

PORTAIL CAPTIF AVEC PFSENSE

TABLE DES MATIERES

Objectifs	1
Fonctionnement.....	1
Maquette	2
Pfsense	2
Interfaces	3
Portail captif.....	5
NPS.....	6
Mise en lien avec Radius - portail	8
déclaration du Certificat du domaine dans pfsense	8
Multi-SSID.....	16
Possible messages d’erreur sur pfsense	16

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

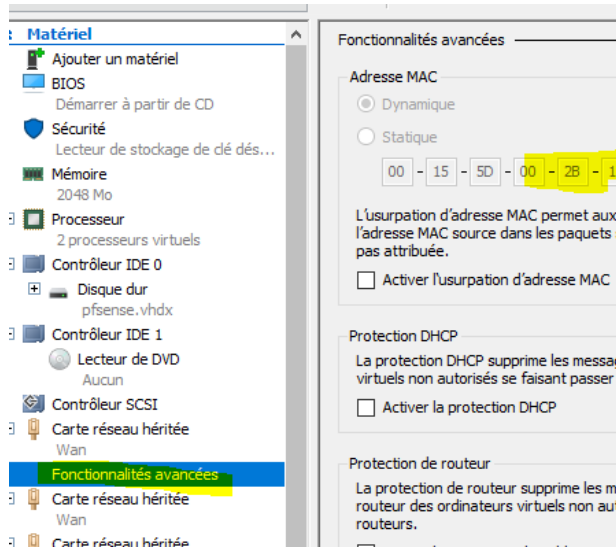
L'installation de pfSense se fait via l'image iso, il suffit de suivre les instructions.

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

pfsense			
Carte	Connexion	Adresses IP	État
Carte réseau héritée (MAC dynamique: 00:15:5D:00:2B:14) - Mode d'accès: VLAN 2	Wan	192.168.4.1, fe80:....	OK (Émulé)
Carte réseau héritée (MAC dynamique: 00:15:5D:00:2B:15) - Mode d'accès: VLAN 10	Wan	192.168.1.1, fe80:....	OK (Émulé)
Carte réseau héritée (MAC dynamique: 00:15:5D:00:2B:16)	Wan	192.168.0.17, fe80...	OK (Émulé)

Portail Captif - RADIUS

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

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.

Dans le menu Interface on obtient

Interfaces - x

	WAN		100baseTX	192.168.0.17	2a01:e35:2e77:5610:215:5dff:fe00:2b16
	LAN		100baseTX	192.168.1.1	
	OPT1		100baseTX	192.168.4.1	

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

Portail Captif - RADIUS

Floating WAN LAN **OPT1**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Act	
<input type="checkbox"/>	✓	32/932 KiB	IPv4 *	OPT1 net	*	*	*	*	none	Default allow LAN to any rule	

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

Captive Portal Configuration

Enable Enable Captive Portal

Interfaces

WAN

LAN

OPT1

Plus bas choisir authentication Local User

Authentication**Authentication
method** No Authentication Local User Manager /
Vouchers Allow only users/groups with "Captive portal login" privilege set

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

Portail Captif - RADIUS

Paramètres Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

PFsense1

Adresse (IP ou DNS) :

192.168.1.1

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel Générer

Secret partagé :

••••

Confirmez le secret partagé :

••••

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

On obtient (en tenant compte du tp précédent)

Portail Captif - RADIUS

Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'a

Nom convivial	Adresse IP	Fabricant du périphérique	Compatible avec la protection d'accès
wii-fit	192.168.0.160	RADIUS Standard	No
hp	192.168.1.162	RADIUS Standard	No
pfSense 1	192.168.1.1	RADIUS Standard	No

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 1^{er} 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

CAs Certificates Certificate Revocation

Create / Edit CA

Descriptive name

Method

Existing Certificate Authority

Certificate data

```
-----BEGIN CERTIFICATE-----
MIIDXzCCakegAwIBAgIQHMjs4xIXEbNnitTrEnSHyj
ANBgkqhkiG9w0BAQUFADBC
MRQwEgYKCZImiZPyLQG8GRYEZGVtbzETMBEGCgmSJo
mT8ixkARkWA2RvbTEVMBMG
A111FEAxMMZG9tL1VNSVj0xL11NBMB4XDTE2MTIwMzA3MT
-----
```

Paste a certificate in X.509 PEM format here.

Certificate Private

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

Portail Captif - RADIUS

Authentication

Authentication method: No Authentication, Local User Manager / Vouchers, RADIUS Authentication

RADIUS protocol: PAP, CHAP-MD5, MSCHAPv1, MSCHAPv2

Primary Authentication Source

Primary RADIUS server: IP address: 192.168.1.241, Port: 123456

Secondary RADIUS server: IP address of the RADIUS server to authenticate against, RADIUS port. Leave blank for default (1812)

Evidement il faudra faire mieux !

