

Portail captif (PfSense) :

Sommaire :

Mise en place de PfSense	2
Installation de PfSense.....	2
Configuration de PfSense	6
 Mise en place du portail captif	 8
Configuration de base du portail captif	8
Authentification local	9
Authentification avec RADIUS	12

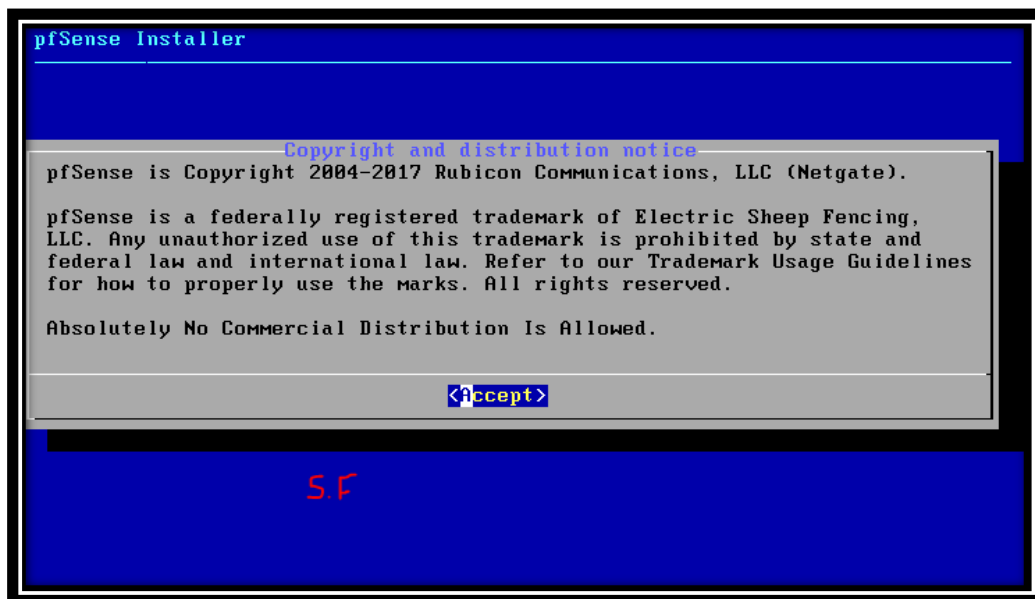
I. Mise en place de PfSense:

1. Installation de PfSense :

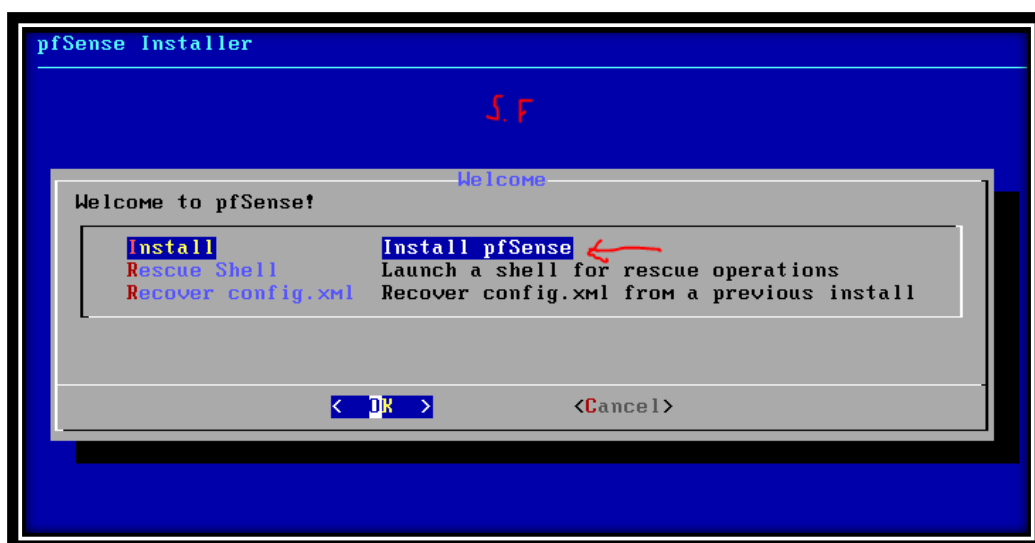
J'ai créé une machine virtuelle PfSense sur VMware. On peut trouver l'iso de cette dernière sur le site officiel <https://www.pfsense.org/>.

J'ai téléchargé la version 2.4.2-1.

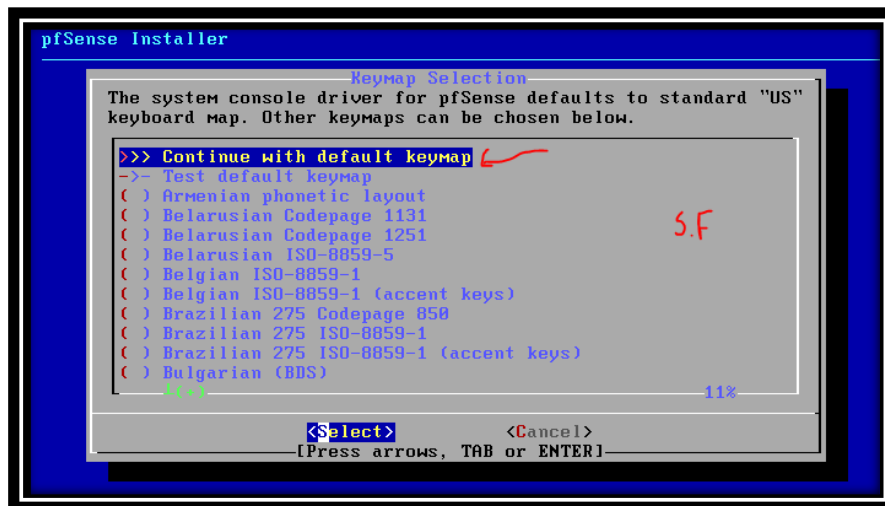
Pour l'installation de la machine, j'ai suivi ces étapes :



Il faut accepter.



Installer PfSense.



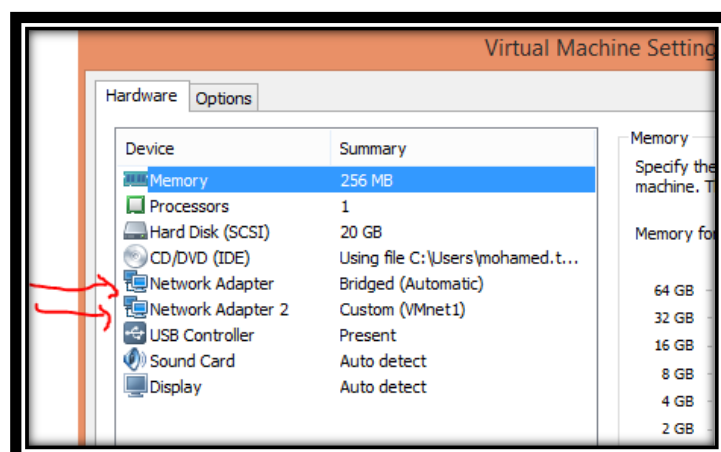
Valider le premier choix.

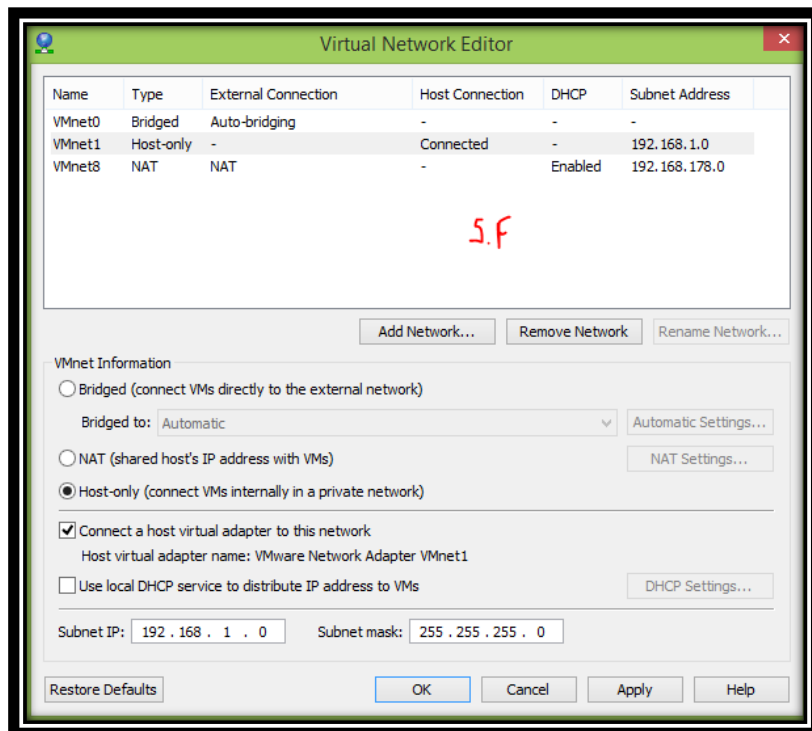


Et enfin, accepter l'Auto (UFS).

Pour la suite il faut sélectionner non et reboot.

Une fois cela fais, j'ai rajouté un Network Adapter à la machine : le premier est connecter en Bridged (Automatic) et le second en Custom (VMnet1). J'ai fait cela pour que ma machine puisse être connectée avec une autre machine par la suite.





Ensuite on reboot le PfSense avec l'option 5.

Une fois cela fait le WAN (Wide Area Network) aura une adresse IP donné par le DHCP mais le LAN (Local Area Network) n'a pas d'adresse IP. Ainsi, il faut attribuer une adresse IP static au LAN.

On doit lui donner comme adresse IP la même que la passerelle par défaut de notre réseau réel, soit ici 192.168.1.1.

