AP 3 WIFI RADIUS

SADEK ADEL

SIO2

Je vais suivre la doc officielle https://support.hpe.com/hpesc/public/docDisplay?docId=c03767483&docLocale=fr_FR

-Je tague le port numéro 5 sur le switch aruba

-Je réinitialise la borne en appuyant sur le bouton reset pendant 7 sec

-L'ip de la borne par défaut au démarrage sera celle la 192.168.1.1 /24 je m'attribue une ip dans ce réseau je vais prendre la 192.168.1.5

-Sur la doc officielle ils demandent de mettre la borne HP comme passerelle par défaut et DNS je ne vois pas où est l'intérêt mais je le mets pour suivre la doc à la lettre

-La doc officiel n'est pas à jour la borne est adresser automatiquement via DHCP je suis partis dans les log DHCP et j'ai trouver l'adresse MAC de la borne HP et son ip

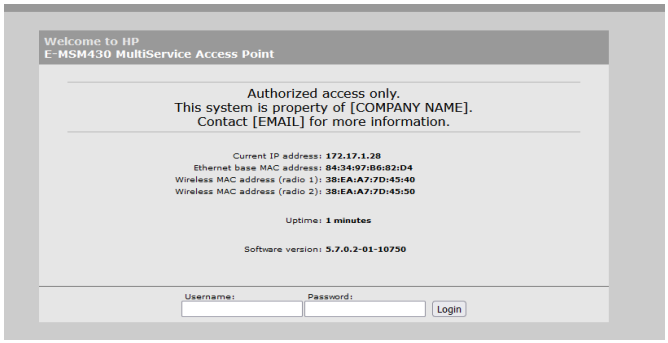
```
DHCPREQUEST for 172.17.1.28 from 84:34:97:b6:82:d4 (CN2BDWZ1KN) via eth0
DHCPACK on 172.17.1.28 to 84:34:97:b6:82:d4 (CN2BDWZ1KN) via eth0
reuse_lease: lease age 0 (secs) under 25% threshold, reply with unaltered, exist
DHCPREQUEST for 172.17.1.28 from 84:34:97:b6:82:d4 (CN2BDWZ1KN) via 172.17.1.50
DHCPACK on 172.17.1.28 to 84:34:97:b6:82:d4 (CN2BDWZ1KN) via 172.17.1.50
```

Son adresse ip = 172.17.1.28

Son adresse MAC = 84:34:97:b6:82:d4

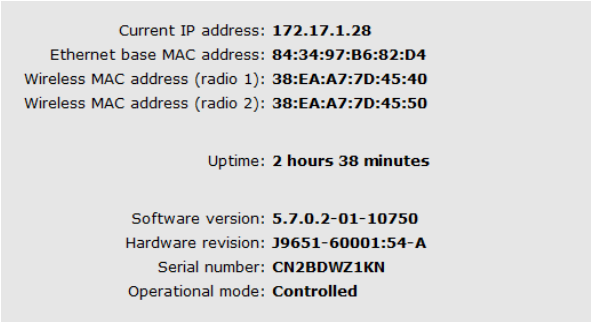
Je rentre cette adresse dans mon navigateur 172.17.1.28

Me voici sur la page de login de la borne



Login par défaut = admin/admin

Ensuite j'ai accès à ses informations



La borne est en mode controlled et on peut la faire passer en mode autonome je ne sais pas exactement ce que c'est mais peut être controlled c'est le mode distribué ou il y'a une borne centrale qui est relié à des bornes en connexion filaire et leur attribue une configuration (ip,vlan,ssid,wpa) pour que après elle fonctionne comme des bornes (point d'accès).

Ou le mode centralisé avec une borne centrale et d'autres bornes distante reliée en filaire avec cette borne centrale et fonctionne comme des ponts et répéteurs et retransmette les données à la borne centrale.

Et le mode autonome sa serait le mode infrastructure deux bornes communiquent via un point d'accès c'est le mode le plus simple et un BSSID qui sera l'adresse mac du point d'accès permettra d'identifier le réseau lors de la transmission sur les canaux 802.11 le BSSID est souvent supplanter par un ESSID qui s'appelle souvent SSID qui est le nom du réseau sur 32 caractères maximum.