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

Logout popup window: Enable logout popup window
 If enabled, a popup window will appear w disconnect themselves before the idle or l

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

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

RADIUS Options	
Reauthentication	<input type="checkbox"/> Reauthenticate connected users every minute If reauthentication is enabled, Access-Requests will be sent to the RADIUS server for each user. If an Access-Reject is received for a user, that user is disconnected from the captive portal.
RADIUS MAC Authentication	<input type="checkbox"/> Enable RADIUS MAC authentication If this option is enabled, the captive portal will try to authenticate users by sending the password entered below to the RADIUS server.
MAC authentication secret	<input type="text"/>
RADIUS NAS IP Attribute	<input type="text" value="OPT1 - 192.168.4.1"/> Choose the IP to use for calling station attribute.
Session timeout	<input type="checkbox"/> Use RADIUS Session-Timeout attributes When enabled, clients will be disconnected after the amount of time retrieved from the RADIUS server.

- Positionner aussi le NAS identifiant pour que tout soit cohérent

NAS Identifier	<input type="text" value="pfsense1.dom.demo"/> Specify a NAS identifier to override the default value (pfSense.localdomain).
-----------------------	---

Activer le serveur DHCP sur l'interface Wifi

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

Portail Captif - RADIUS

DNS servers

Leave blank to use the system default servers configured on the System /

Other Options

Gateway

The default is to use the IP on this in

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)

Floating WAN LAN **OPT1**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 *	OPT1 net	*	*	*	*	none	Default allow Wifi to any rule	

🌐 Dans NPS Créer une stratégie qui corresponde

- Stratégie de demande client

Stratégies de demande de connexion

Les stratégies de demande de connexion vous permettent de spécifier si les demandes de connexion sont traitées localement ou si elles sont transférées vers des serveurs RADIUS distants. Pour les connexions NAP VPN ou 802.1X, vous devez configurer l'authentification PEAP dans la stratégie de demande de connexion.

Nom de la stratégie	État	Ordre de traitement	Source
NAP 802.1X (sans fil)	Activé	1	Non spécifié
Utiliser l'authentification Windows pour tous les utilisateurs	Activé	2	Non spécifié

NAP 802.1X (sans fil)

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Type de port NAS	Sans fil - Autre OU Sans fil - IEEE 802.11

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Fournisseur d'authentification	Ordinateur local
Configuration du protocole EAP (Extensible Authentication Protocol)	Configuré
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP) OU Microsoft: Carte à puce ou autre certificat OU Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)
Méthode d'authentification	Protocole EAP OU MS-CHAP v2 OU MS-CHAP v2 (l'utilisateur peut modifier le mot de passe après son expiration)
Remplacer l'authentification	Activé

Portail Captif - RADIUS

- Puis dans les stratégies réseau :

Nom de la stratégie	Etat	Ordre de traitement	Type d'accès	Source
psense1	Actif	1	Accorder l'accès	Non spécifié
NAP 802.1X (sans R)	Actif	2	Accorder l'accès	Non spécifié
NAP 802.1X (sans R) Non conforme	Actif	3	Accorder l'accès	Non spécifié
NAP 802.1X (sans R) Conforme	Actif	4	Accorder l'accès	Non spécifié
NAP 802.1X (sans R) Non conforme	Actif	5	Accorder l'accès	Non spécifié
NAP 802.1X (sans R) Non compatible NAP	Actif	6	Accorder l'accès	Non spécifié

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes Windows	DOM\win1
Adresse IP=4 NAS	192.168.4.1

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Méthode EAP (Extensible Authentication Protocol)	Microsoft PEAP (Protected EAP) OU Microsoft: Mail de passe sécurisé (EAP-MSCHAP version 2) C
Type de port NAS	Ethernet OU Sans fil IEEE 802.11 OU Sans fil - Autre
Méthode d'authentification	Protocole EAP OU MS-CHAP v1 OU MS-CHAP v2 OU MS-CHAP v2 (utilisateur peut modifier le m
Contrainte de mise en conformité NAP	Autoriser un accès réseau complet
Mettre à jour les clients non conformes	Via
Paramètres IP	Le client peut demander une adresse IP

Il faut aller dans les propriétés

Propriétés de psense1

Vue d'ensemble Conditions **Contraintes** Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

- Méthodes d'authentification
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS**

Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie

Types de tunnels pour connexions d'accès à distance et VPN standard

- Asynchrone (Modem)
- RNIS synchrone
- Synchrone (ligne T1)
- Virtuel (VPN)

Types de tunnels pour connexions 802.1X standard

- Ethernet
- FDDI
- Sans fil - IEEE 802.11
- Token Ring

Si la borne gère le multi Ssid, 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 une 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