Pour ce faire, on choisit l'option « Set interface(s) IP address » ensuite en sélectionne le LAN et pour finir on met l'adresse IP du LAN.

```

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.10.67/24
LAN (lan)      -> em1      -> ?

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1

```

Une fois cela fait, on doit donner le CIDR de l'adresse IP du LAN, soit ici 24. La suite jusqu'à la question du DHCP c'est en fonction de ce que vous voulez, ici je n'ai mis aucune valeur sauf le non (« n ») pour la question portant sur le DHCP (« Voulez-vous activer le serveur DHCP sur le LAN ? ») car je veux une adresse static. Et pour finir j'ai continué.

```
255.0.0.0      = 8
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) n
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://192.168.1.1/
Press <ENTER> to continue. S.F
```

Comme on peut le voir ci-dessous le LAN a maintenant l'adresse IP que je lui ai donnée :

```
*** Welcome to pfSense 2.4.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.10.67/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
Enter an option: 
```

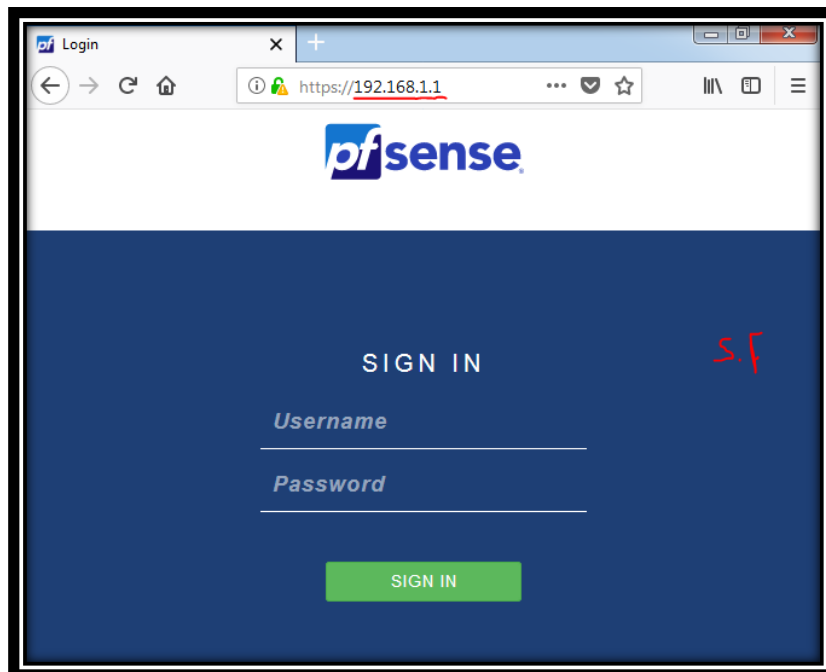
On vient de finir l'installation de PfSense.

2. Configuration de Pfsense :

Maintenant que l'installation de PfSense est faite nous pouvons configurer ce dernier. Pour cela, nous devons créer un serveur au choix et le connecter en Custom (VMnet1) pour que les deux machines (PfSense et le serveur) soit dans le même réseau.

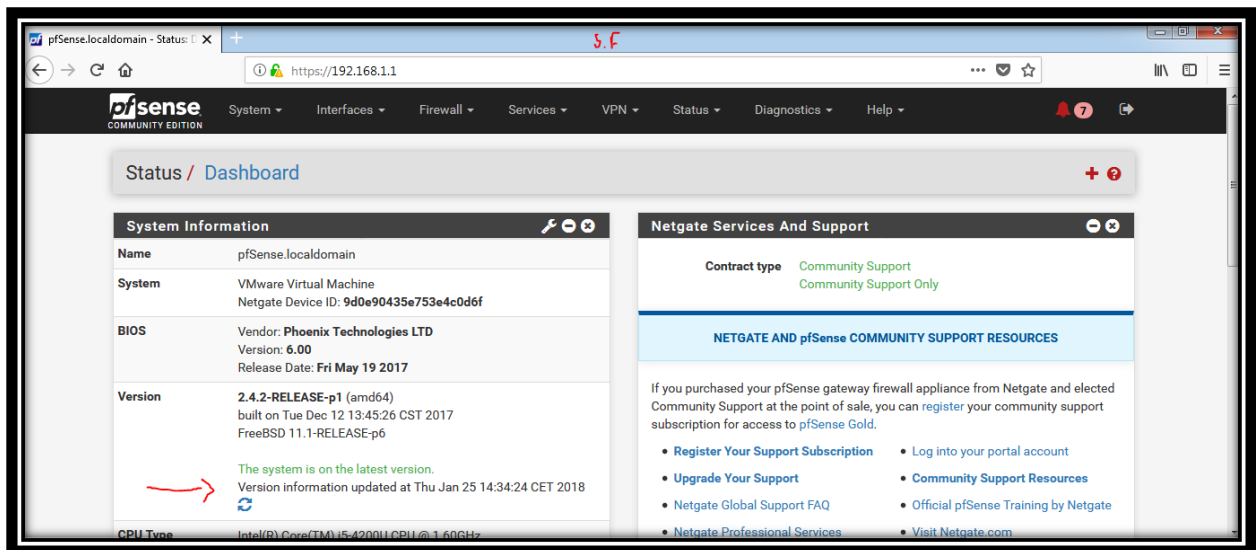
J'ai choisie de prendre un serveur Windows 2012 R2 déjà utilisé pour mes études, donc pour l'installation de ce dernier je vous laisse vous référer aux tutoriels faciles d'accès sur internet.

Une fois le serveur créer, il faut ouvrir un navigateur de préférence ne pas utiliser Internet Exploreur. Dans ce navigateur, entrez l'adresse du LAN de PfSense, soit ici 192.168.1.1, pour pouvoir configurer le portail captif.



L' « Username » et le « Password » sont, dans l'ordre : « admin » et « pfsense » (par défaut).

Lors de la connexion à l'adresse de PfSense, il est conseillé d'utiliser l'aide à la configuration même si par la suite les informations peuvent être modifiées. Nous arrivons sur la page par défaut d'administration de PfSense.



Si PfSense n'est pas mis à jours, il est conseillé de le faire. Pour la mise à jour vous n'avez qu'à aller dans la sous-catégorie « Version » situé dans la catégorie « System Information ».

Une fois cela fait, il faut aller dans « System » puis dans « Setup Wizard » et cliquer sur « next » jusqu'à arriver sur la page General Information. Sur cette dernière il faut entrez le nom de la machine (pfSense), le domaine (localdomain) et IP du DNS (8.8.8.8).

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
 Enter the hostname (FQDN) of the time server.

Timezone

» Next

S.F

Ensuite cliquez sur « next » sur cette nouvelle page pour option « Selectes Type dans la configuration WAN Interface il faut choisir DHCP et laisser tout le reste par défaut sauf les deux cases à cocher tout en bas de la page.

PPTP Idle timeout

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

RFC1918 Networks

Block RFC1918 Private Networks ☒ Block private networks from entering via WAN
 When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks ☒ Block non-Internet routed networks from entering via WAN
 When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

» Next

S.F

Sur la prochaine page, il faut entrer l'adresse IP du LAN de PfSense (192.168.1.1) et le Subnet Mask (24).
 Ensuite vous pouvez changer le mot de passe mis par défaut.

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

» Next


S.F

Et vous continuez.

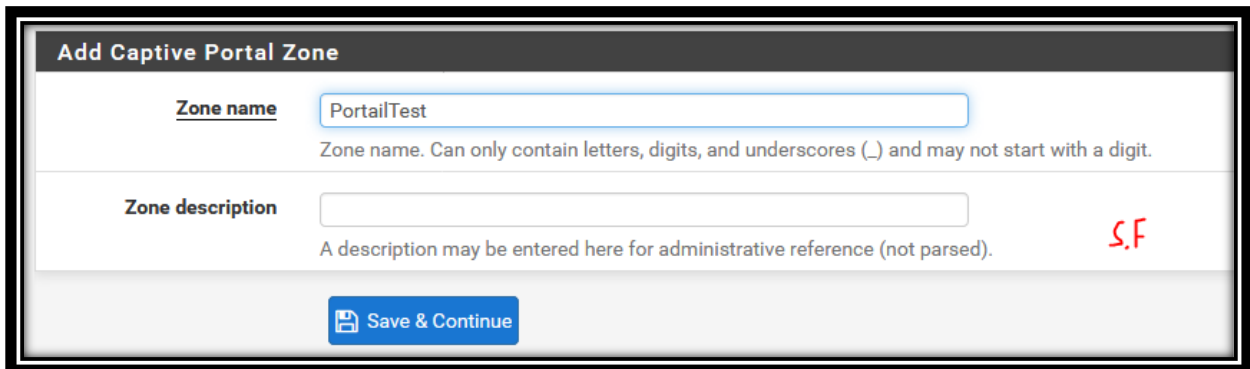
II. Mise en place du portail captif:

1. Configuration de base du portail captif :

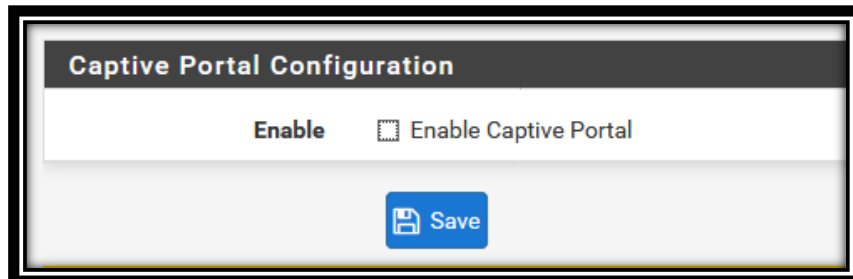
Pour cela, on doit partir dans la sous-catégorie « Captive Portal » qui se trouve dans la catégorie « Services ».

Une fois arrivée là-bas, on clique sur la touche .

Dès lors vous devez donner un nom à votre portail captif et sauvegarder.



