PORTAIL CAPTIF AVEC PFSENSE

TABLE DES MATIERES

OBJECTIFS

- Mettre en place un portail captif wifi avec authentification Radius-NPS via pfSense.

FONCTIONNEMENT

Un portail captif est un accès wifi accessible par le biais d'un navigateur web. L'authentification peut être anonyme (attention a la loi), via une base locale ou et c'est ici le cas par un serveur Radius sous Windows serveur - NPS.

Pour voir les principes de Radius et la mise en place se reporter à http://general.sio57.info/wp/?attachment_id=944

MAQUETTE

- 1 AD DNS CA
- 1 DHCP et 1 RADIUS-NPS
- 1 borne sans sécurité (réseau wifi ouvert, c'est Pfsense est le client Radius et fait transiter la demande d'authentification.

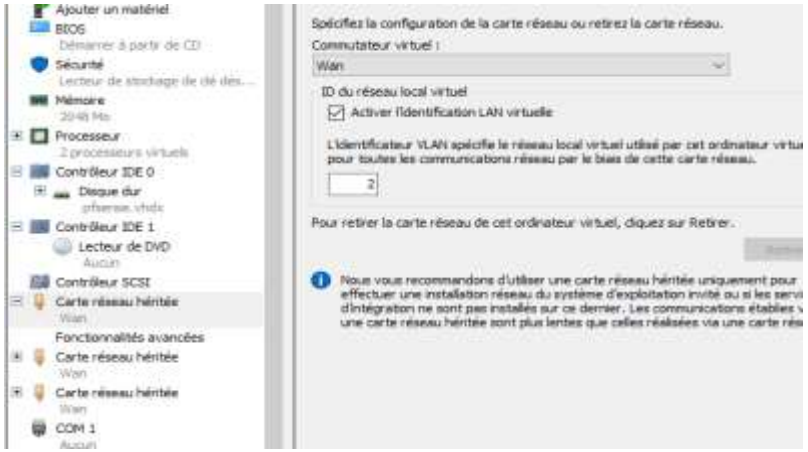
Sur les bornes HP wm200 il est possible de gérer plusieurs ssid. Un SSid gère l'authentification via le portail pfSense sur un vlan différent qui permet d'accéder à Internet ; l'autre Ssid permet l'accès au réseau local ; l'authentification est transmise alors par la borne wifi dont les paramètres sont sécurisés.

- 1 pfSense

Radius est fonctionnel voir TP Radius NPS http://general.sio57.info/wp/?p=943

On ajoute ici 1 Pfsense avec 3 cartes réseaux : 1 wan, 1 lan, 1 wlan (lan et wlan : même carte physique avec des vlans différents (dans cette doc, c'est une seule carte avec des vlans).

(Pourquoi j'ai mis des cartes héritées ? parce qu'avec certaines distrib Linux et BSD, les cartes fonctionnent mieux ainsi- Après je n'ai pas testé toutes les config).



PFSENSE

L'installation de pfSense se fait via l'image iso, il suffit de suivre les instructions.

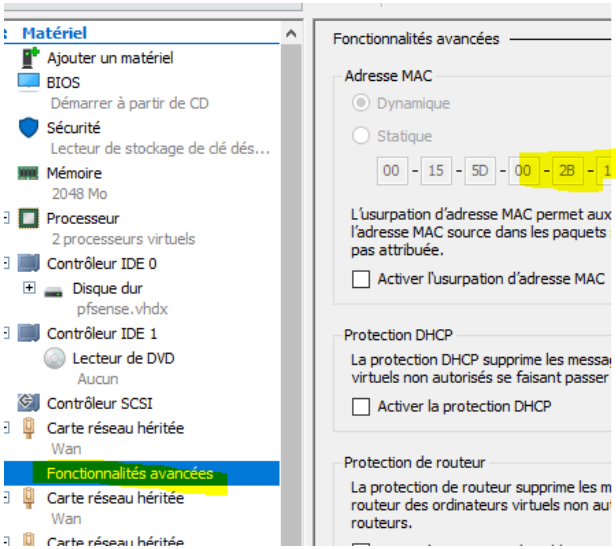
La seule difficulté est l'attribution des cartes réseaux.

