UCOPIA

TURN YOUR WI-FI UP

Architecture Out Of Band
Ucopia avec Ruckus vSZ-H

Mai 2016

Table des matières

1. Objectif

Ce document a pour objectif de se familiariser avec l'architecture Out-of-Band dans le cadre d'un WiFi constructeur Ruckus avec un contrôleur vSZ-H.
L'architecture Out-of-Band est disponible depuis la version 5.0.11.

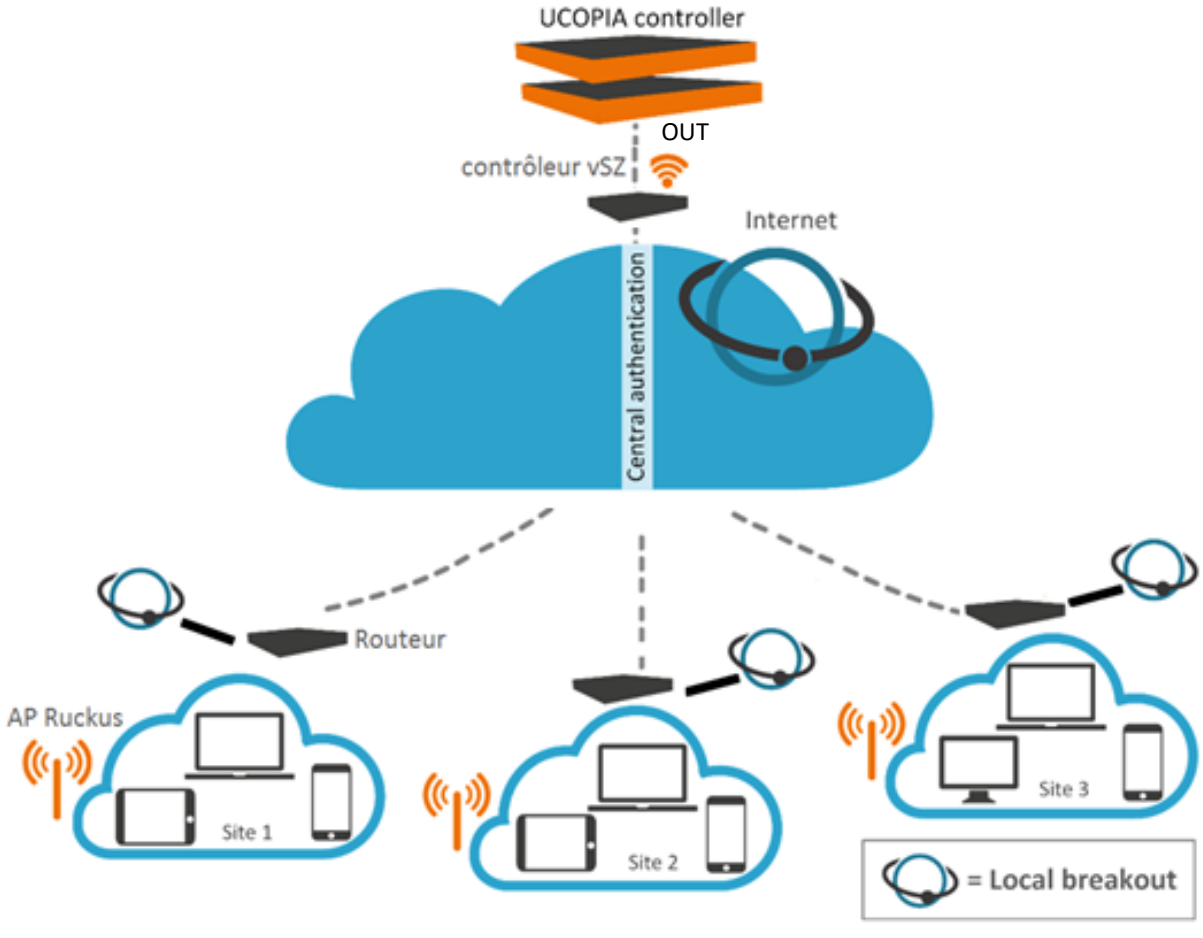
Nous verrons les différentes étapes ci-dessous :

- Architecture de la solution
- Cinématique de fonctionnement
- Prérequis au déploiement de la solution
- Configuration du contrôleur vSZ
- Configuration du contrôleur UCOPIA

2. Architecture

L'architecture Out-of-Band constructeur Ruckus avec contrôleur vSZ est composée de :

- Un contrôleur vSZ central qui gère l'ensemble des bornes des différents sites.
- Un contrôleur Ucopia central et accessible depuis Internet, qui délivre le portail captif et authentifie les utilisateurs.

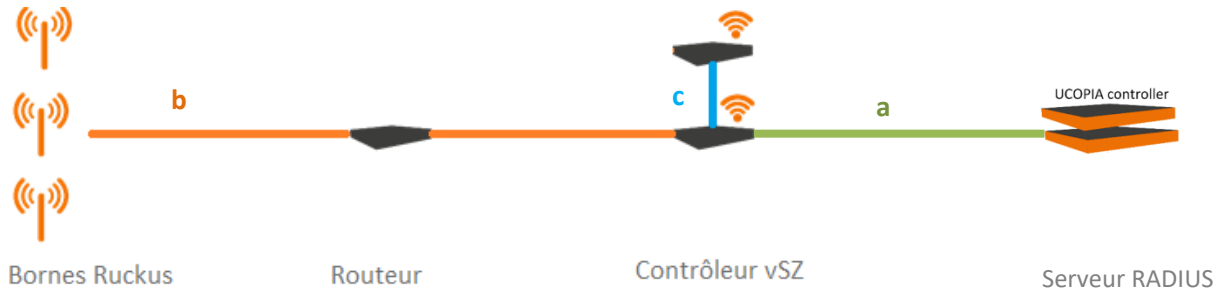


Le contrôleur UCOPIA centralise la configuration des profils, zones, politiques de récupération de mot de passe, services et portail.
Le contrôleur vSZ centralise le management des bornes et l'interrogation auprès du serveur RADIUS (qui sera l'UCOPIA).
Les routeurs sur chaque site correspondent à la Gateway par laquelle passent les flux des utilisateurs authentifiés sur le site en question (échappement local).