Ensuite il faut cocher la case « Enable Captive Portal »



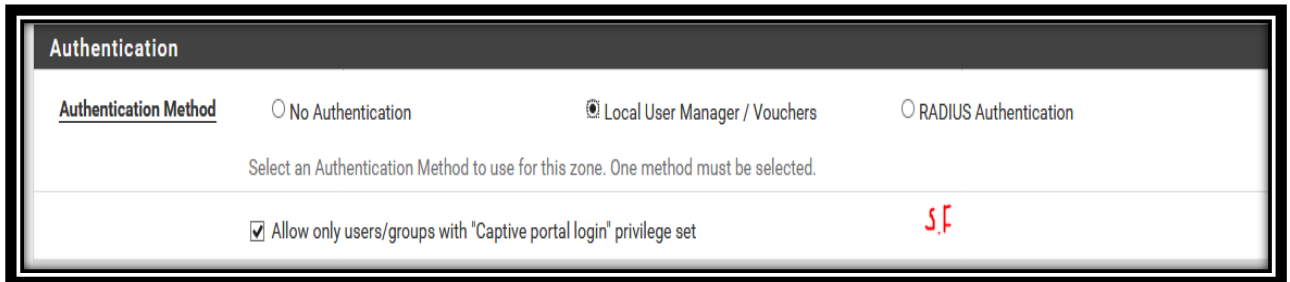
Lorsque c'est fait vous devez sélectionner l'interface LAN.


(Vous pouvez laisser les options par défaut ou les changer c'est en fonction de vos préférences.)

*Il y a deux méthodes d'authentification avec le portail captif :
une locale et une via un serveur RADIUS.*


2. Authentication Local :

Il y a tout d'abord une authentication « **Local User Manager/Vouchers** » à cocher dans « Authentication », il ne faut pas oublier de cocher le « Allow only users/groups with 'Captive portal login' privilege set » :




Une fois cela fait, on sauvegarde .

- En premier lieu, il faut créer un groupe :
Pour cela, il faut aller sur la sous-catégorie « User Manager » dans la catégorie « System ».

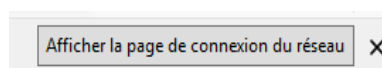
Delà nous devant partir dans « Groups » et cliquer sur .

Ensuite nous donnons un nom au groupe et on doit sélectionner « Local » pour le « Scope ». Attention « admin » doit être mis dans la case « Not members » sinon le groupe aura tous les droits. Et pour finir il faut assigner le privilège « User – Services : Captive Portal login » au groupe et sauvegarder.

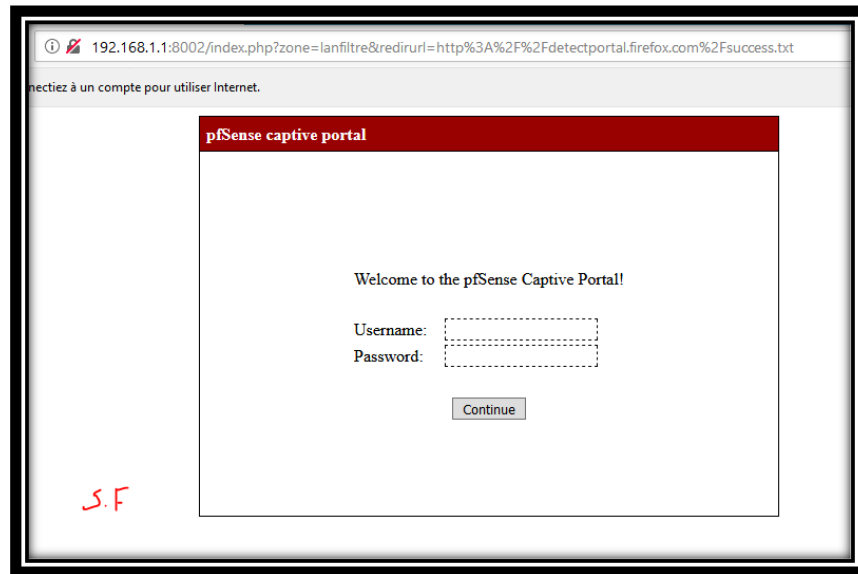
- En second lieu, il faut créer des utilisateurs :
Pour cela il faut aller dans « Users » et cliquer sur .

Ensuite nous donnons un nom à notre utilisateur et un mot de passe pour la connexion. Attention vous devez mettre « admins » dans « Not member of » et le groupe que vous avez précédemment créé doit être mis dans la case « Member of » et sauvegarder.

- ✓ On a fini la configuration, maintenant nous allons tester :
Pour ce faire, nous allons ouvrir une page d'un navigateur. Normalement, si vous avez bien suivie les consignes, la page de l'authentification du portail captif peut s'ouvrir automatiquement sinon il faut cliquer sur :




La page par défaut d'authentification de PfSense ressemble à ça :



The screenshot shows a web browser window with the address bar displaying `192.168.1.1:8002/index.php?zone=lanfiltre&redirurl=http%3A%2F%2Fdetectportal.firefox.com%2Fsuccess.txt`. Below the address bar, a message reads "Connectez à un compte pour utiliser Internet." The main content area features a red header bar with the text "pfSense captive portal". Below this, a white box contains the text "Welcome to the pfSense Captive Portal!". Underneath, there are two input fields labeled "Username:" and "Password:". A "Continue" button is positioned below the password field. A red handwritten mark "S.F" is visible in the bottom left corner of the white box.

Cette dernière vous pourrez la changer, pour cela je ne peux pas vous aidez car ce n'est pas dans mes compétences. Je peux juste vous dire où vous devez mettre votre page de connexion personnalisé. Pour cela lors de la configuration de base, en bas de page, il y a une catégorie spécialement pour changer la page par défaut de PfSense. Vous n'avez qu'à cliquer sur Parcourir dans la rubrique « HTML Page Contents » et vous sélectionnez la page que vous avez créé.



The screenshot shows the "HTML Page Contents" configuration page. At the top, there is a section titled "Portal page contents" with a "Parcourir..." button and the text "Aucun fichier sélectionné." Below this, there is a detailed instruction: "Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to '\$PORTAL_ACTION\$') with a submit button (name='accept') and a hidden field with name='redirurl' and value='\$PORTAL_REDIRURL\$'. Include the 'auth_user' and 'auth_pass' and/or 'auth_voucher' input fields if authentication is enabled, otherwise it will always fail." An example code snippet is provided:

```
<form method='post' action='$PORTAL_ACTION$'>
  <input name='auth_user' type='text'>
  <input name='auth_pass' type='password'>
  <input name='auth_voucher' type='text'>
  <input name='redirurl' type='hidden' value='$PORTAL_REDIRURL$'>
  <input name='zone' type='hidden' value='$PORTAL_ZONE$'>
  <input name='accept' type='submit' value='Continue'>
</form>
```

 A red handwritten mark "S.F" is visible in the bottom right corner of the page.

Maintenant, vous entrez le nom de l'utilisateur et son mot de passe que vous avez précédemment créé.

Bien sûr vous pourrez créer d'autres utilisateurs et vous pourrez même créer des groupes avec le privilège du portail captif et des privilèges différents pour chaque groupe.

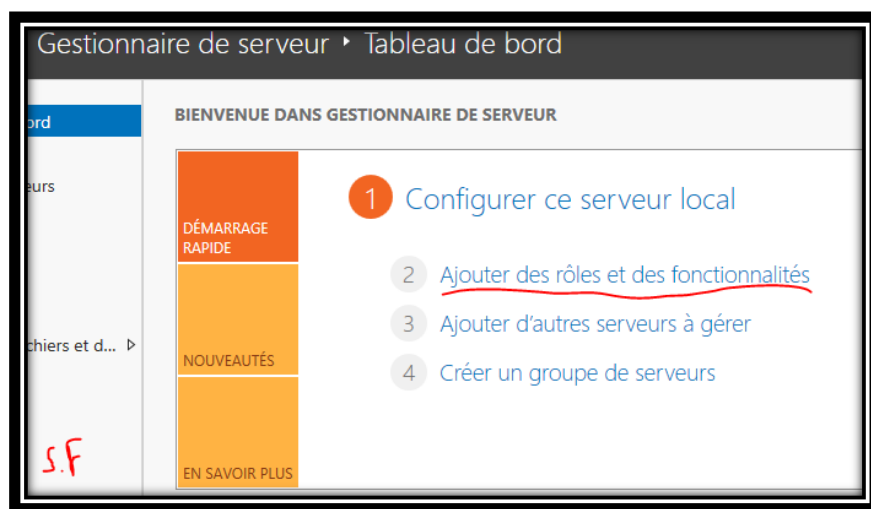
Si il n'y a pas eu d'erreur, vous pourrez utiliser internet.

3. Authentification avec Radius :

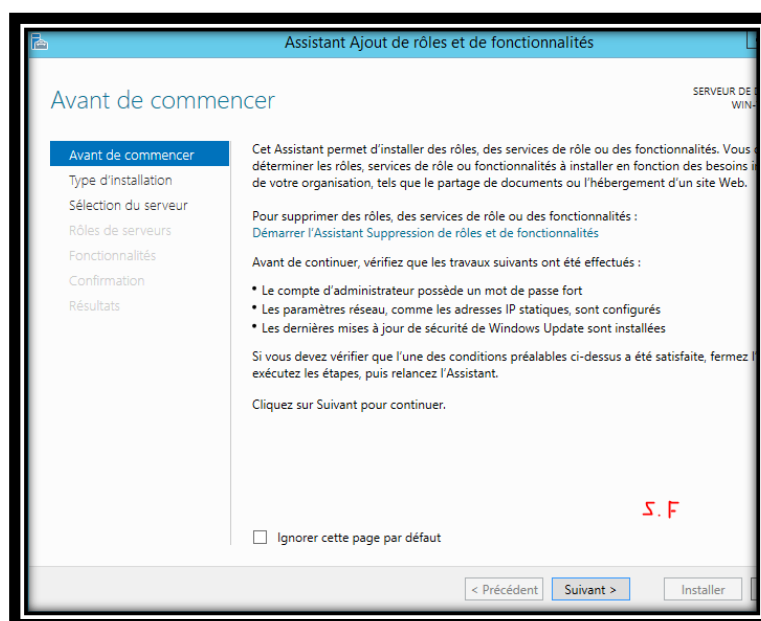
Ensuite nous avons une authentification « **Radius Authentication** » à cocher dans « Authentication » :

- Pour cette méthode, nous allons créer un serveur Radius, personnellement j'ai utilisé un serveur Windows 2012 R2 pour la création de ce dernier. Ainsi, pour ce faire, une fois la machine virtuelle créée (voir les tutoriels facile d'accès sur internet) au démarrage, une page de gestionnaire de serveur s'ouvre automatiquement.