INTERFACES

Il faut se reporter aux propriétés avancées des cartes réseaux dans les Paramètres de la vm pour obtenir l'adresse mac de chacune.

```
Valid interfaces are:

de0     00:15:5d:00:2b:14 (down) Digital 21140A Fast Ethernet
de1     00:15:5d:00:2b:15 (down) Digital 21140A Fast Ethernet
de2     00:15:5d:00:2b:16 (down) Digital 21140A Fast Ethernet
```



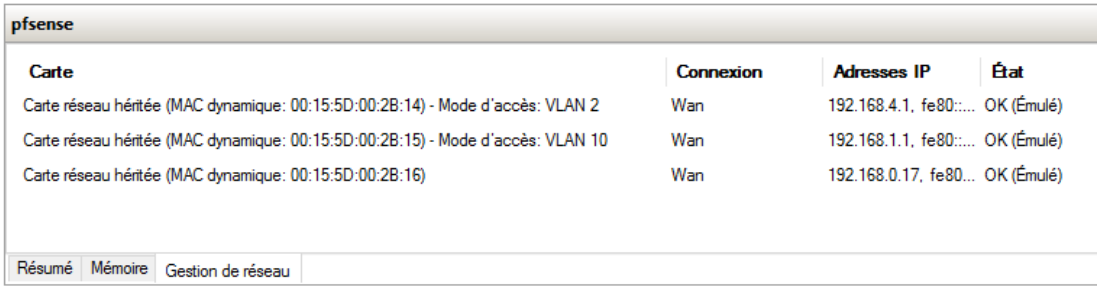
Attribuer vos cartes en fonction de votre configuration

-Wan, Lan et

Opt1 sera la carte reliée à la borne wifi

```
WAN  -> de2
LAN  -> de1
OPT1 -> de0
```

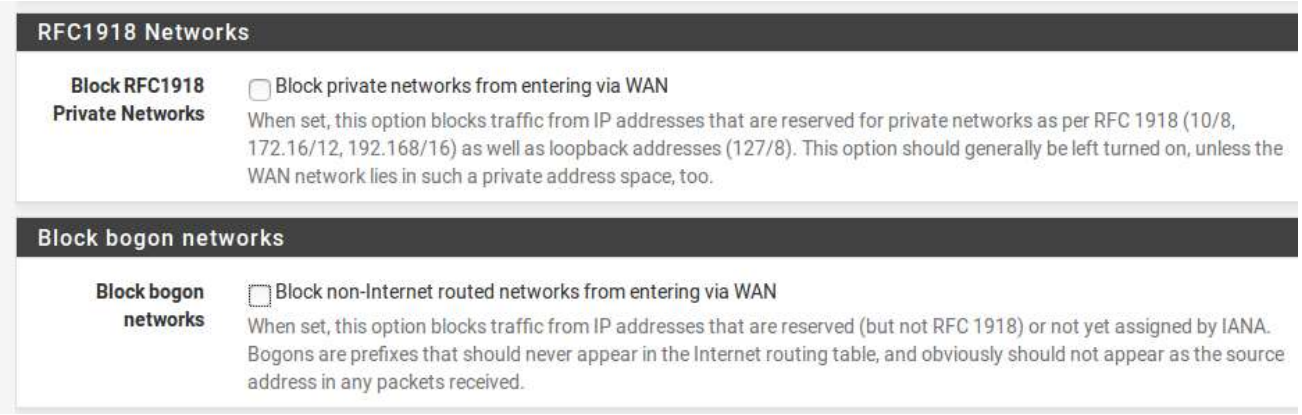
Dans hyper-v on peut voir



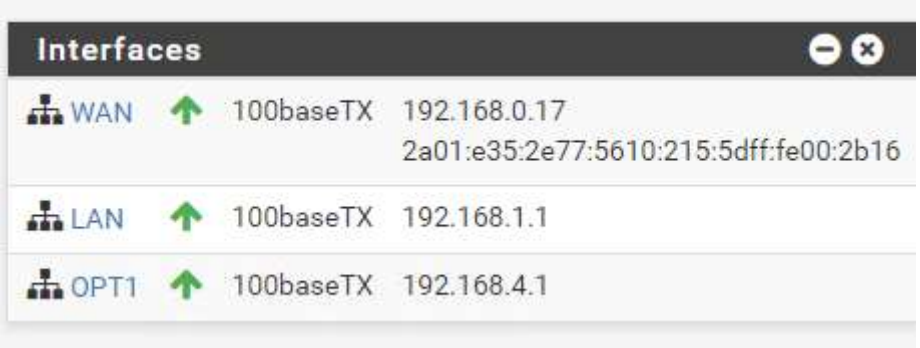
Par défaut l'interface Lan est 192.168.1.1.