3. Généralités sur Ruckus

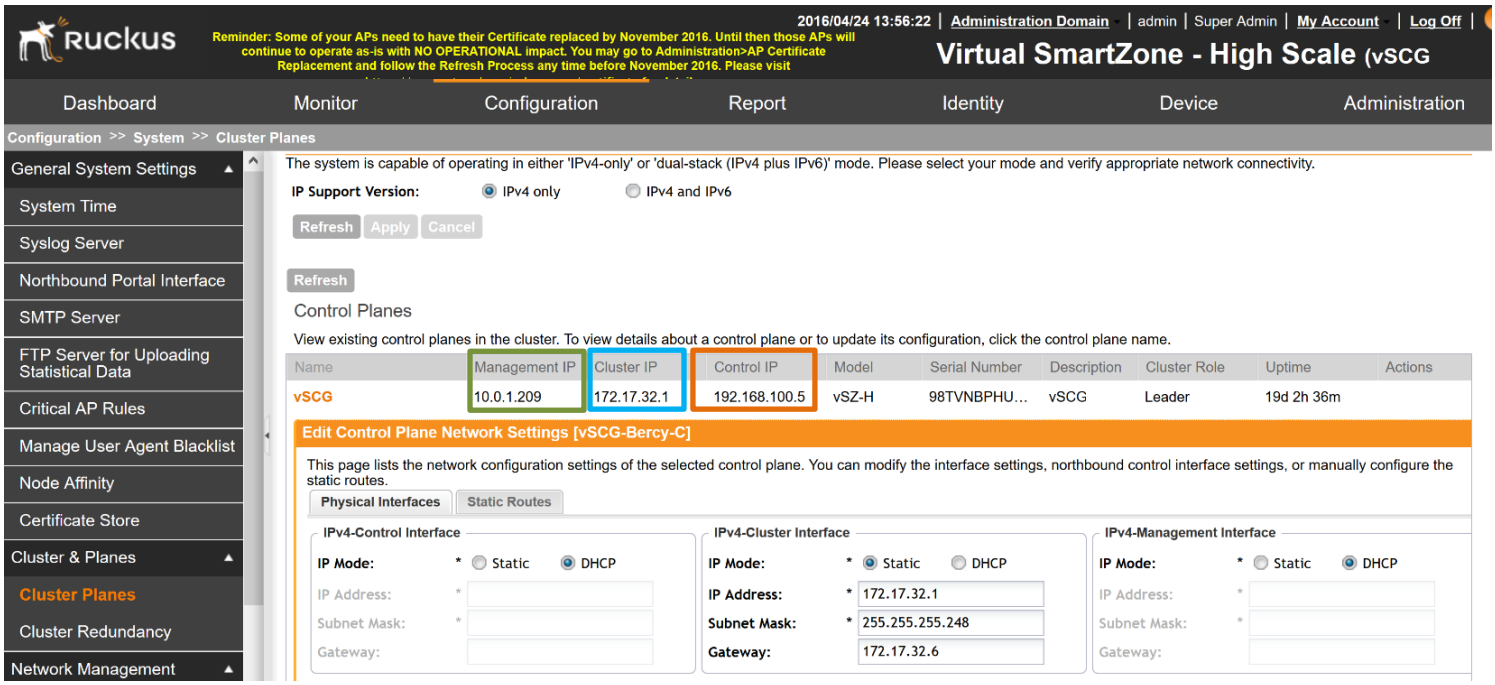
Ruckus propose 2 types de contrôleurs de bornes Ruckus :

- **Zone Director** : allant de la gamme conçue pour les plus petits déploiements, à destination des PME, à des gammes gérant jusque 1 000 points d'accès. *Ex : ZD 1200, ZD 3000, ZD 5000*
- **vSZ (virtual Smart Zone)**, anciennement SCG (SmartCell Gateway), adapté aux plus gros déploiements. Il existe 2 gammes de vSZ :
    - vSZ-E (vSZ-Enterprise) : VM gérant jusque 1 024 AP et adaptée pour les entreprises. La VM n'a qu'une interface réseau.
    - vSZ-H (High-Scale) : VM gérant jusque 10 000 AP et adaptée pour les opérateurs faisant du multi-tenants. La gamme vSZ est sous forme de machine virtuelle uniquement, et prend en charge les hyperviseurs VMware et KVM les plus déployés. La VM a 3 interfaces réseau :
        a. l'interface de management (pour communication type RADIUS)
        b. l'interface de contrôle (pour communication avec les bornes)
        c. l'interface de cluster (pour faire de la haute disponibilité)



Interface de management
Interface de contrôle
Interface de cluster

Vous pouvez voir les différentes interfaces du contrôleur vSZ et leur adresse IP sur le dashboard de Ruckus sous **Configuration > System > Cluster Planes**, comme illustré ci-dessous :



Pour plus d'informations sur les gammes de contrôleurs WiFi Ruckus, veuillez-vous rendre sur leur site web : http://fr.ruckuswireless.com/products

4. Cinématique de fonctionnement

C'est dans le cadre de l'Alliance Program d'Ucopia, programme regroupant les partenariats constructeurs, qu'Ucopia et Ruckus Wireless se sont rapprochés, afin de travailler ensemble sur le marché des implémentations de réseaux sans fil.

4.1 Compatibilité Ruckus - Ucopia

Aujourd'hui, Ucopia a **validé le fonctionnement de ses contrôleurs avec la gamme Zone Director ainsi que la gamme vSZ-H de Ruckus, à partir de la version 3.1**. En revanche, la compatibilité n'a pas encore été testée ni validée pour la gamme vSZ-E de Ruckus, dans le cadre d'une architecture Out-of-Band.

Dans la suite de ce document, nous nous concentrons sur le fonctionnement d'UCOPIA avec un contrôleur vSZ-H, dans le cadre d'une architecture Out-of-Band.