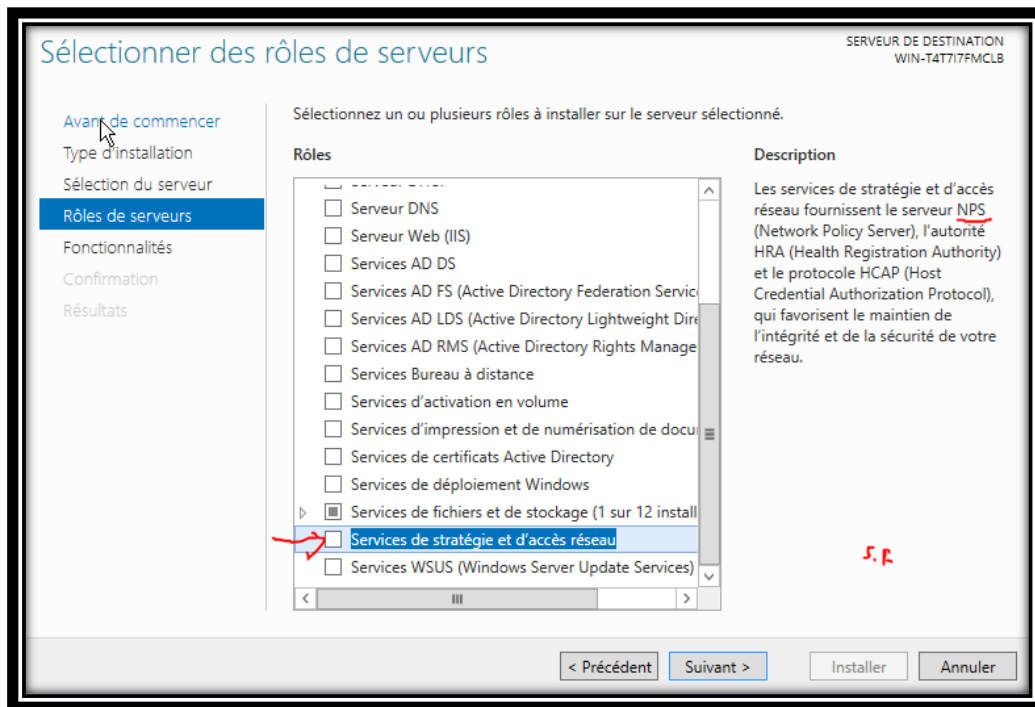
Vous devez ajouter le rôle « Serveur NPS » (Network Policy Server).



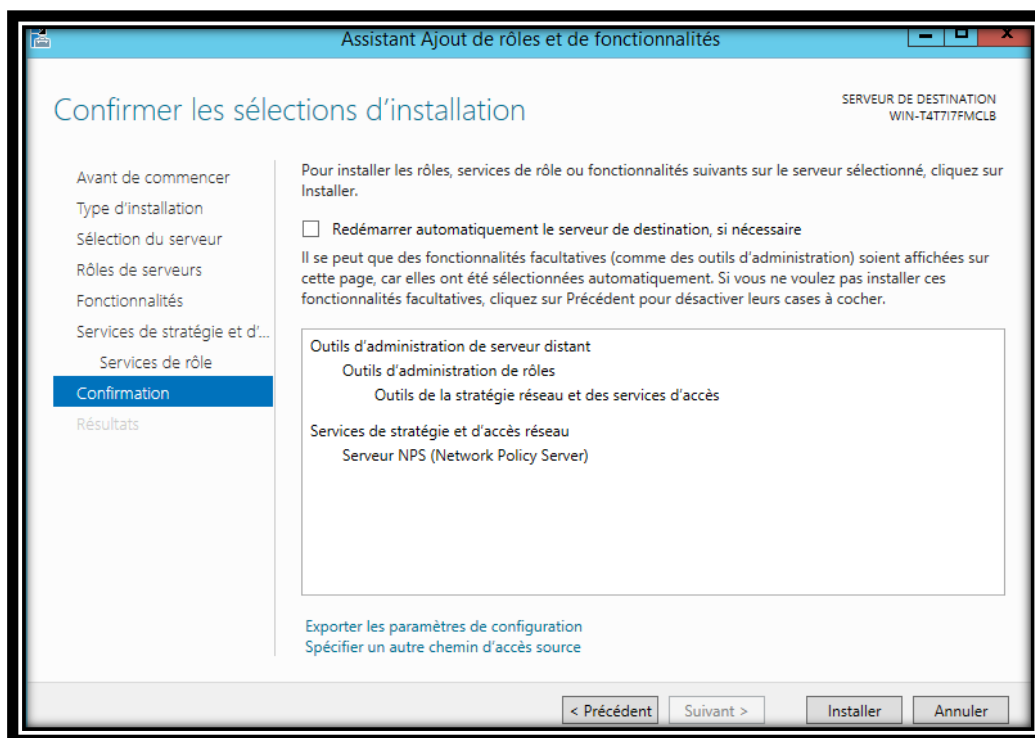
Pour cela, nous devons cliquer sur « Ajouter des rôles et des fonctionnalités ».



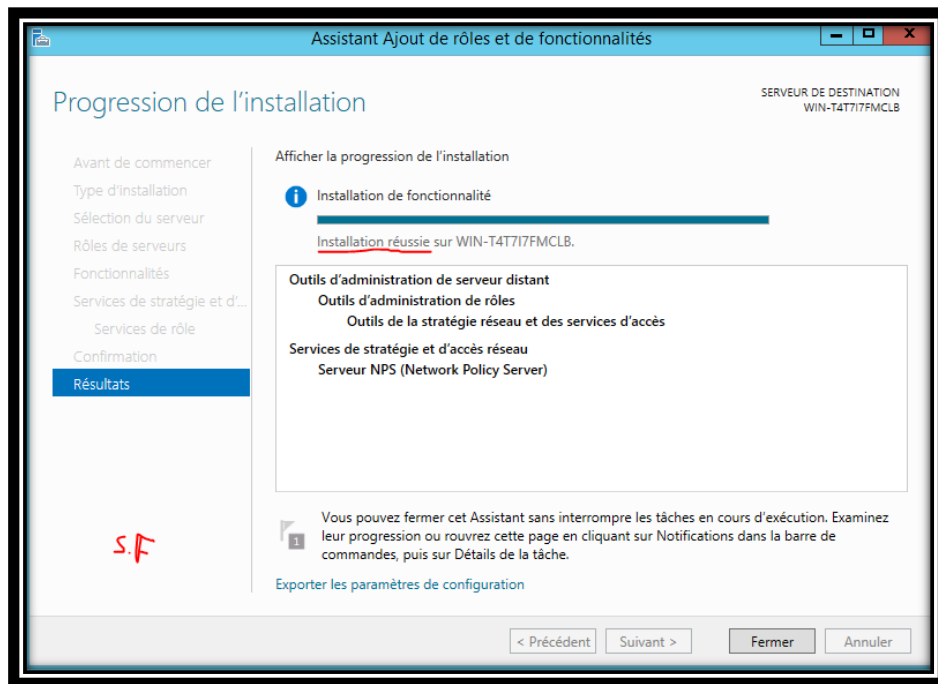
Cliquez sur suivant.



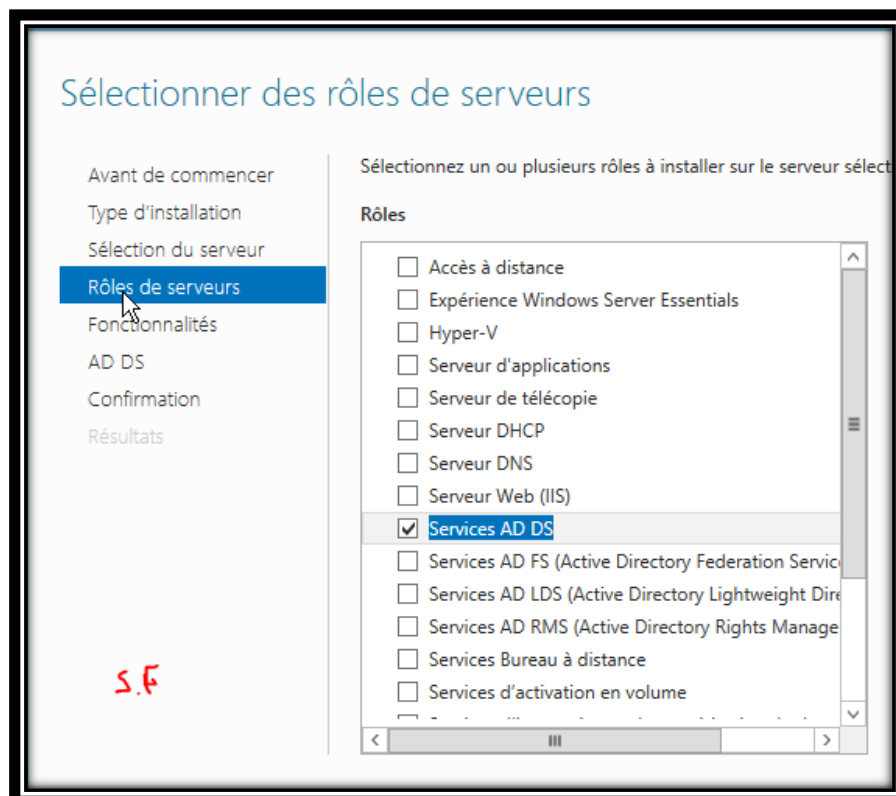
Ensuite vous continuez à cliquer sur suivant jusqu'à la page où vous devez cliquer sur Installer.