Je fais une réservation d'IP pour la borne dans le vlan 10 elle gardera la même IP

```
host borneAdel {
hardware ethernet 84:34:97:B6:82:D4 ;
fixed-address 172.17.1.28 ;
}
```

Je passe la borne en mode autonome

Le souci maintenant c'est que malgré le fait que j'ai fait une réservation d'IP la borne à changer d'adresse mac et la réservation devient caduque la borne à eu l'IP : 172.17.1.40 maintenant

Extrait des logs DHCP :

```
DHCPACK on 172.17.1.40 to 38:ea:a7:7d:45:40 (CN2BDWZ1KN) via 172.17.1.1
reuse_lease: lease age 0 (secs) under 25% threshold, reply with unaltered, existing lease for 172.17.1.40
DHCPREQUEST for 172.17.1.40 (172.17.1.88) from 38:ea:a7:7d:45:40 (CN2BDWZ1KN) via 172.17.1.50
DHCPACK on 172.17.1.40 to 38:ea:a7:7d:45:40 (CN2BDWZ1KN) via 172.17.1.50
```

On voit bien que l'adresse mac a changé

Bien faire attention à sa et vérifier les baux dhcp

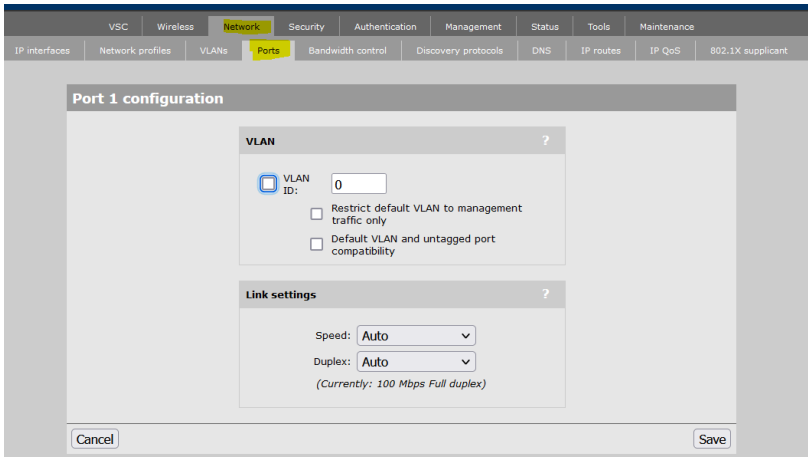
Ensuite j'arrive sur un écran qui me demande mon pays

Le nom de l'user admin l'ancien mdp et le nouveau mdp qui sera siojjr

Connexion de la borne sur un lien tagué

Jusqu'à maintenant la borne été directement connecter au vlan 10 via un port non tagué car je ne pouvais pas modifier le vlan ID dans l'interface de la borne car le port console été bloquer.

Donc pour modifier le vlan ID d'une interface il faut aller dans Network > Port > Choisir port1

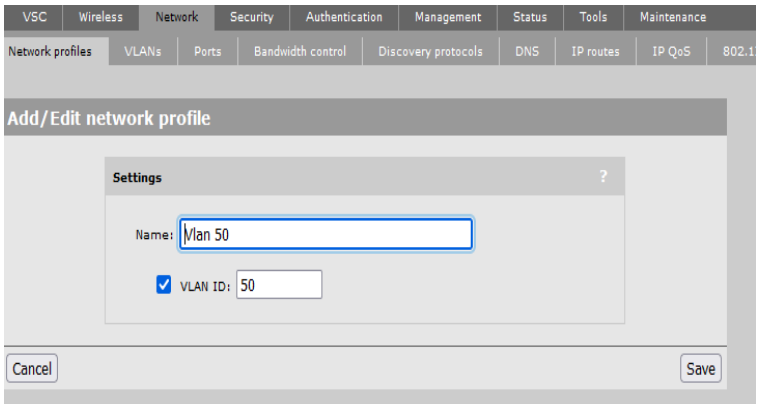


Je coche vlan ID et je mets le vlan 10,et je branche la borne sur un port trunker le port 5 du switch aruba