4.2 Architecture Out-of-Band et cheminement des flux

Les principales étapes de cheminement des flux sont :

a- Connexion au réseau WiFi et association à la borne WiFi

b- Première requête web d'un utilisateur non authentifié (qui demande par exemple http://www.free.fr)

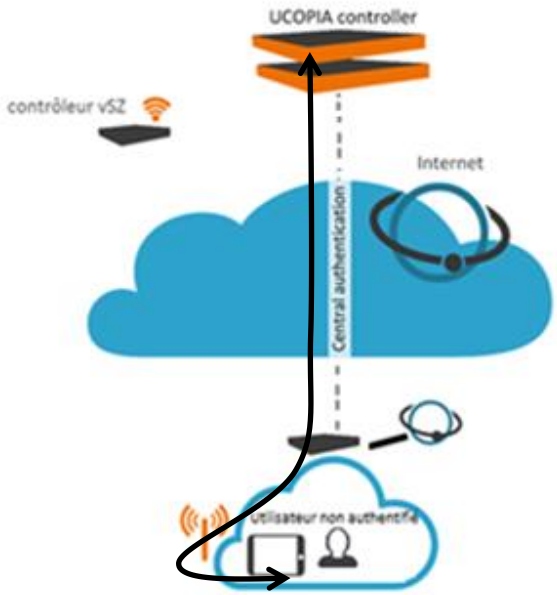
c- Redirection de la requête par la borne vers le portail captif d'Ucopia

d- Indication du login / mot de passe (pour une authentification standard, par exemple)

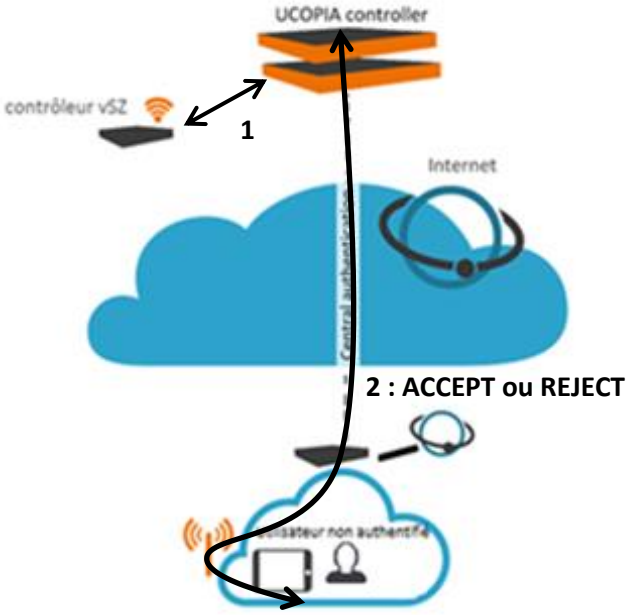
e- Envoi des informations d'authentification par Ucopia vers le vSZ qui envoie les requêtes au serveur RADIUS d'UCOPIA. Celui-ci répond au vSZ avec un message ACCEPT ou REJECT.

f- Navigation de l'utilisateur authentifié avec succès si bons identifiants

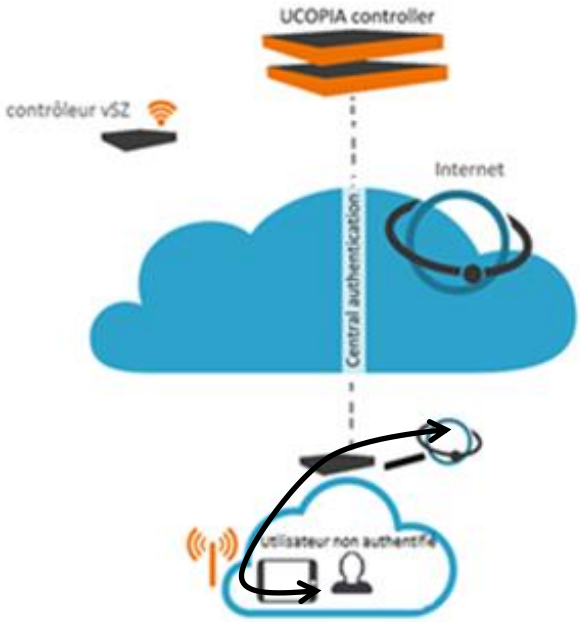
Etapes a, b, c et d : Redirection d'une requête web d'un utilisateur non authentifié vers le portail captif qui entre son login / mot de passe pour se connecter



Etape e : échanges entre le contrôleur UCOPIA, le serveur RADIUS (UCOPIA ou équipement tierce) et le vSZ