Une fois, l'installation terminée vous pouvez fermer la page.



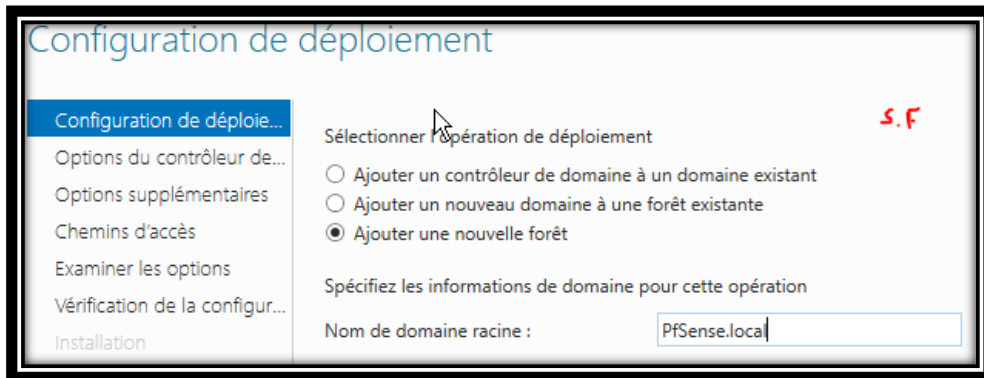
Ensuite vous rajoutez le rôle « AD DS » vous suivez les mêmes étapes que pour l'ajout du « Serveur NPS ».



Ensuite, il faut promouvoir ce dernier en contrôleur de domaine, pour ce faire, il faut

cliquer sur .

Vous ajoutez une nouvelle forêt et vous donnez un nom de domaine racine (exemple : PfSense.local).

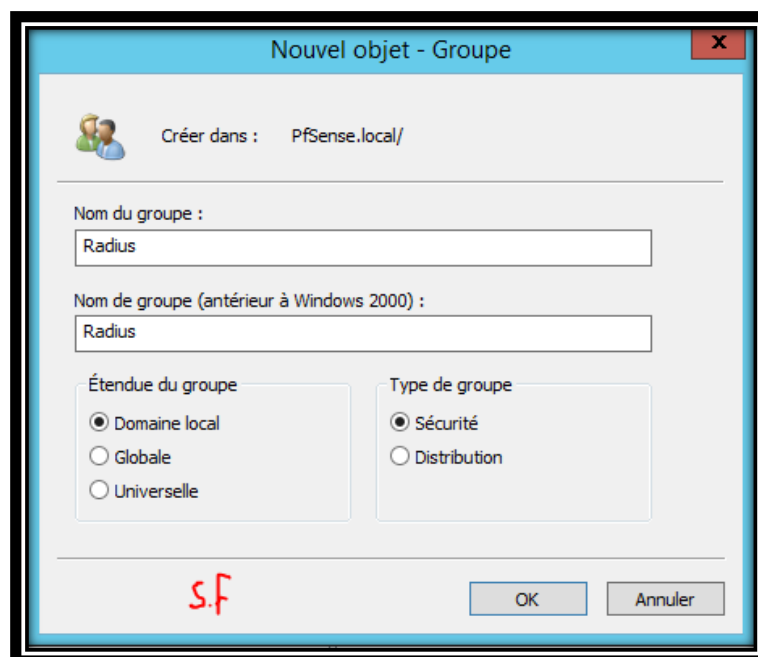


Pour la suite, vous donnez un mot de passe et décocher la fonctionnalité « Serveur DNS », vous donnez un nom de domaine NetBIOS et vous continuez jusqu'à pouvoir cliquer sur Installer.

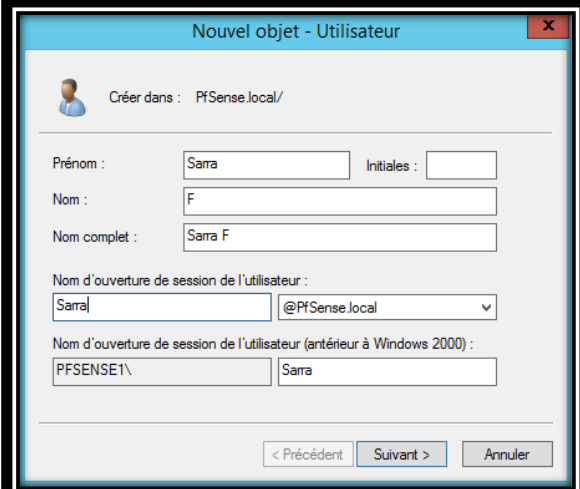
Votre machine va redémarrer.

Au démarrage vous mettez le mot de passe administrateur que vous avez choisi plutôt.

Dans la page gestionnaire de serveur sélectionnez la sous-catégorie « Utilisateurs et ordinateurs Active Directory » dans la catégorie « Outils ». Delà nous devons créer un groupe dans le domaine racine que nous avons créé précédemment (exemple : PfSense.local). Ce groupe doit être étendu dans le domaine local et il doit être de type sécurité.



Une fois le groupe créé, vous devez créer des utilisateurs dans le domaine racine (PfSense.local). Vous pouvez créer autant d'utilisateurs que vous voulez avec des noms (a) et mot de passe (b) différent.



Nouvel objet - Utilisateur

Créer dans : PfSense.local/

Prénom : Sarra Initiales :

Nom : F

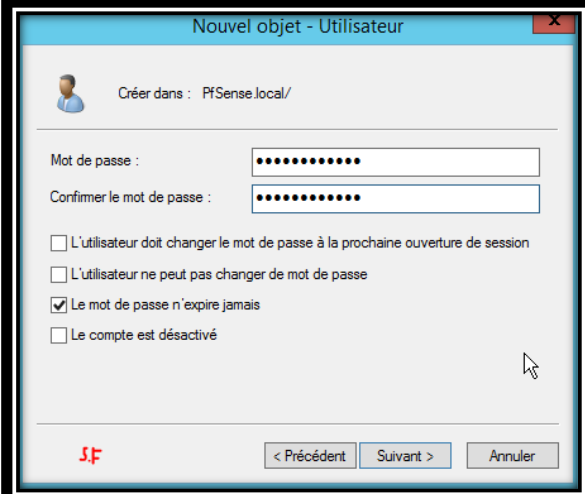
Nom complet : Sarra F

Nom d'ouverture de session de l'utilisateur : Sarra @PfSense.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : PFSENSE1\ Sarra

< Précédent Suivant > Annuler

(a)



Nouvel objet - Utilisateur

Créer dans : PfSense.local/

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

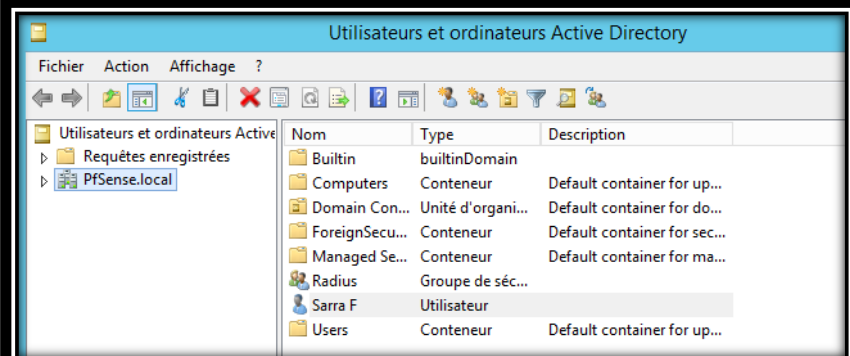
☐ L'utilisateur ne peut pas changer de mot de passe

☒ Le mot de passe n'expire jamais

☐ Le compte est désactivé

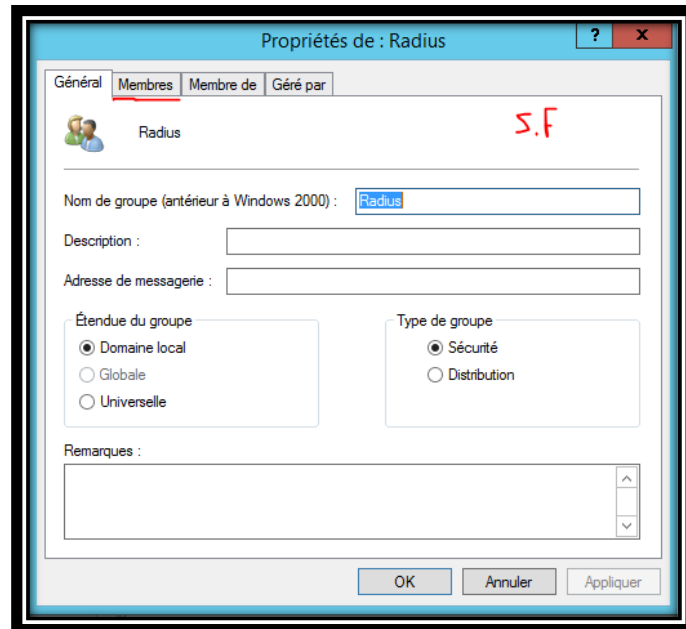
< Précédent Suivant > Annuler

(b)

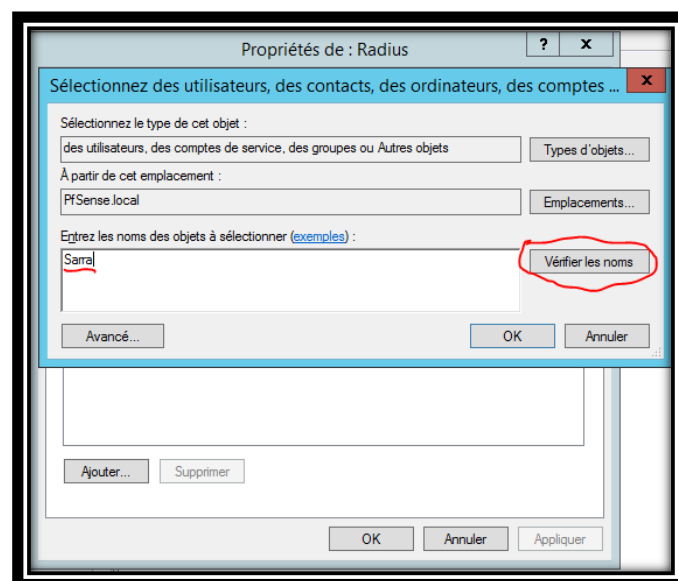


Nom	Type	Description
Builtin	builtinDomain	
Computers	Conteneur	Default container for up...
Domain Con...	Unité d'organi...	Default container for do...
ForeignSecu...	Conteneur	Default container for sec...
Managed Se...	Conteneur	Default container for ma...
Radius	Groupe de séc...	
Sarra F	Utilisateur	
Users	Conteneur	Default container for up...