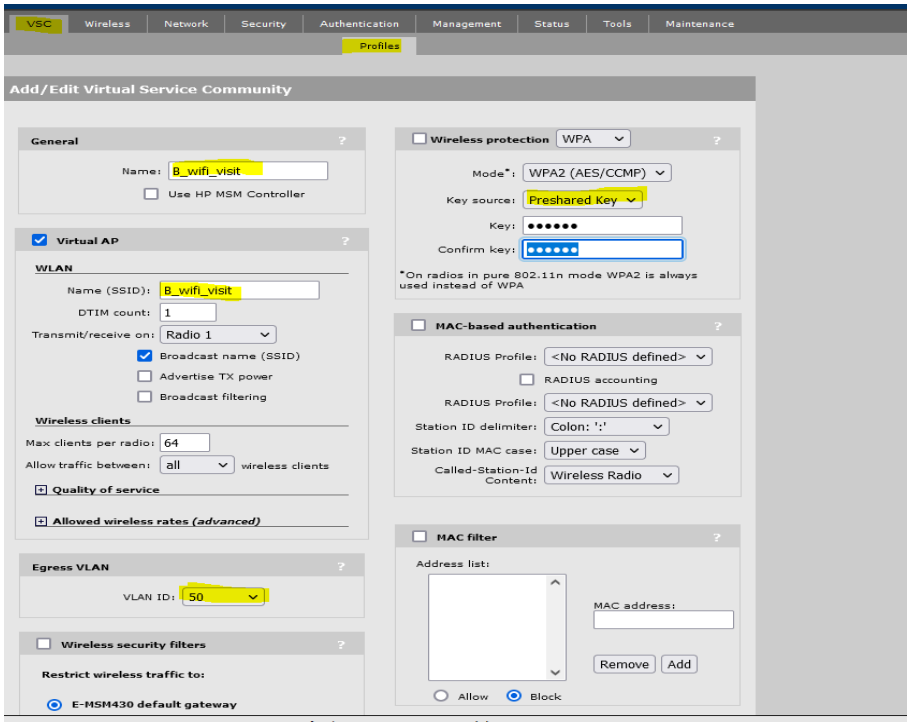
Ensuite je re-accède à la borne via son ip elle a encor changé d'ip sa sera 172.17.1.20

Avant de créer un SSID qui sera assigner au vlan 50 je dois créer ce profil réseau qui sera mapper au vlan 50 je dois aller network > network profiles

Je crée un nouveau profil qui s'appellera VLAN 50 et qui aura comme VLAN ID le numéro 50 ne pas oublier de cocher la case pour l'activer



Ensuite je crée un nouveau réseau Wi-Fi je vais dans VSC et je crée un nouveau profile



Je définis un nom (SSID) le vlan ID et l'authentification se fera avec une clé prée-partager et sera crypter avec WPA2-AES je ne mets pas d'authentification RADIUS pour l'instant sa sera plus tard

Ensuite je valide et le réseau s'affiche sur mon téléphone je mets mon mdp et sa fonctionne parfaitement

Je crée le VLAN 51 et son ip réseau sera 192.168.0.0/24

Ensuite en regardant dans le DHCP je vois qu'une ip a été attribuer à mon téléphone avec son adresse MAC un relais DHCP a été automatiquement mis en place sur ma borne wifi

```
DHCPDISCOVER from 3e:9c:b2:3b:82:c4 via 172.19.0.1
DHCPOFFER on 172.19.0.9 to 3e:9c:b2:3b:82:c4 via 172.19.0.1
reuse_lease: lease age 115 (secs) under 25% threshold, reply with unaltered, existing lease for 172.19.0.

DHCPREQUEST for 172.19.0.9 (172.17.1.88) from 3e:9c:b2:3b:82:c4 via 172.19.0.1
DHCPACK on 172.19.0.9 to 3e:9c:b2:3b:82:c4 via 172.19.0.1
reuse_lease: lease age 115 (secs) under 25% threshold, reply with unaltered, existing lease for 172.19.0.
```

Sur le switch aruba je mets ceci

```
HP-2530-8-PoEP(eth-5)# vlan 51
HP-2530-8-PoEP(vlan-51)# tagu
Invalid input: tagu
HP-2530-8-PoEP(vlan-51)# tagged port 5
Module not present for port or invalid port: port
HP-2530-8-PoEP(vlan-51)# tagged  5
HP-2530-8-PoEP(vlan-51)#
```

Sur mes autres ports taguer j'autorise le vlan 51 à passer

Sur le switch cisco déjà sur les ports taguer j'autorise tout les vlan du numéro 2 au 4091 pour être tranquille sur mes autres AP

Ensuite après avoir créer le vlan 51 je le vois activer dans les ports taguer

```
Port        Vlans allowed and active in management domain
Fa0/20      10,20,30-31,40,50-51,60,70
Fa0/21      10,20,30-31,40,50-51,60,70
Fa0/22      10,20,30-31,40,50-51,60,70
Fa0/23      10,20,30-31,40,50-51,60,70
Gi0/1       10,20,30-31,40,50-51,60,70

Port        Vlans allowed and active in management domain
Gi0/2       10,20,30-31,40,50-51,60,70
```