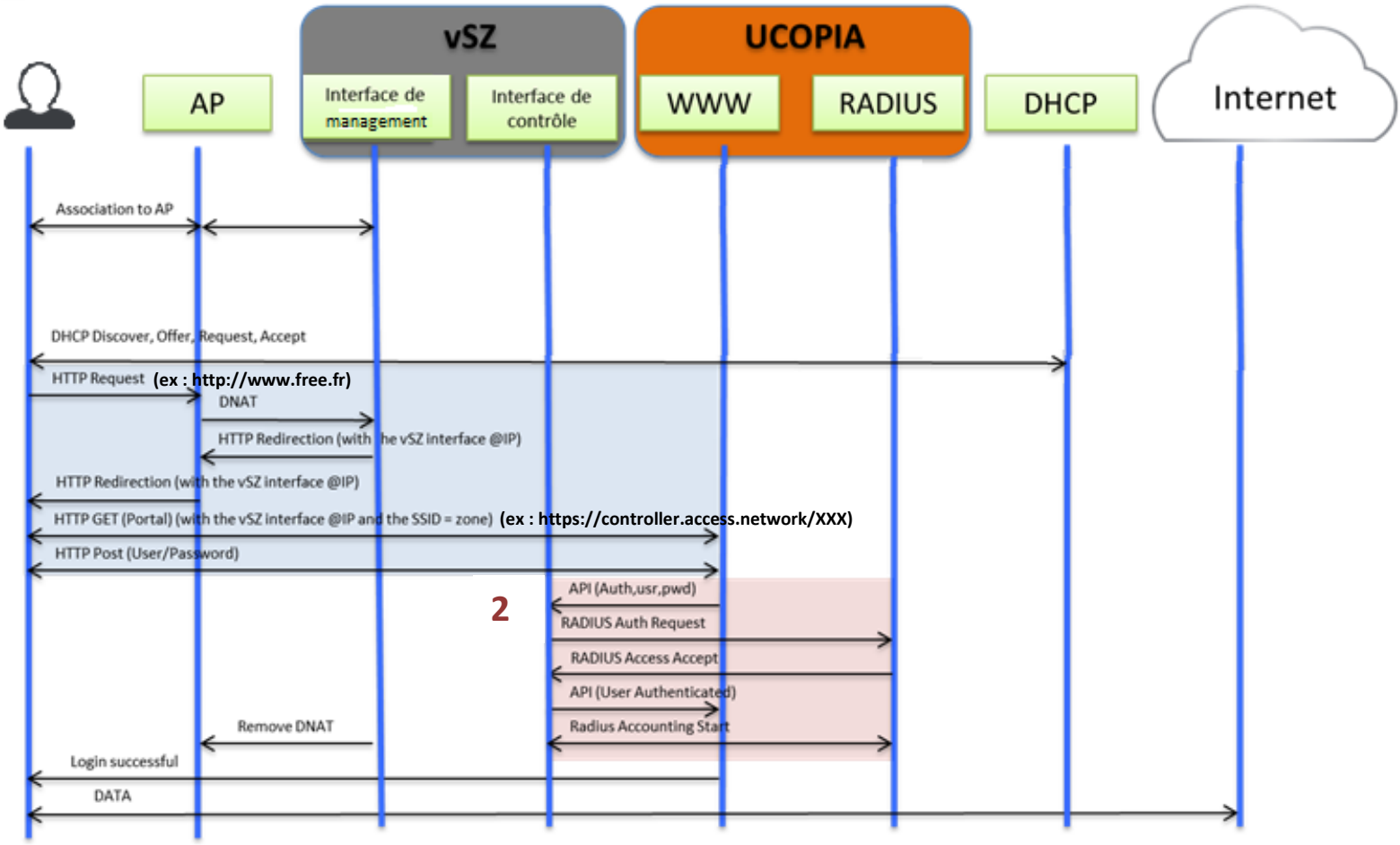
Etape f : navigation de l'utilisateur sur Internet, avec un échappement local (si ACCEPT)



4.3 Diagramme des messages échangés

4.2.1 Lors d'une 1re connexion sur le réseau WiFi

Voici les principaux échanges de flux entre les équipements UE / AP / vSZ / UCOPIA, lorsqu'un utilisateur se connecte pour la 1re fois sur le réseau WiFi :



1 : REQUÊTES HTTP

Quand un utilisateur arrive sur le réseau WiFi pour la première fois :

- Il reçoit une adresse IP par le serveur DHCP ;
- Puis, il envoie sa requête http (ex : http://www.free.fr) qui est DNATé par la borne, i.e. que celle-ci remplace l'@IP destination par celle du vSZ. Le vSZ invite l'utilisateur non authentifié à renvoyer sa requête http à l'UCOPIA, et lui indique :
    - Un de ses @IP (nous verrons laquelle plus précisément, dans le § 6. Prérequis)
    - L'@IP de l'utilisateur
- Enfin, l'utilisateur fait sa requête web directement à l'UCOPIA, avec une URL de type :

https://controller.access.network/zone/<nom de la zone>?nbiIP=<@IP du vSZ>etc, qui lui retournera le portail captif d'Ucopia.

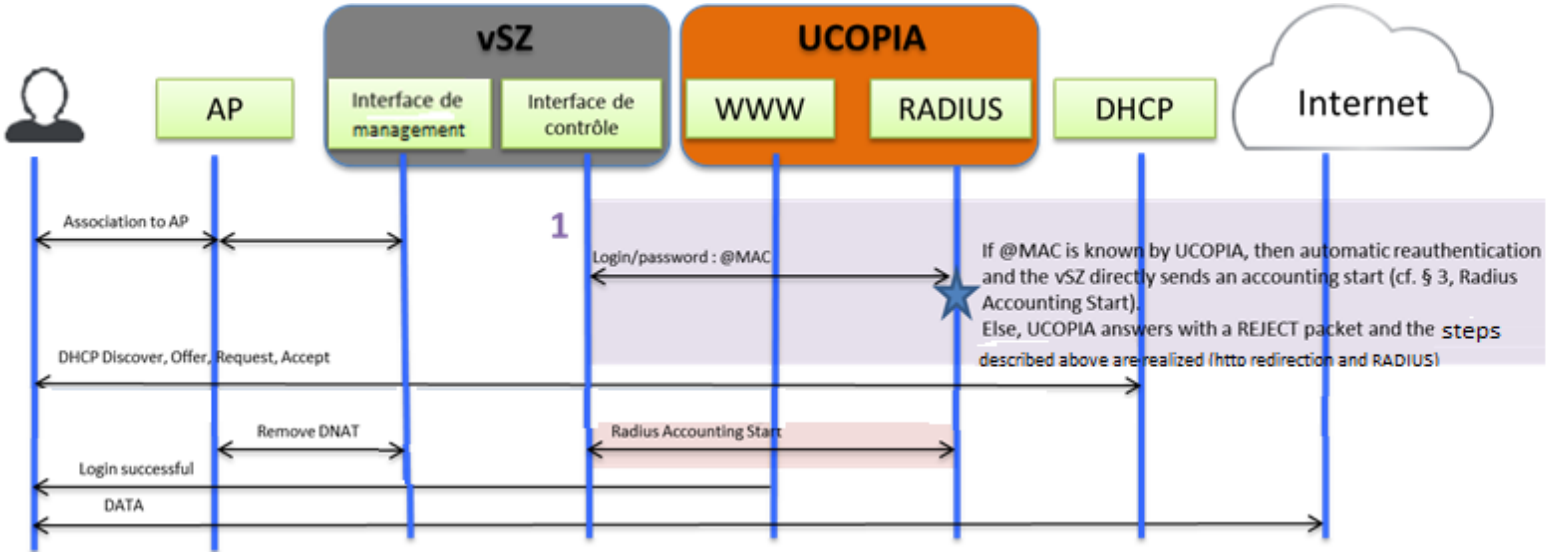
Pour plus d'informations sur la requête http GET envoyée par le vSZ, vous pouvez vous référer à l'annexe 1.