Se connecter depuis un navigateur et suivre les instructions pour la configuration de base.

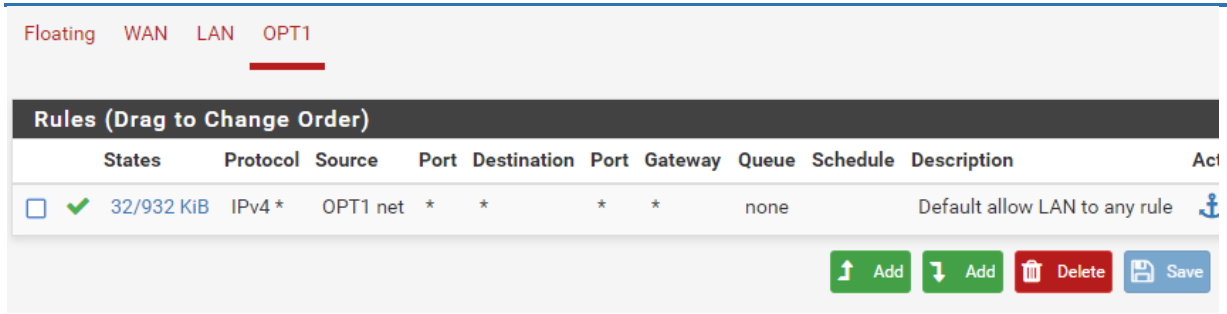
Attention nous n'utilisons que des plages privées alors il faut les laisser passer



Dans le menu Interface on obtient



Règles du pare feu (pour les 1ers tests on baisse la sécurité)

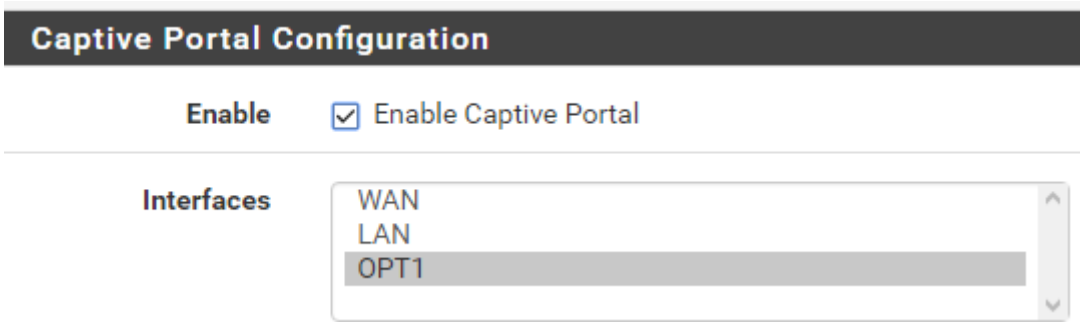


PORTAIL CAPTIF

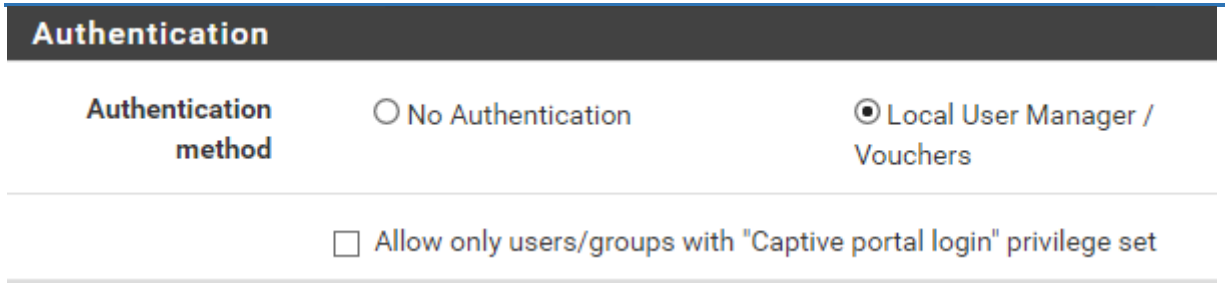
Essayer d'abord sans sécurité et avec un utilisateur local à créer depuis le menu Système de pfsense, User Manager

Créer le Portail

- PfSense, menu Services, Portail Captif
- Cocher enable – puis en choisissant l'interface du wifi opt1



Plus bas choisir authentication Local User



Avoir au préalable mit la borne wifi dans le même réseau que Opt1 de pfsense et vérifier la communication entre les 2

Enlever toute sécurité sur la borne- mode ouvert.