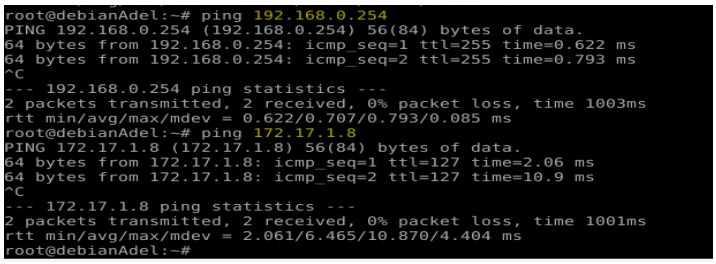
Ensuite je dois sur mes 2 routeurs ajouter une nouvelle interface virtuelle

Routeur 1 (master) :

```
routeurSlave(config)#interface gigabitEthernet 0/0.51
routeurSlave(config-subif)#encapsulation dot1q 51
routeurSlave(config-subif)#ip addr
routeurSlave(config-subif)#ip address 192.168.0.254 255.255.255.0
```

Avant de passer au second routeur je place une machine dans ce réseau et teste le ping

Je peux pinger le routeur et mon serveur DNS

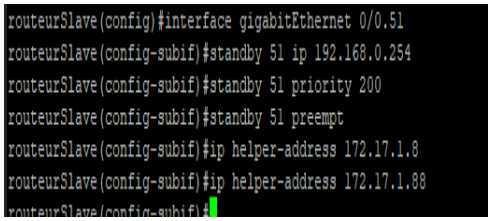


C'est parfait maintenant l'ip du routeur master dans le vlan 51 sera la 192.168.0.250

Celle du routeur slave : 192.168.0.251

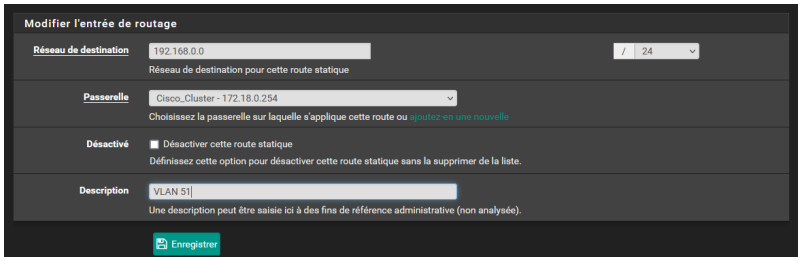
Et leur ip virtuelle 192.168.0.254

Ici les commandes réaliser sur le routeur master



J'ai mis en place l'agent relais aussi

Ensuite je rajoute une route sur le pfsense vers le nouveau réseau



Sur la borne je crée un nouveau profil wifi

Mapper avec le vlan 51

Avant sa sur le serveur DHCP je crée la nouvelle plage ip

```
#VLAN 51 WIFI 2

subnet 192.168.0.0 netmask 255.255.255.0{
#pool{
#       failover peer "test";

        range 192.168.0.1 192.168.0.100;
        option routers 192.168.0.254;
#       option domain-name-servers 192.168.0.21,192.168.0.204 ;
        option domain-name-servers 172.17.1.8, 172.17.1.88;
```

Je peux maintenant terminer la création du nouveau réseau wifi

Le voila crée

Name	SSID	VLAN		IP	MAC	TKIP	AES	WEP	802.1x	MAC	
Booktic_wifi_E	Booktic_wifi_E	51	DiffSrv	-	-	-	✓	-	-	-	1
B_wifi_visit	B_wifi_visit	50	DiffSrv	-	-	-	✓	-	-	-	1

Je vérifie sur mon téléphone s'il est bien présent

Cela fonctionne parfaitement j'ai réussi à me connecter et en parallèle j'ai regardé dans les logs du serveur si une ip a bien été distribué dans le réseau du vlan 51

```
Jan  5 11:39:02 srvdhcp dhcpd[50652]: reuse_lease: lease age 0 (secs) under 25%
threshold, reply with unaltered, existing lease for 192.168.0.2
Jan  5 11:39:02 srvdhcp dhcpd[50652]: DHCPREQUEST for 192.168.0.2 (172.17.1.88)
from 86:5c:71:41:d4:84 via 192.168.0.250
Jan  5 11:39:02 srvdhcp dhcpd[50652]: DHCPACK on 192.168.0.2 to 86:5c:71:41:d4:8
4 via 192.168.0.250
```