2 : ECHANGES ENTRE UCOPIA ET RADIUS

Une fois que l'user a envoyé à UCOPIA sa requête http et entré ses identifiants, l'UCOPIA et vSZ échangent via une API car c'est le vSZ qui interrogera toujours le serveur RADIUS.
UCOPIA reçoit de la part de vSZ (qui est son NAS) une requête RADIUS indiquant entre autres adresses IP, MAC… Si UCOPIA accepte la requête RADIUS, alors le vSZ envoie un « Accounting start ».

4.2.2 Lors d'une reconnexion sur le réseau WiFi

Voici les principaux échanges de flux entre les équipements UE / AP / vSZ / UCOPIA, lorsqu'un utilisateur qui s'est déjà authentifié sur le réseau WiFi s'y connecte de nouveau :



REAUTHENTIFICATION AUTOMATIQUE PAR ADRESSE MAC

A chaque nouvelle association de l'user à une AP, vSZ envoie une requête à UCOPIA, avec comme login/mdp = @MAC de l'user.
→ Si UCOPIA ne trouve pas l'@MAC dans sa base d'utilisateurs interne, alors il envoie un Reject et les échanges présentés ci-dessus (pour la présentation du portail captif) sont réalisés.

→ Sinon, UCOPIA envoie un « Access accept » au vsZ. Le vSZ envoie ensuite un « Accounting start » (en indiquant l'@IP de l'utilisateur) à Ucopia et l'utilisateur est connecté à Internet.

5. Avantages et considérations

5.1 Avantages de l'architecture Out-Of-Band

5.2.1 Centralisation des comptes utilisateurs

Les comptes utilisateurs sont centralisés sur le contrôleur dans le cloud. L'architecture permet à un utilisateur de se connecter avec un même compte sur l'ensemble des sites gérés par le contrôleur UCOPIA, et permet d'assurer la fonction de roaming.

5.2.2 Centralisation des portails captifs

Les portails captifs sont centralisés sur le contrôleur dans le cloud.
La modification d'un portail captif sur le site central est prise en compte par les utilisateurs sur l'ensemble des sites.

5.2.3 Echappement local

Chaque site local utilise son propre accès Internet pour la connexion des utilisateurs et évite de remonter l'ensemble flux par le contrôleur sur une sortie Internet centralisée.

5.2.4 Mutualisation de la licence

Une licence globale sur le site central est contractée. Cette licence est mutualisée sur l'ensemble des sites locaux.
Aucune licence sur les sites locaux ne sera contractée.

5.2 Considérations

5.2.1 Journaux utilisateurs

Les sessions utilisateurs sont centralisées sur le contrôleur dans le cloud.
Cependant, les paquets (trafic utilisateur) et les URLs visitées sont, eux, uniquement vus par les bornes mais ne sont pas stockés. Ainsi, la traçabilité du trafic, qui est requise par la loi dans de nombreux pays européens doit être réalisée par un équipement tiers sur site et ne peut pas être assurée par l'Ucopia en central

5.2.2 Coupure de liaison du site central

Le site central est l'unique annuaire de l'architecture.
Les sites locaux ne sont donc pas autonomes en cas de coupure de la liaison vers le site central.
Ucopia recommande fortement de redonder le contrôleur sur le site central.

5.2.3 Restriction aux sites gérés par un vSZ

Cette documentation ne présente que le cas d'architecture Out-Of-Band constructeur Ruckus et ne s'applique qu'aux sites ayant des bornes gérées par le contrôleur vSZ-H Ruckus.

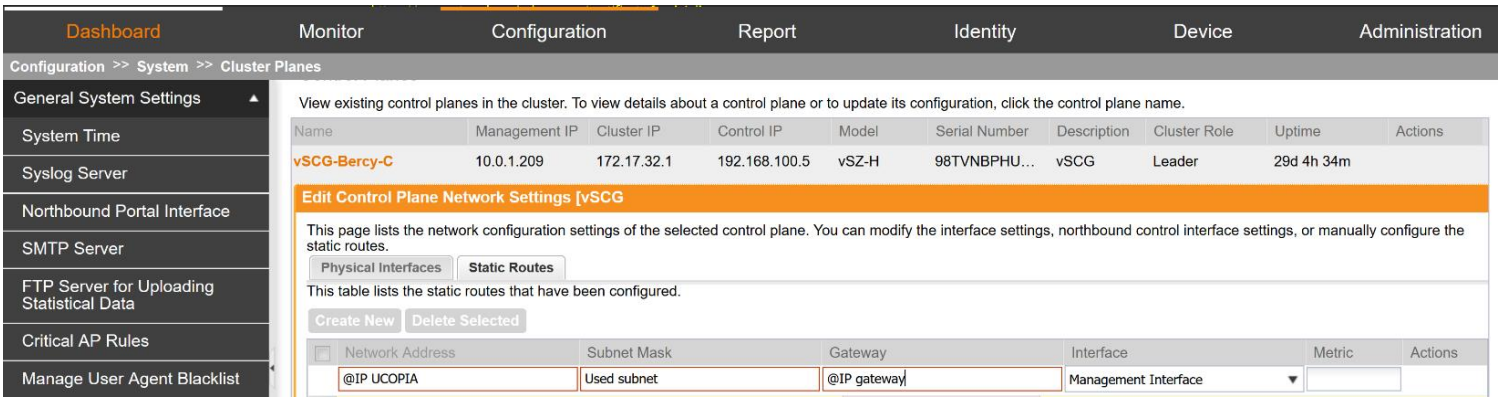
D’autres équipements sont compatibles avec UCOPIA et peuvent s’intégrer dans une architecture Out-of-Band tels que Meraki, Aerohive et le routeur DSL One Access.