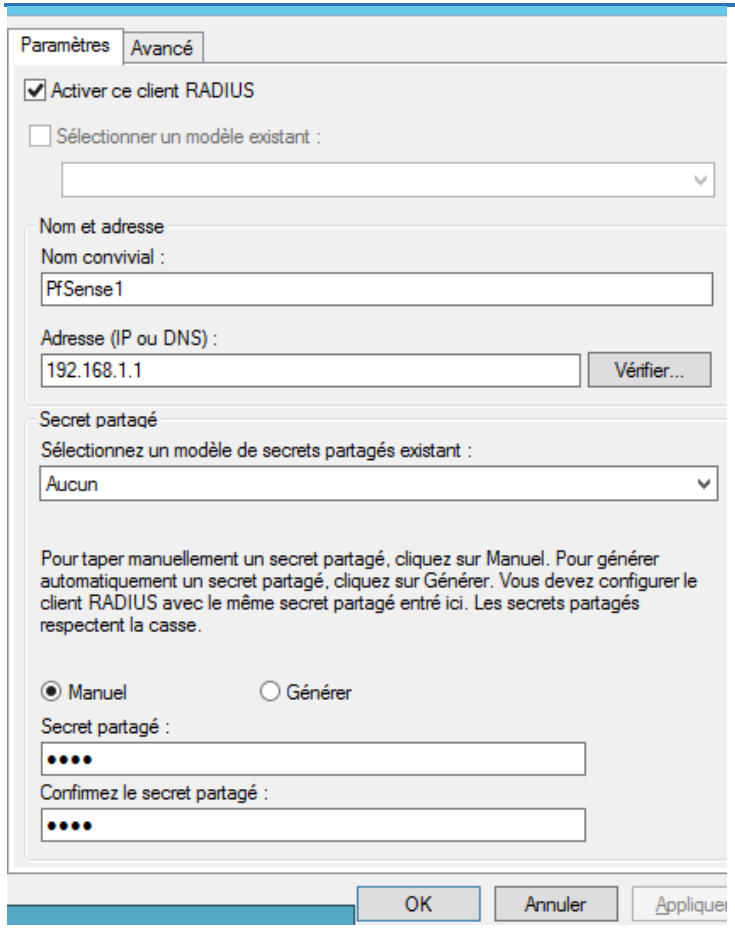
Tester la connexion depuis un appareil wifi – réseau ouvert, demande de connexion à un navigateur

Vous devriez avoir une page de login de base.

NPS

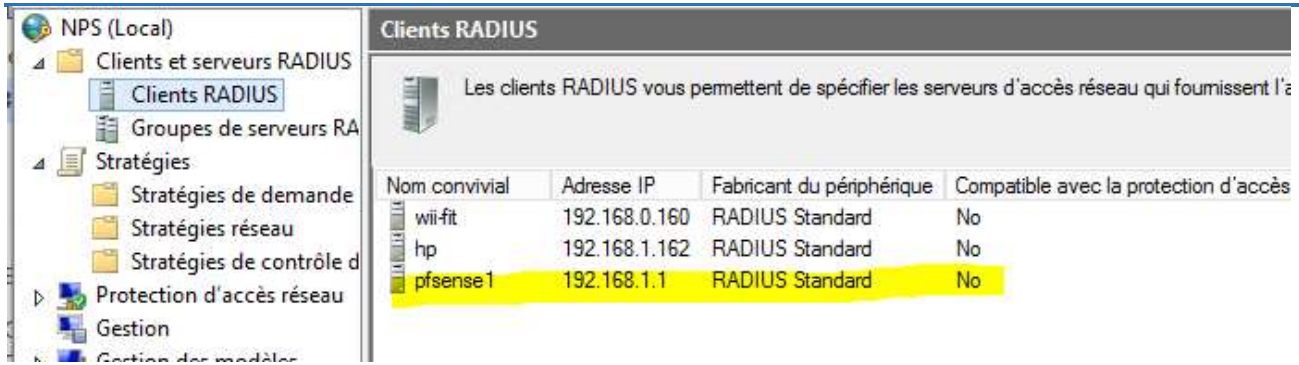
Par précaution, régler le nom d'hôte 'pfsense' dans le dns.