Sur le pare feu pfsense je fais une règle interdisant tout les flux http et https de passer si ce n'est par le proxy

Ensuite je rajoute dans squidGuard le vlan51

Maintenant je passe aux ACL sur Cisco

<u>Je configure une ACL étendue pour le vlan 50</u>

```
routeurMaster(config)#ip access-list extended filtrage
routeurMaster(config-ext-nacl)#permit ip any 172.17.1.0 0.0.0.255
routeurMaster(config-ext-nacl)#deny any any
                               ^
% Invalid input detected at '^' marker.

routeurMaster(config-ext-nacl)#deny ip any any
routeurMaster(config-ext-nacl)#interface gig
routeurMaster(config-ext-nacl)#interface giga 0/0.50
routeurMaster(config-subif)#ip access-group filtrage in
routeurMaster(config-subif)#
```

Je crée l'ACL avec le nom « filtrage » et j'autorise le trafic ip qui englobe TCP et UDP vers le réseau du VLAN 10

Et j'interdis tout autre trafic ip vers n'importe où (un peu comme POLICY sur iptables)

Ensuite je configure l'ACL pour le vlan 51 pour autoriser un accès que vers internet

Sa veut dire que je n'autorise le vlan 51 qu'a communiquer avec le proxy

```
routeurMaster(config)#ip access-list extended vlan51
routeurMaster(config-ext-nacl)#permit ip any host 172.17.1.84
routeurMaster(config-ext-nacl)#deny ip any any
routeurMaster(config-ext-nacl)#
```

```
routeurMaster(config-subif)#ip access-group vlan51 in
routeurMaster(config-subif)#no ip access-group vlan51 in
routeurMaster(config-subif)#interface giga 0/0.51
routeurMaster(config-subif)#ip access-group vlan51 in
```

Ip access-list extended <nomACL>

Permit <protocole> <source> <destination>

L'acl fonctionne parfaitement je ne peux pas pinguer mon réseau interne mais je peux aller sur internet en passant par le proxy

Pour loguer toutes les connexions et les archiver

Je vais afficher la date au format ISO avec -I dans mon script car sinon je ne pourrai pas enregistrer le fichier à la date du jour je met date -I

Script qui filtre les log en fonction de l'user

```
#!/bin/bash
#JE FILTRE LES LOGS
cat /var/log/squid/access.log.1 | grep adel
#JE RECUPERE L'ETAT DE LA COMMANDE PRECEDENTE POUR VOIR SI IL YA DES LOGS QUI CONCERNENT CET USER
etat=$?
#CONDITION QUI RENVOIE TOUT LES LOG DANS UN FICHIER  LE COMPRESSE ET L ENREGISTRE A LA DATE DU JOUR EN MODE ISO -I
#POUR QUE SA PUISSE ETRE ENREGISTRER
#ENSUITE JE SUPPRIME LE FICHIER .GZ AVEC LE NOM DE BASE JE REFAIS UN FICHIER DE LOG ET JE MET LES DROITS TOTAL POUR TOUT LE MONDE
if [ $etat -eq 0 ]
        then
                echo "LOG POUR L UTILISATEUR ADEL" >> logFiltre.txt
                echo $(date) >> logFiltre.txt
                echo "" >> logFiltre.txt
                cat /var/log/squid/access.log.1 | grep adel >> logFiltre.txt
                echo "FIN LOG" >> logFiltre.txt
fi
```

Script pour l'archivage

```
#!/bin/sh
#COMPRESSE LES LOG ET ENVOIE CETTE COMPRESSION VERS UN FICHIER ENREGISTRER AVEC LA DATE DU JOUR
gzip /var/log/squid/access.log.1 >$(date -I).gz -f
echo "" > access.log.1
#FICHIER ENVOYER DANS UN REPERTOIRE D'ARCHIVE
mv $(date -I).gz /archivage/squid/
```

Crontab (script exécuter tout les jours)

```
# m h  dom mon dow   command
# * * 15 * * /root/filtreLog.sh
 * * */1 * * /var/log/squid/filtreLog.sh
 * * */1 * * /var/log/squid/archivage.sh
```