6. Prérequis

- Le contrôleur vSZ doit être un contrôleur vSZ-H, de version minimale 3.1. La compatibilité d’UCOPIA avec les autres contrôleur WiFi de Ruckus n’a pas été validée (sauf pour les contrôleurs Zone Director).

- Le SSID sur chaque site doit être exactement identique au nom d’une zone entrée dans UCOPIA. Cette condition est nécessaire aussi bien pour faire de la reconnexion automatique par adresse MAC que pour avoir l’affichage du portail captif. Pour plus d’informations sur la raison de ce prérequis, vous pouvez vous référer aux annexes 2 et 3.

- Il est recommandé d’utiliser l’interface de management pour la communication entre le vSZ-H et l’Ucopia. Pour ce faire, il suffit d’ajouter dans la table de routage du vSZ une route statique indiquant d’emprunter l’interface de management du vSZ pour atteindre Ucopia (dashboard Ruckus > **Configuration > System > Cluster Planes > Static Routes**). Ainsi, toute requête à destination du nom de domaine d’UCOPIA (ex : « controller.access.network ») doit être résolue par le vSZ et routée vers l’interface de management.



Si vous souhaitez utiliser une autre interface du contrôleur vSZ que son interface de management (ex : interface de contrôle), pour communiquer avec Ucopia, alors vous devez vous assurer que l’interface de contrôle est bien la gateway, vers lesquels les flux en direction d’Ucopia sont routés (souvent, l’interface de contrôle étant la gateway par défaut)

- Communication entre les équipements

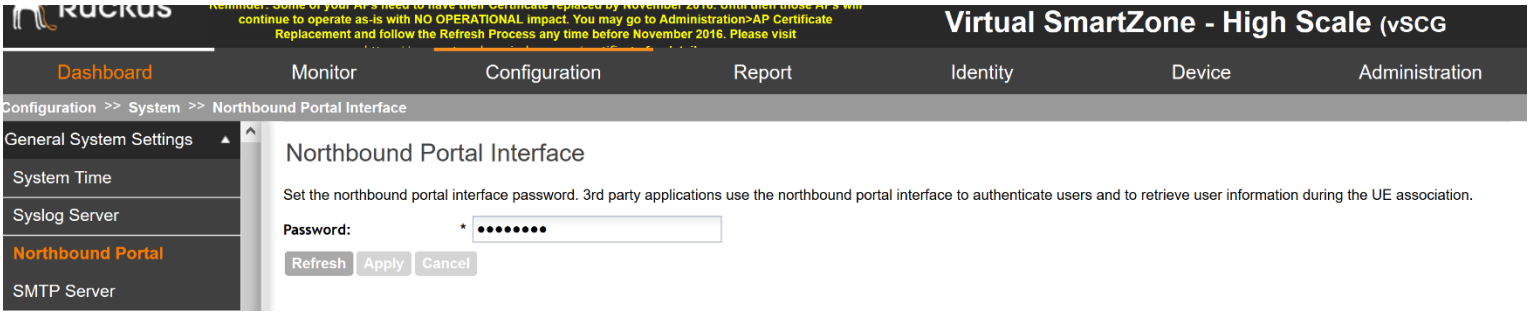
Les communications à ouvrir pour réaliser cette architecture sont les suivantes :

IP Source	IP destination	Port	Objectif
Adresse IP de l'utilisateur	Adresse IP du vSZ (interface de contrôle)	TCP/443	Redirection vers le portail Ucopia
Adresse IP de l'utilisateur	Adresse IP de l'Ucopia (interface IN ou OUT)	TCP/443	Affichage du portail
Adresse IP du vSZ (de préférence utiliser l'interface de management)	Adresse IP de l'Ucopia (interface IN ou OUT)	TCP/9080	Communication API
Adresse IP du vSZ (de préférence utiliser l'interface de management)	Adresse IP de l'Ucopia (interface IN ou OUT)	UDP/1812	Authentification Radius
Adresse IP du vSZ (de préférence utiliser l'interface de management)	Adresse IP de l'Ucopia (interface IN ou OUT)	UDP/1813	Radius Accounting