Quand vous avez fini de créer vos utilisateurs, vous devez les incorporer dans le groupe que vous avez créé. Pour cela vous cliquez sur le groupe, ensuite vous cliquez sur ajouter dans « Membres » (a) et là vous sélectionnez les utilisateurs (b) que vous avez créé.



(a)



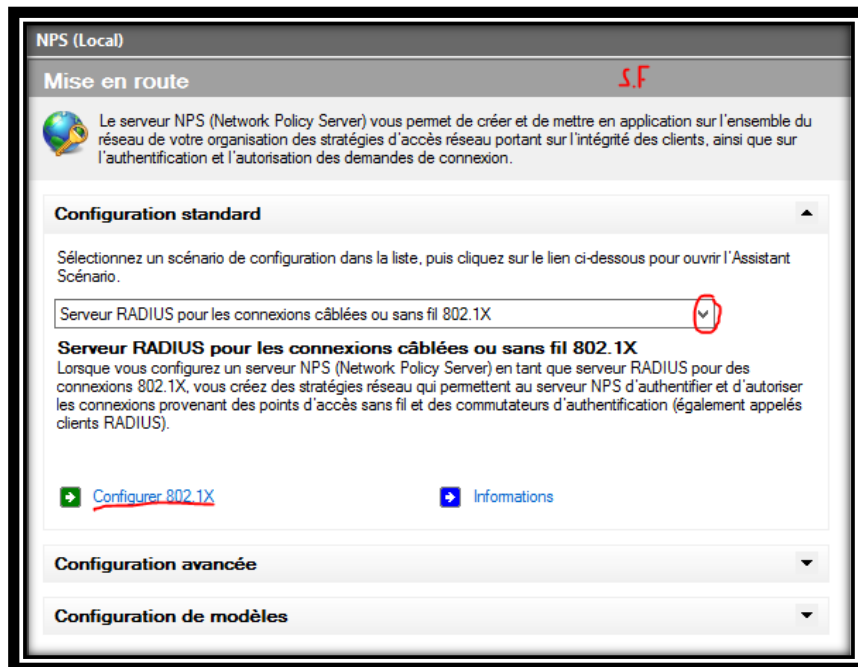
(b)

- Maintenant que nous avons installé le serveur RADIUS, nous devons configurer ce serveur.

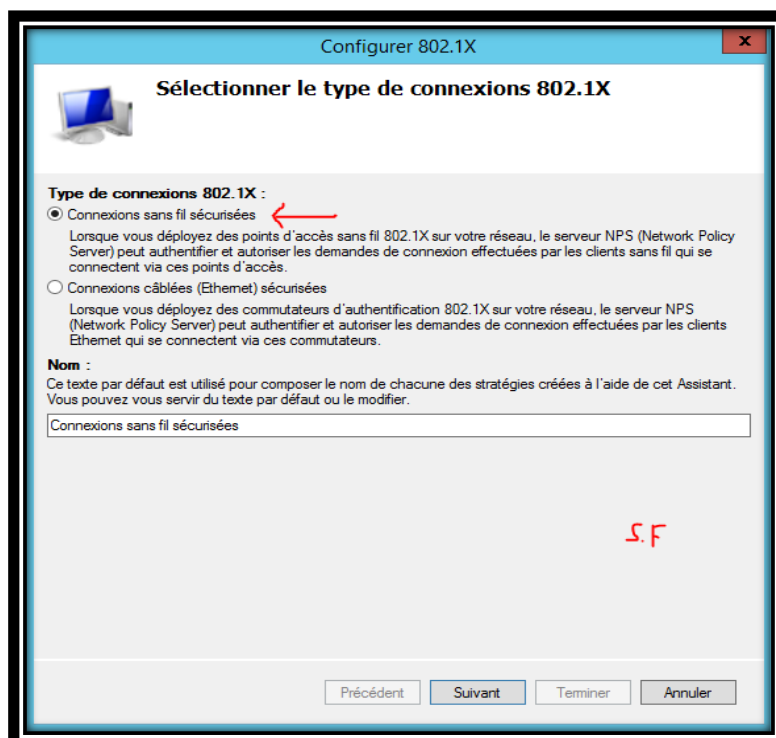
Pour ce faire, vous devez partir sur « Serveur NPS (Network Policy Server) » qui se trouve dans la rubrique « Outils » dans la page de Gestionnaire de Serveur.

Sélectionnez Serveur Radius pour les connexions câblées ou sans fil 802.1X dans la liste de scénario.

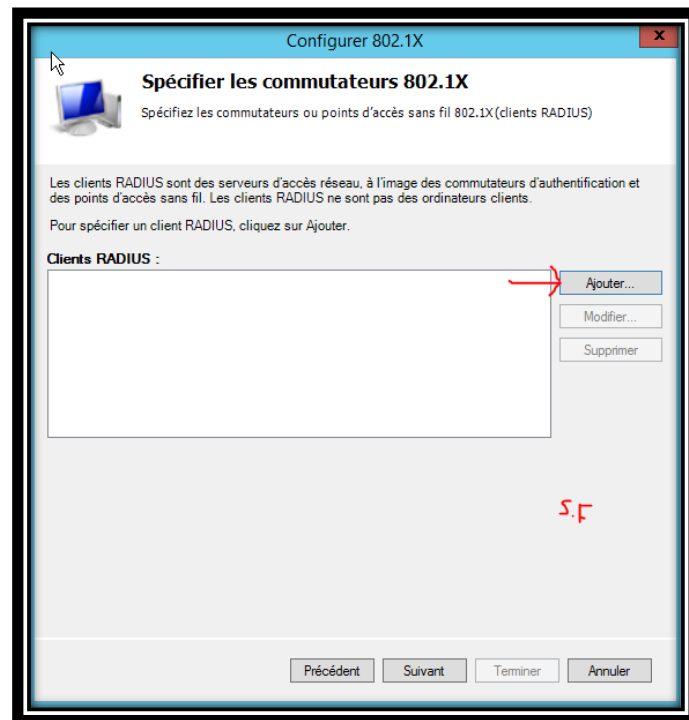
Par la suite, vous devez cliquer sur « Configurer 802.1X ».



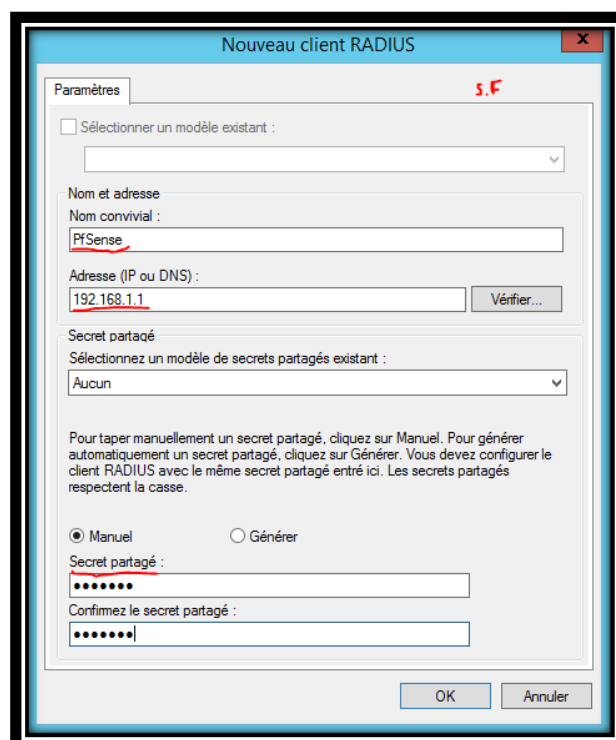
Ensuite, j'ai sélectionné « Connexion sans fil sécurisées » car moi je veux faire un portail captif en Wifi mais il n'y a pas un grand changement pour la configuration entre les deux types de connexions.



Ensuite on va créer un nouveau client Radius. Pour cela, vous devez cliquer sur « Ajouter ».



Vous devez donner un nom convivial et il faut entrer l'adresse IP LAN du PfSense. Il faudra, aussi mettre un secret partagé manuel (qui est en quelques sortes un mot de passe), j'ai personnellement choisi PFSENSE.

