autorité exécutive indépendante qui assure la

régulation des secteurs des dépêches
Les associations assimilées à des caffs
ou les aérodromes doivent si elles proposent un accès public à Internet
elles doivent également conserver des données spécialisées similaires à une adresse IP qui permet d'identifier l'utilisateur.
Semblable à une adresse IP qui permet d'identifier un appareil sur Internet ou la durée de chaque
connexion.
encore, des informations sur le contenu des dépêches, comme le corps d'un e-mail ou les URLs
encore, les informations sur le contenu des dépêches, comme le corps d'un courrier électronique ou les URL consultées sur un site web, ne doivent pas être conservées.
Ils doivent collecter des données professionnelles pour une période déterminée et ne les communiquer qu'aux personnes suivantes
uniquement aux personnes autorisées par la loi, notamment les autorités judiciaires dans le cadre d'un

Cette obligation de conservation des données professionnelles résulte de la loi sur la sécurité diurne de 2001 et de la loi sur la protection de la vie privée.
Cette obligation de conservation des données professionnelles résulte de la loi de 2001 sur la sécurité quotidienne et de la loi de 2006 sur la lutte contre le terrorisme.

Ils ont une obligation de couverture du réseau public, ils doivent donc mettre en place
un système de filtrage à l'entrée afin de lutter contre les téléchargements illégaux et la publication d'images choquantes.

Selon la CNIL, les entreprises et les administrations qui offrent un accès à Internet à leurs travailleurs ne sont pas concernées par cette obligation de conservation. néanmoins, un employeur a la possibilité de mettre un dispositif de surveillance sur ses travailleurs pour voir leur effort comme par exemple pour savoir quels sites web ont été visités par le travailleur.Toutefois, les travailleurs doivent être informés mais la CNIL doit également être informée de la mise en place de ce type de dispositif.

Les conséquences du non-respect de ces règles sont les suivantes

Une confiscation de 75 000€ et 1 peine d'emprisonnement pour une personne physique est représentée comme étant une seule et même personne.

Une confiscation de 350 000€ pour une personne morale, une personne morale est un groupe de personnes physiques qui se réunissent pour négocier un projet commun

https://blog.matrixpost.net/set-up-a-radius-server-on-windows-server-2019-for-802-1x-wireless-connections/

https://docs.pulsesecure.net/WebHelp/PPS/5.4R3/Content/PPS_Admin_Guide_5.4R3/MAC_Address_Authentication.htm

https://techexpert.tips/fr/ubuntu-fr/ubuntu-radius-authentication-a-laide-de-freeradius/

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Wi-Fi-Cloud/manage_wirelessmanager/configuration/wifi_access/radius_mac_auth.html

https://openclassrooms.com/fr/courses/2557196-administrez-une-architecture-reseau-avec-cisco/5135511-mettez-en-place-un-serveur-radius

https://www.alliedtelesis.com/sites/default/files/documents/how-alliedware/c613-16053-00-a1.pdf

https://techexpert.tips/ubuntu/ubuntu-radius-authentication-freeradius/

https://fr.slideshare.net/JeffHermannElaAba/mise-en-place-dun-serveur-radius

https://blog.devensys.com/introduction-authentification-reseau-802-1x/

database name: datamed
mdp: helloworld
user: mehdi