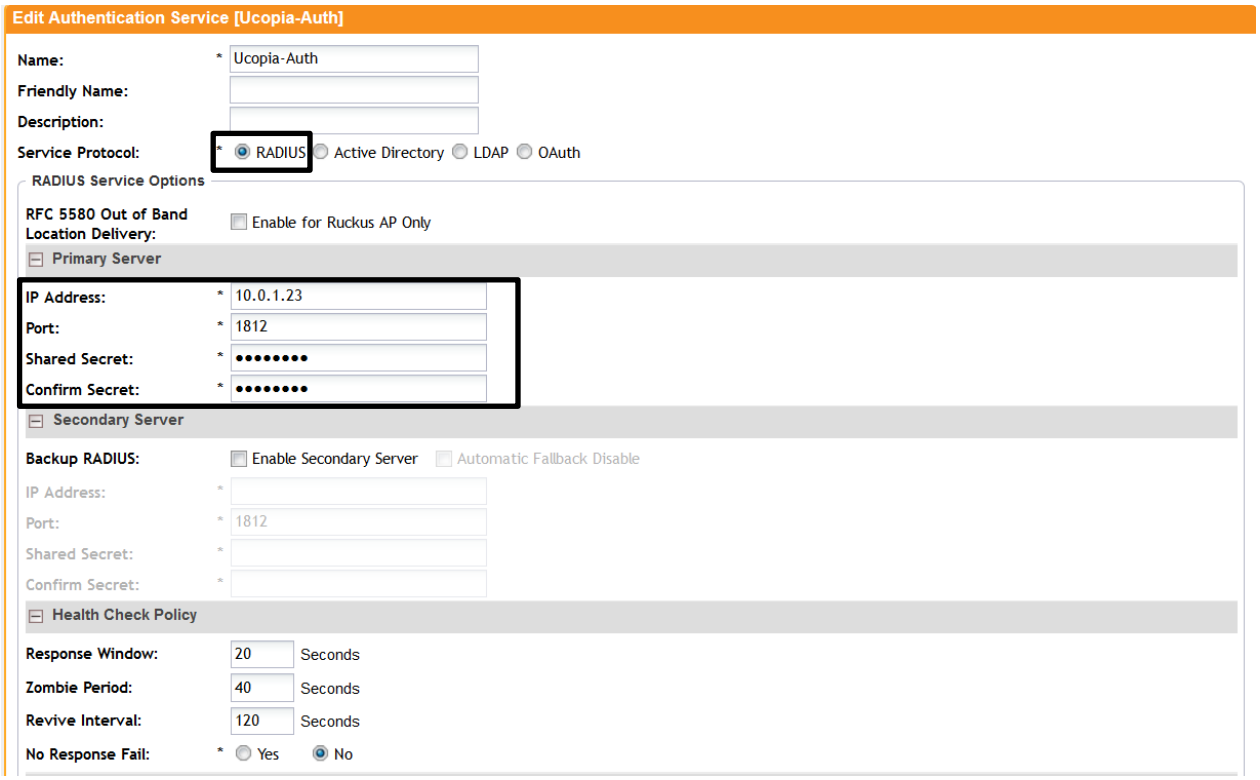
7. Configurations du contrôleur vSZ

Voici les configurations à entrer, sur le dashboard de Ruckus, pour assurer la compatibilité avec UCOPIA en environnement Out-Of-Band :

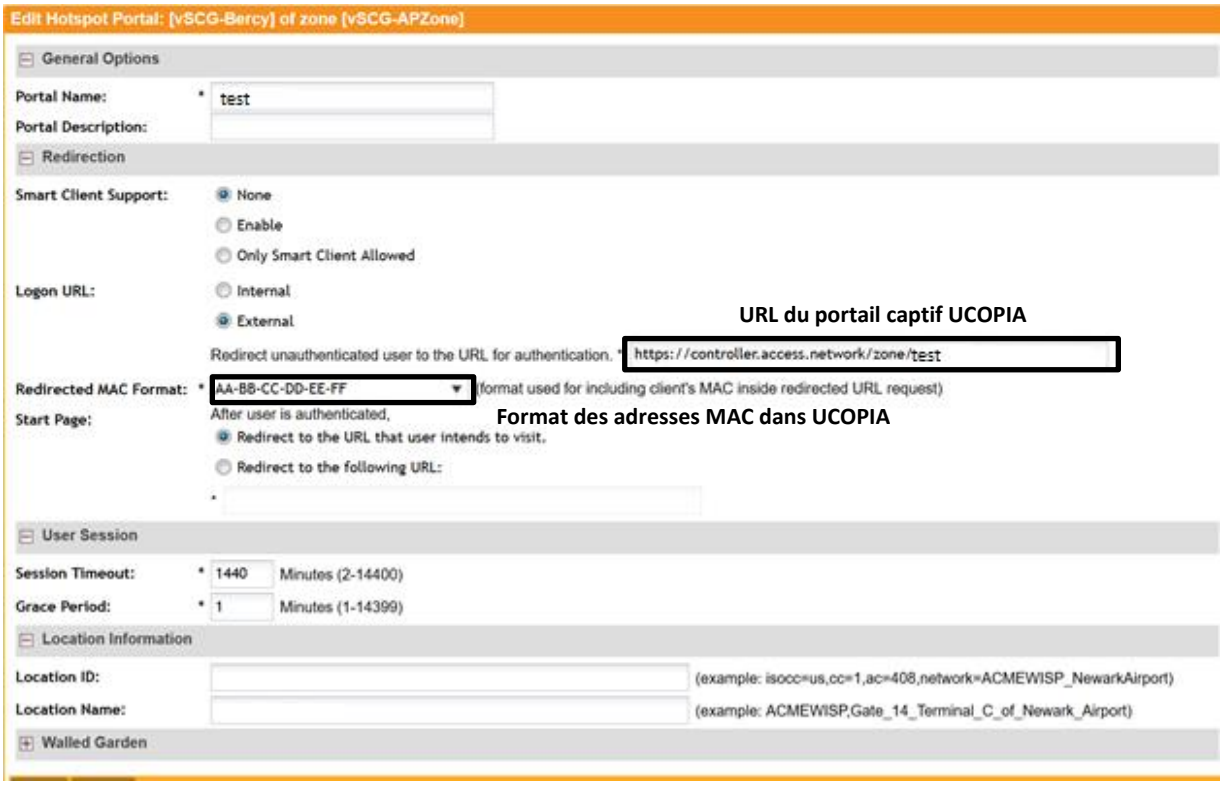
- **Configuration > System > Northbound Portal :** Configuration d'une NorthBound Portal Interface avec un secret de redirection (utilisé par l'API). Ceci permet à l'Ucopia de communiquer avec vSZ via l'API (envoi du {login ; mot de passe} au vSZ, récupération du résultat de l'authentification…).