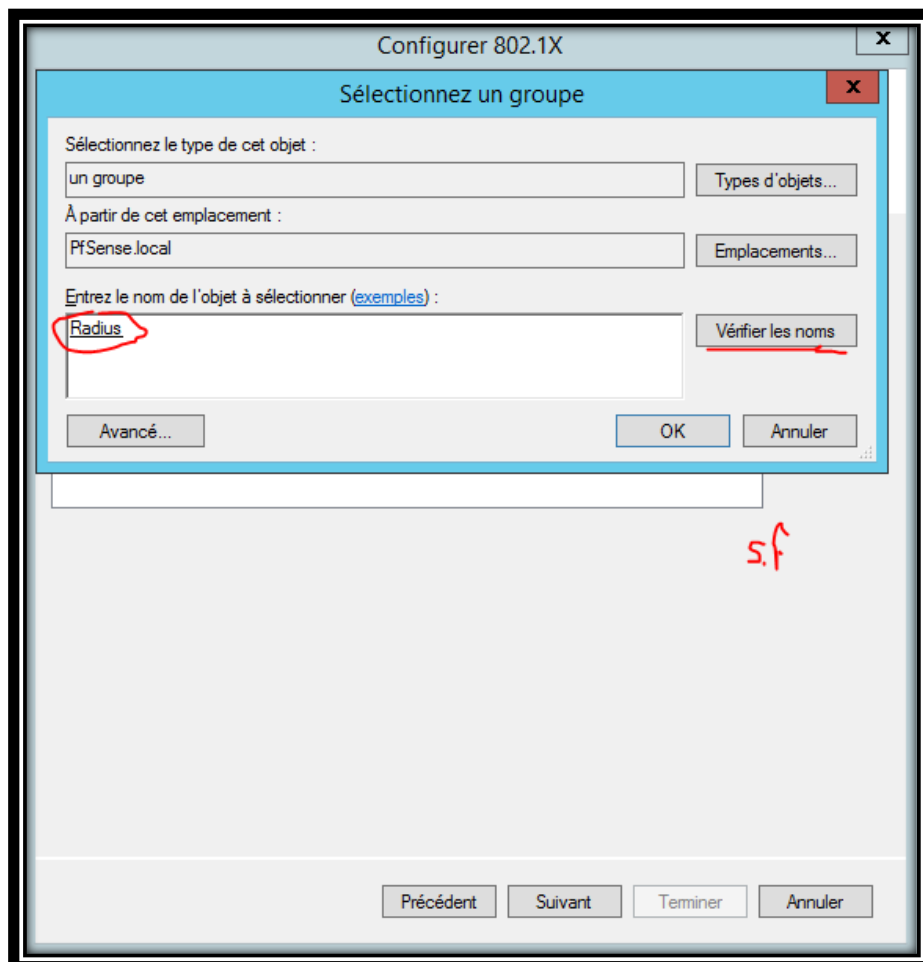


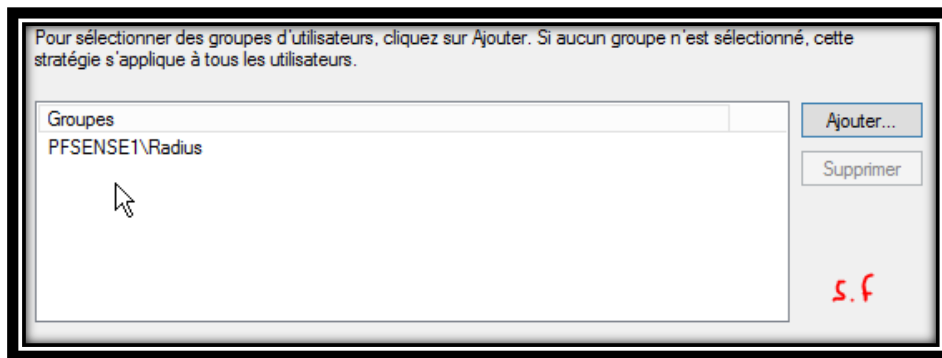
A la suite, nous devons choisir le type de protocole EAP (Extensible Authentication Protocol) : j'ai personnellement choisi PEAP (Protected EAP).

EAP est un protocole de communication réseau embarquant plusieurs méthodes d'authentification.

PEAP est une méthode de transfert sécurisée mais ce n'est pas une méthode de chiffrement, c'est une procédure qui sert à l'authentification d'un client dans un réseau. Ce protocole utilise TLS (Transport Layer Security) pour créer un canal chiffré entre un client PEAP authentifiant (exemple : ordinateur portable) et un authentificateur (exemple : serveur RADIUS).

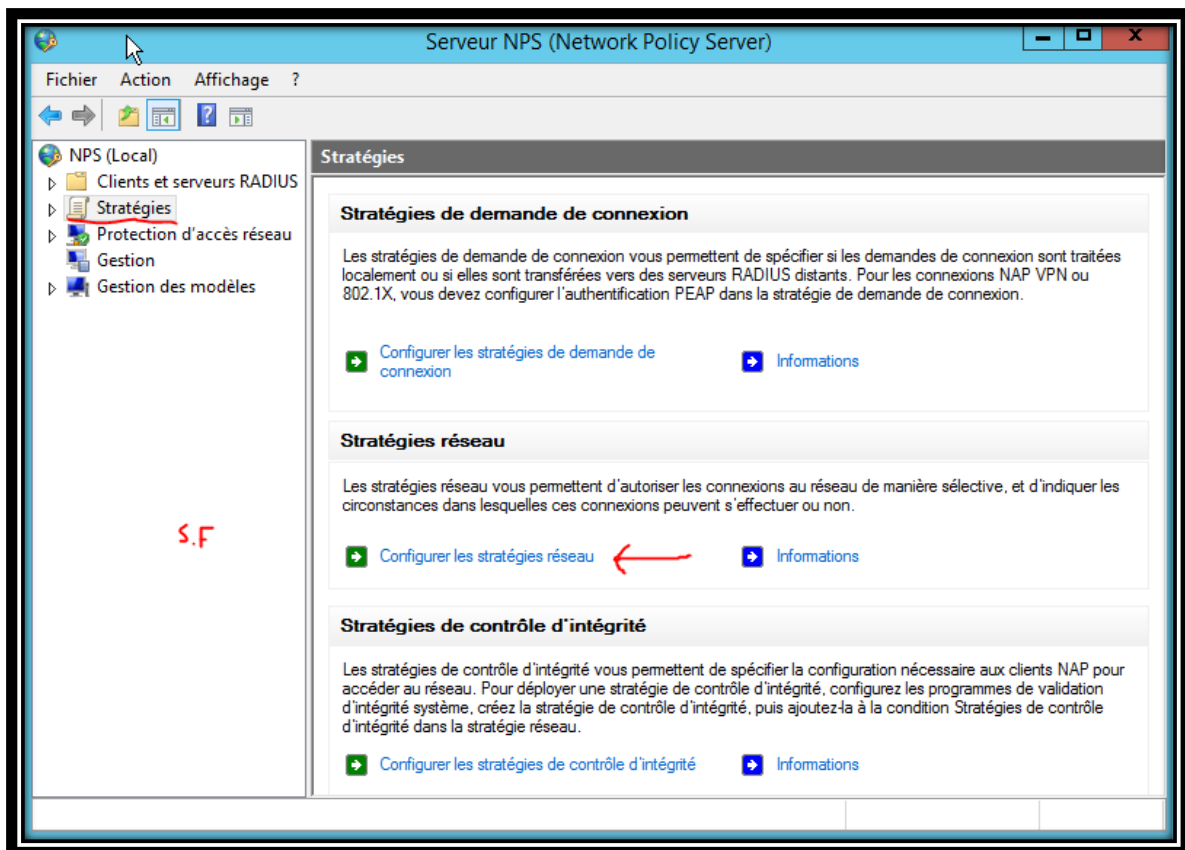
Après avoir cliqué sur « Suivant », nous devons ajouter les groupes qui seront autorisés à accéder au PfSense. Ainsi, nous devons ajouter le groupe précédemment créé, soit Radius pour ma part.



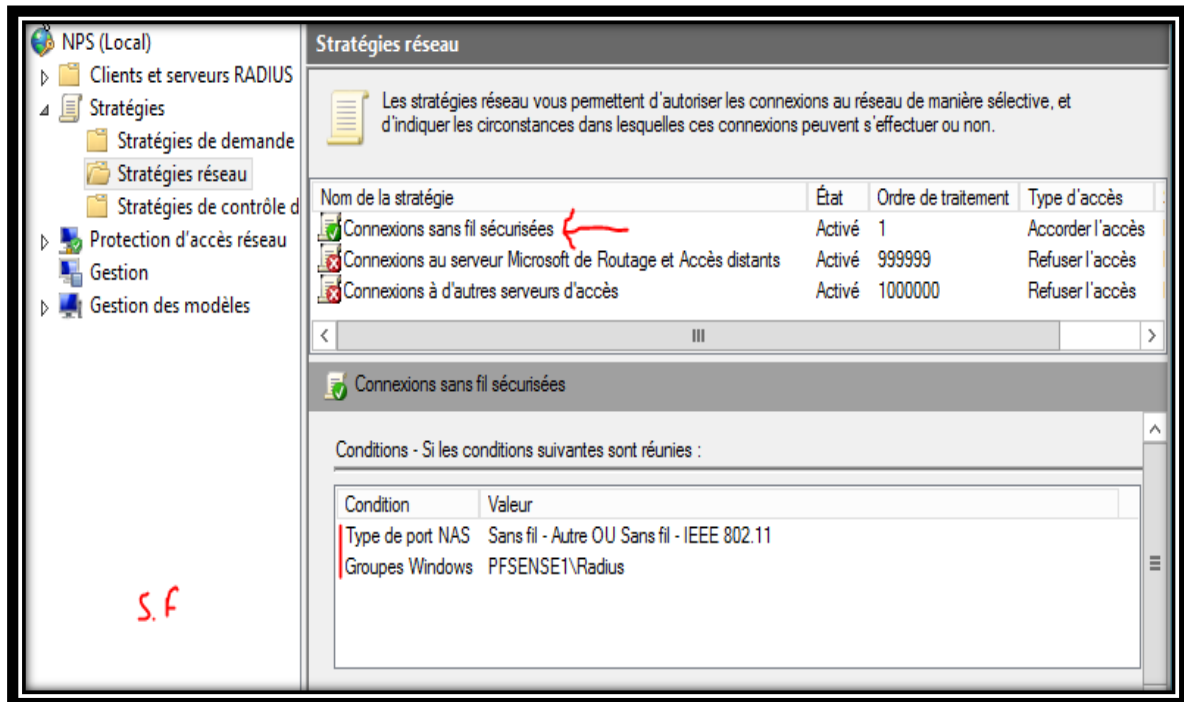


Ensuite vous cliquez sur « Suivant » et « Terminer ».

Une fois cette étape terminée, nous partons sur le menu de gauche de la fenêtre « Serveur NPS » et nous allons dans « Stratégies » puis nous cliquons sur « Configurer les stratégies réseau ».