Dans NPS, créer un nouveau client Radius



Il faudra créer aussi une stratégie mais nous y reviendrons plus tard.

On obtient (en tenant compte du tp précèdent)



MISE EN LIEN AVEC RADIUS - PORTAIL

DECLARATION DU CERTIFICAT DU DOMAINE DANS PFSENSE

Pour que les que pfsense reconnaisse le serveur NPS, il faut qu'il reconnaisse l'autorité de certification. Pour cela il faut importer le certificat de l'autorité de certification (créer au préalable : voir TP 1er TP Radius

Copier le certificat de l'autorité de certification dans la vm depuis laquelle vous gérer pfsense ((je gère mes vm depuis une lubuntu : facilité d'exporter les certificats en .pem)

Dans l'explorateur de fichier, cliquer sur le certificat, puis bouton droit exporter

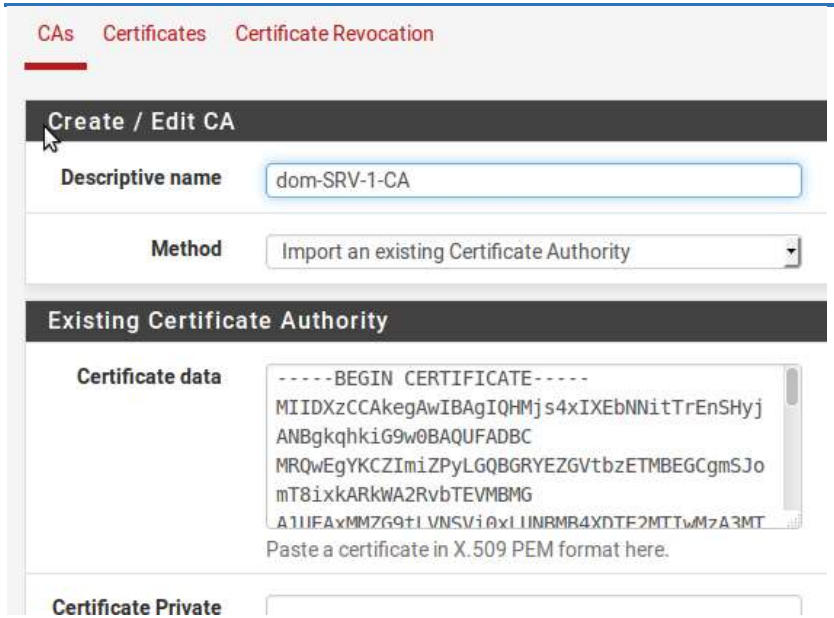
Exporter au format PEM

Ouvrir avec LeafPad

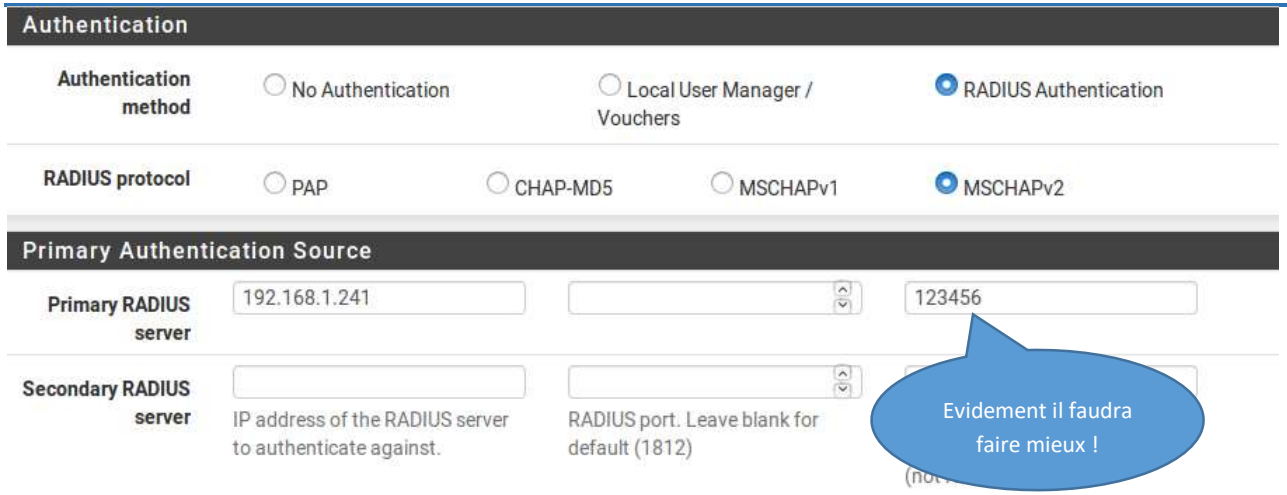
- Et copier tout le certificat

Sur pfsense, dans le menu System, certificats, CA

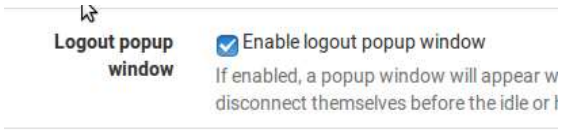
- Coller le certificat



Mans le menu, Services, Portail, passer la sécurité sur Radius et MSCHAP v2. Régler le serveur NPS dans les paramètres Radius.

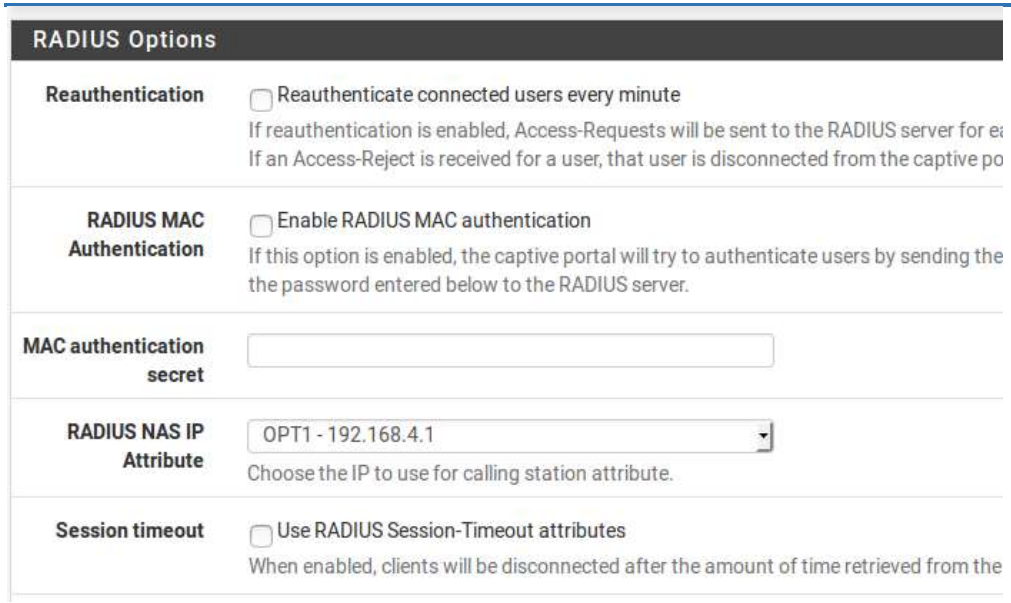


Au niveau des options j'ai choisi de mettre un bouton de déconnexion dans le navigateur

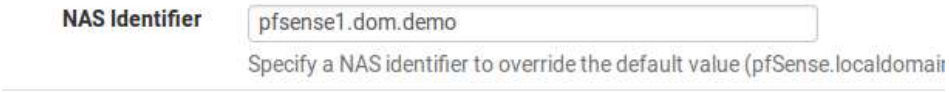


Ensuite il faut mettre en cohérence la stratégie NPS et le Radius attribut

Sur le portail de pfsense, dans le Radius NAP attribute, choisir la carte d'écoute des requêtes des clients.