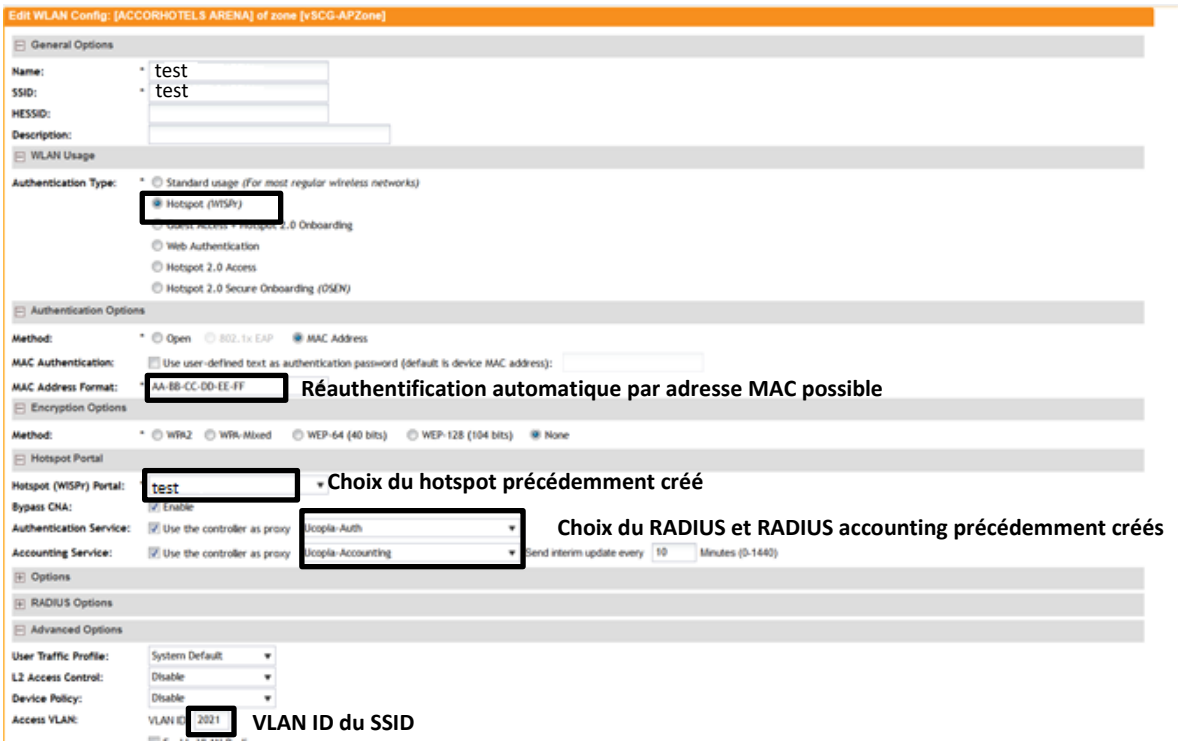
- **Configuration > Services & Profiles > RADIUS et RADIUS accounting, avec leur <u>secret partagé</u>**



- **Configuration > AP Zones > Sélection d'une borne > Hotspot (WISPr)** :
  Dans cette partie, vous déterminez le comportement de votre borne quand une personne non authentifiée ouvre son navigateur et tente d'accéder à Internet.



- **Configuration > AP Zones > WLAN** :



- **Désactiver le cryptage de l'adresse MAC**

Par défaut, vSZ enverra à Ucopia l'adresse MAC du client de façon cryptée (notamment nécessaire pour la réauthentification automatique par adresse MAC). Pour ce faire, il faut taper une commande dans le CLI du vSZ ou bien en mode ssh (mêmes identifiants qu'en CLI) :

```
ruckus> enable
Password :
ruckus# config
ruckus(config)# no encrypt-mac-ip
```

8. Configurations sur le contrôleur UCOPIA

- **Configuration > Authentification > Radius** : Création du NAS vSZ

- **Configuration > Authentification > Radius > Options avancées pour l'authentification RADIUS** : Décocher "Activer le délai de rejet pour renforcer la sécurité".

- **Configuration > Réseaux > Routes statiques** : Si vous êtes dans une architecture niveau 3 (i.e. un routeur devant le port OUT d'UCOPIA), alors il vous faut déclarer les routes statiques vers les réseaux de vos utilisateurs dans l'Ucopia.

9. Troubleshooting

En cas d'erreur lors d'une telle architecture, veuillez à vérifier les points ci-dessous :

- L'interface de contrôle du vSZ est accessible depuis les bornes
- L'interface de management du vSZ est accessible depuis le contrôleur UCOPIA (sauf si vous avez choisi d'utiliser une autre interface, auquel cas cf. Annexe)
- Les prérequis sont respectés (SSID = zone, routage)
- Le secret de redirection côté vSZ (Northbound Interface) est identique au secret de redirection côté Ucopia
- Le secret partagé entre le serveur RADIUS (en l'occurrence, Ucopia) et le NAS sont identiques

Si votre erreur demeure après avoir vérifié les points ci-dessus, veuillez regarder les paquets échangés entre le vSZ et Ucopia, avec un *tcpdump* et déterminer à quel moment de l'échange un problème apparaît (impossibilité de rediriger vers le portail captif d'UCOPIA, problème dans les échanges API ou dans les échanges via API…).

10. Annexe

Annexe 1 : Analyse de la requête http envoyée par l'utilisateur pour obtenir le portail captif

Vous pouvez vérifier le contenu des informations transmises par l'utilisateur au contrôleur Ucopia lors de sa requête web vers le portail captif. L'URL contient les éléments suivants :
https://controller.access.network/zone/**UCOPIA%20TEST**?nbiIP=**10.0.1.209**&wlan=**1**&reason=Un-Auth-SSL-Captive&mac=**d4:68:4d:2c:94:b0**&uip=**192.168.21.100**&url=http%3A%2F%2Ffree.fr%2F&zoneName=vSCG-APZone&client_mac=**30-52-CB-E9-03-61**&sip=**scg.ruckuswireless.com**&proxy=0&ssid=**MY+WIFI**&wlanName=**MY+WIFI**&dn=**scg.ruckuswireless.com**

L'URL contient les informations sur :

- La zone d'entrée (**UCOPIA TEST**)
- L'adresse IP de vSZ (**10.0.1.209**, en l'occurrence, interface de management) et de l'utilisateur (**192.168.21.100**)
- L'adresse MAC de l'AP et de l'utilisateur (respectivement, **30-52-CB-E9-03-61** et **d4:68:4d:2c:94:b0**)
- Le n° et le nom du réseau WiFi (ici, WLAN n° **1** et nom : **MY WIFI**)
- Le nom de domaine local (ici, **scg.ruckuswireless.com**)