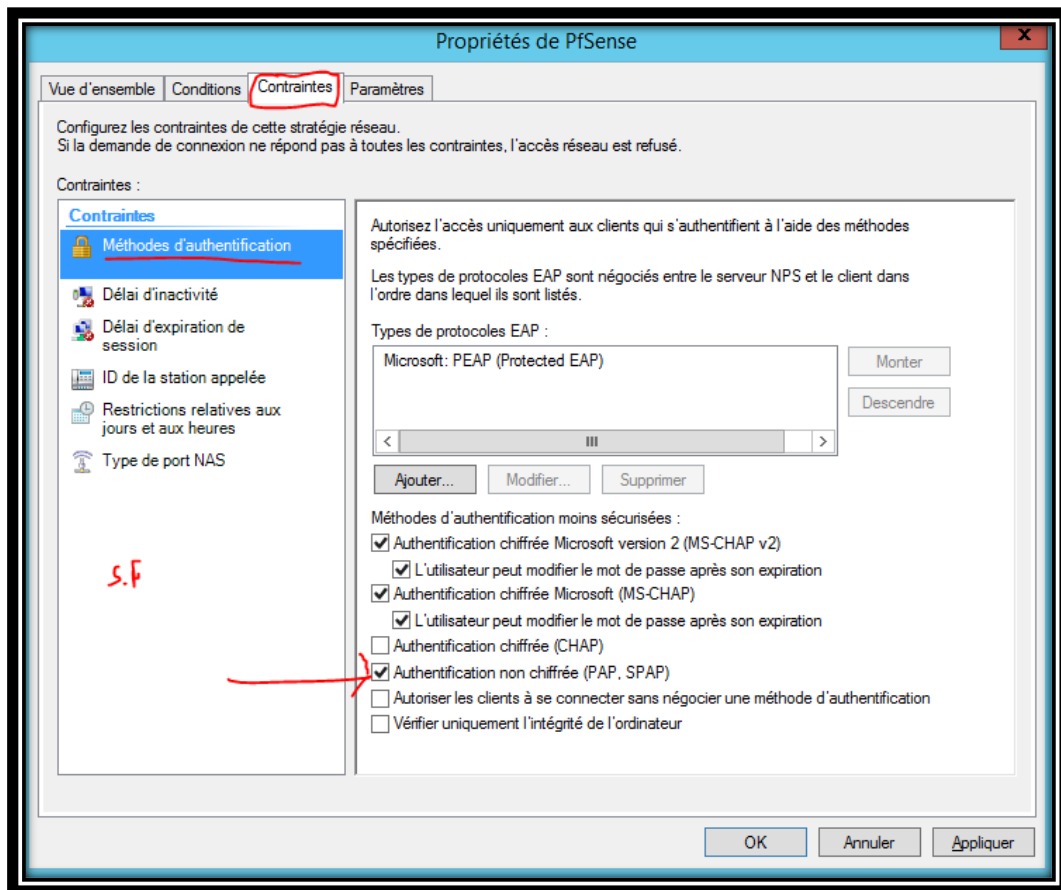


On sélectionne la stratégie que nous avons précédemment créée, on fait un clic droit puis « Propriétés » :

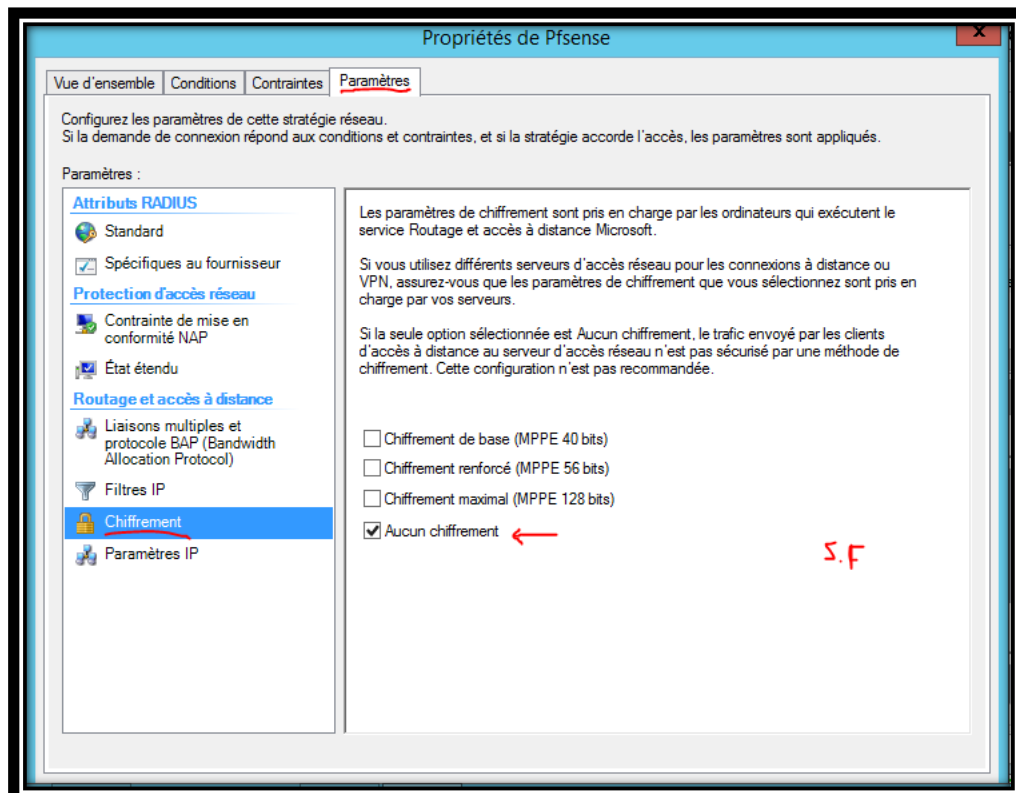


J'ai changé le nom de la stratégie pour ne pas confondre, maintenant la stratégie s'appelle « Stratégie PfSense ».

Vous devez aller dans l'onglet Contraintes puis dans Méthodes d'authentifications et ensuite vous devez cocher « Authentification non chiffrée (PAP, SPAP) » car avec PfSense nous ne pouvons pas utiliser le protocole PEAP.



Après cela, vous devez aller dans l'onglet « Paramètres » puis dans « Chiffrement » et là, vous devez cocher « Aucun chiffrement ».



Vous finissez en cliquant sur « Appliquer » et vous avez fini de configurer le serveur maintenant vous devez configurer l'Authentification Radius au sein de PfSense.

Pour ce faire vous rouvrez la page de PfSense sur le navigateur grâce à l'adresse IP LAN de ce dernier.

Puis vous allez dans la catégorie « Captive Portal » dans l'onglet « Services » et ensuite vous allez dans la rubrique « Authentication ». Vous cochez « RADIUS Authentication » puis « MSCHAPv2 ».

MSCHAPv2 est la deuxième version Microsoft du protocole CHAP (Challenge-Handshake Authentication Protocol). C'est un protocole d'authentification basé sur la résolution d'un « défi ».

En combinant le protocole PEAP et MS-CHAPv2, vous augmentez considérablement la sécurité de votre réseau car l'association des deux nous permet de:

- ✓ Fournir l'authentification du client en utilisant des mots de passe ;
- ✓ Vérifier que le serveur a accès aux informations d'identification ;
- ✓ Authentifier le serveur ;
- ✓ Empêcher l'usurpation des points d'accès sans fil ;
- ✓ Empêcher un serveur non autorisé de négocier la méthode d'authentification la moins sécurisée ;
- ✓ Utiliser les clés TLS générées avec une clé publique ;
- ✓ Fournir un chiffrement de bout en bout ;
- ✓ Empêcher les attaques par dictionnaire ou par force brute ;
- ✓ Empêcher les attaques de rejouer ;
- ✓ Faire le chaînage des méthodes d'authentification.

Dans « Primary RADIUS server » dans la rubrique « Primary Authentication Source » vous mettez l'adresse IP du serveur Radius, soit 192.168.1.133 pour ma part.

(Il est fortement conseiller d'avoir une adresse IP static pour le serveur.)

Dans « RADIUS shared secret », on rentre le secret partagé défini dans le serveur RADIUS, soit PFSense pour ma part.

Authentication			
Authentication Method <input type="radio"/> No Authentication <input type="radio"/> Local User Manager / Vouchers <input checked="" type="radio"/> RADIUS Authentication ←			
Select an Authentication Method to use for this zone. One method must be selected.			
RADIUS protocol <input type="radio"/> PAP <input type="radio"/> CHAP-MD5 <input type="radio"/> MSCHAPv1 <input checked="" type="radio"/> MSCHAPv2 ←			
Primary Authentication Source			
Primary RADIUS server <input type="text" value="192.168.1.133"/> <input type="button" value="IPADDR"/> <input type="text" value="PFSENSE"/>			
Secondary RADIUS server <input type="text"/> <input type="button" value="IPADDR"/> <input type="text"/>			
IP address of the RADIUS server to authenticate against.		RADIUS port. Leave blank for default (1812)	RADIUS shared secret. Leave blank to not use a shared secret (not recommended) S.F
Secondary Authentication Source			

Dans la rubrique « Accounting », veuillez cocher « Send RADIUS accounting packets » et « No updates ».

Accounting	
RADIUS	<input checked="" type="checkbox"/> Send RADIUS accounting packets to the primary RADIUS server. S.F
Accounting Port	<input type="text"/> Leave blank to use the default port (1813).
Accounting updates	<input checked="" type="radio"/> <u>No updates</u> <input type="radio"/> Stop/Start <input type="radio"/> Stop/Start (FreeRADIUS) <input type="radio"/> Interim

Vous avez fini, vous pouvez maintenant tester comme avec la première méthode sauf que cette fois vous utilisez les noms et mot de passe des utilisateurs que vous avez incorporé dans le groupe créé dans le serveur RADIUS.

Si il n'y a pas d'erreur vous pourrez utiliser internet.