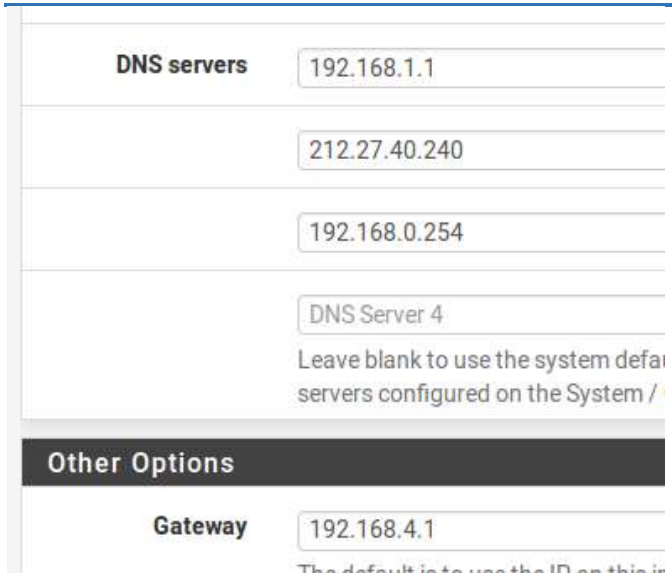


- Positionner aussi le NAS identifier pour que tout soit cohérent

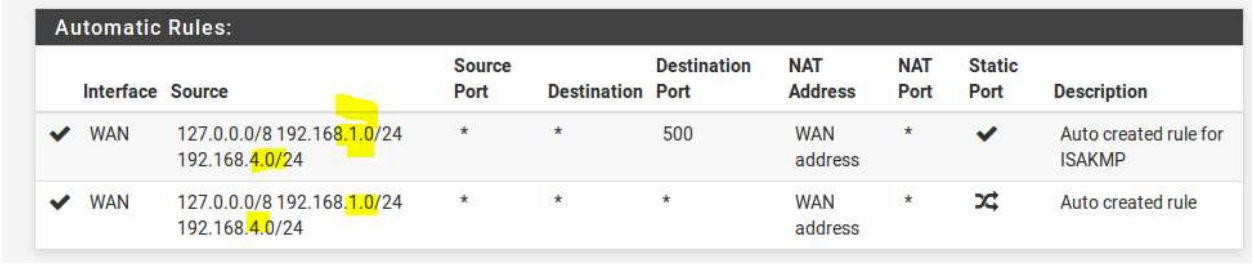


Activer le serveur DHCP sur l'interface Wifi

Verifier l'adresse de la passerelle dans les options du DHCP



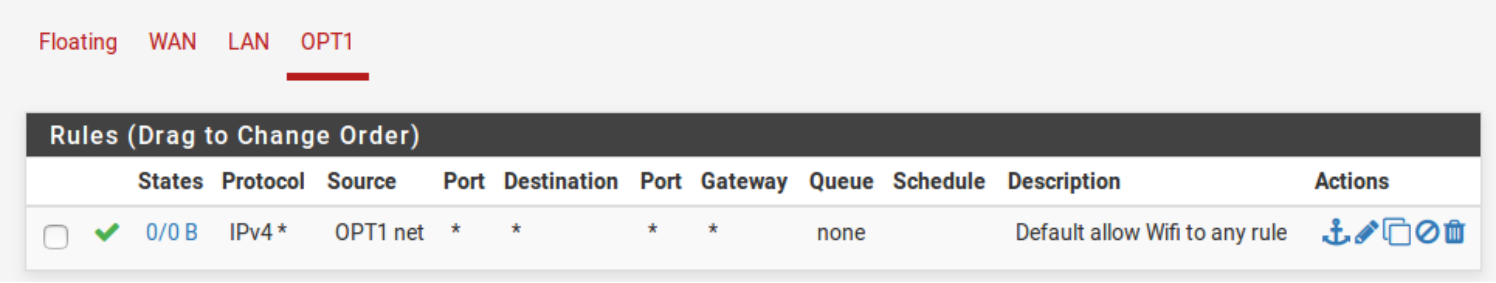
Vérifier d'avoir les règles qui NAT pour le réseau sans fil.



Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✔	WAN	127.0.0.0/8 192.168.1.0/24 192.168.4.0/24	*	*	500	WAN address	*	✔	Auto created rule for ISAKMP
✔	WAN	127.0.0.0/8 192.168.1.0/24 192.168.4.0/24	*	*	*	WAN address	*	⇄	Auto created rule

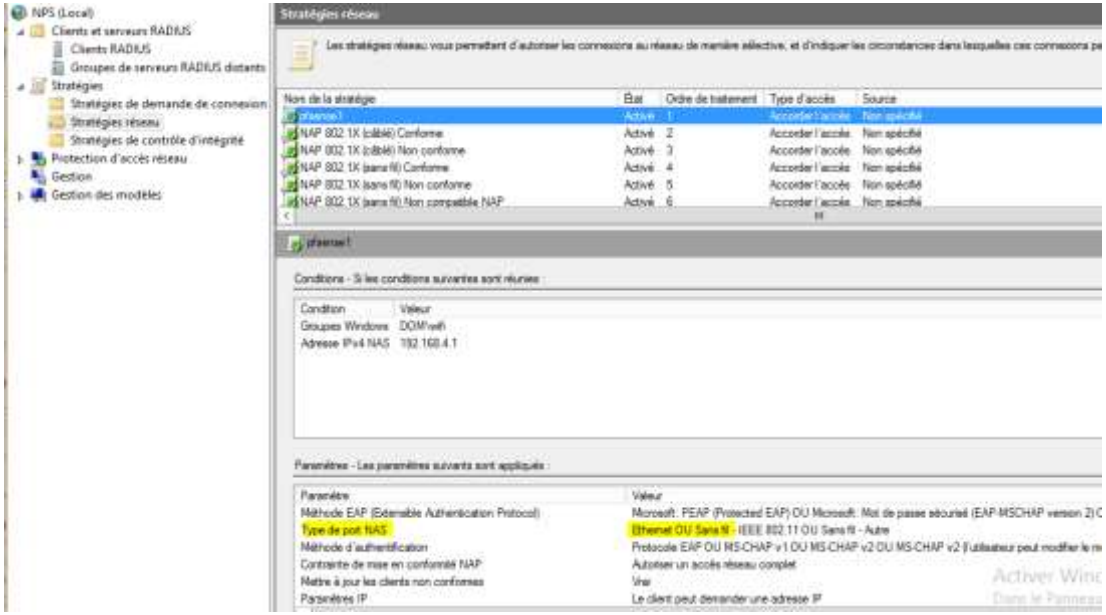
Et dans les règles (a affiner quand tout fonctionne)



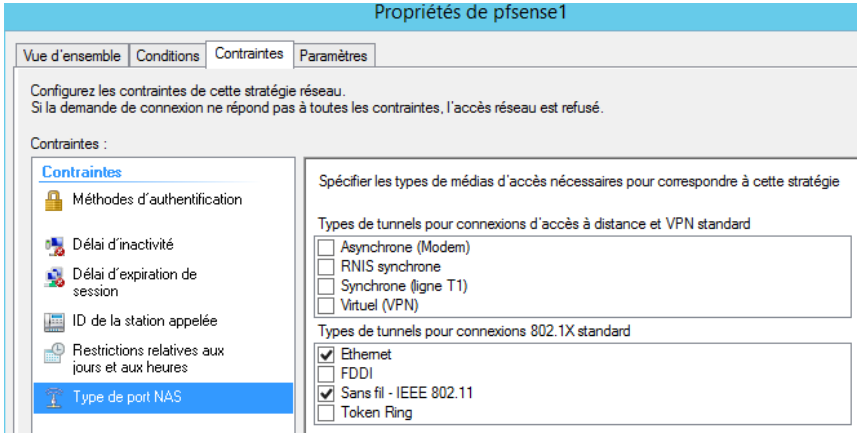
- Dans NPS Créer une stratégie qui corresponde

- Stratégie de demande client

- Puis dans les stratégies réseau :



Il faut aller dans les propriétés



Si la borne gère le multi Sssid, alors il est possible de mettre un ssid ‘portail’ avec la stratégie pfsense sur nps et l’affectation dans le vlan adapté (opt1 : pour internet) .

MULTI-SSID

On peut régler le second ssid pour accès sécurisé wpa2-radius sur le réseau LAN. Le client est alors la borne et il faut faire ne stratégie avec un autre groupe d’utilisateurs et définir l’adresse IPV4 du NAS avec l’adresse de la borne

POSSIBLE MESSAGES D’ERREUR SUR PFSENSE

Ping no buffer space available

- Redémarrer les interfaces : ifconfig de0 (ou de1, ou de2) down, puis ifconfig de0 up