



## Livre Blanc UCOPIA

---

Avril 2015



## Table des matières

<b>INTRODUCTION.....</b>	<b>7</b>
<b>2 PRESENTATION GENERALE DE LA SOLUTION UCOPIA .....</b>	<b>9</b>
2.1 ARCHITECTURE GLOBALE DE LA SOLUTION UCOPIA .....	10
<b>3 FONCTIONNALITES UCOPIA .....</b>	<b>12</b>
3.1 SECURITE .....	12
3.1.1 Certification de sécurité CSPN .....	12
3.1.2 Authentification .....	12
3.1.2.1 Authentification depuis le portail Web captif .....	12
3.1.2.2 Authentification par réseaux sociaux .....	14
3.1.2.3 Authentification RADIUS/802.1x .....	15
3.1.2.4 Authentification automatique par adresse MAC .....	16
3.1.2.5 Authentification par adresse MAC ou adresse IP fixe .....	16
3.1.2.6 Authentification en environnement Windows .....	16
3.1.2.7 Authentification Shibboleth .....	16
3.1.3 Contrôle d'accès par profil utilisateur .....	17
3.1.4 Traçabilité .....	17
3.1.5 Organisation en réseaux virtuels (VLAN) .....	17
3.1.6 Filtrage d'URLs .....	18
3.1.7 DPSK (Dynamic Pre Share Key) Ruckus .....	19
3.1.8 Détection d'intrusion .....	20
3.1.9 Politiques de mot de passe .....	20
3.1.10 Contrôle du mot de passe et quarantaine .....	20
3.1.11 Sécurité Radio .....	20
3.1.12 Journal d'audit .....	21
3.2 MOBILITE .....	21
3.2.1 Modèle de mobilité .....	21
3.2.2 Profils adaptables .....	22
3.2.3 BYOD (Bring Your Own Device) .....	22
3.2.4 Transparence d'accès ou « Zéro configuration » .....	22
3.2.5 Qualité de Service .....	23
3.2.5.1 QoS par service .....	23
3.2.5.2 QoS par utilisateur .....	24
3.2.6 Quota de volume de données .....	24
3.2.7 Multi portails .....	24
3.2.8 Personnalisation du portail .....	24
3.2.9 Portail captif et contenu dynamique .....	25
3.2.10 Application mobile pour smartphones et tablettes .....	26
3.2.11 Compatibilité iPass .....	26
3.3 PROVISIONNEMENT DE COMPTES UTILISATEUR .....	27
3.3.1 Auto-enregistrement depuis le portail captif .....	27
3.3.1.1 Auto-enregistrement « One Click Button » .....	27
3.3.1.2 Auto-enregistrement libre (formulaire) .....	27
3.3.1.3 Auto-enregistrement par SMS .....	28
3.3.1.4 Auto-enregistrement par email .....	28
3.3.1.5 Auto-enregistrement par impression de ticket .....	29
3.3.2 Parrainage .....	30
3.3.3 Portail de délégation .....	30
3.3.3.1 Prérogatives des administrateurs délégués .....	30
3.3.3.2 Personnalisation du portail de délégation .....	32
3.3.3.3 Multi zones .....	32
3.3.3.4 Génération de comptes en masse .....	32
3.4 PAIEMENT ET FACTURATION .....	32
3.4.1 Paiement en ligne .....	32
3.4.2 Connexion avec outil de facturation (PMS) .....	33
3.4.3 Connexion avec serveur de cartes prépayées (PPS) .....	33
3.4.4 Gestion d'événements .....	33
3.5 ADMINISTRATION .....	34
3.5.1 Profils d'administration .....	34

3.5.2	Administration des politiques de sécurité et de mobilité .....	34
3.5.3	Supervision, traçabilité .....	35
3.5.4	Reporting .....	40
3.5.5	Configuration du contrôleur UCOPIA .....	41
3.5.6	Exploitation du contrôleur UCOPIA .....	41
3.5.7	Administration centralisée .....	41
3.5.8	Administration SNMP .....	41
3.5.9	Administration via CLI .....	41
3.5.10	Exportation Syslog .....	41
3.5.11	Administration multi sites .....	41
3.5.12	Gestion de compte par l'utilisateur .....	42
<b>4</b>	<b>ARCHITECTURE UCOPIA .....</b>	<b>43</b>
4.1	CONTROLEUR UCOPIA .....	43
4.2	ADMINISTRATION UCOPIA .....	45
4.3	POINTS D'ACCES WI-FI .....	47
4.4	PREREQUIS DES POSTES UTILISATEURS .....	47
<b>5</b>	<b>INTEGRATION UCOPIA DANS UNE INFRASTRUCTURE RESEAU .....</b>	<b>48</b>
5.1	INTEGRATION AVEC UN OU PLUSIEURS ANNUAIRES D'ENTREPRISE .....	48
5.2	ADRESSAGE IP ET ARCHITECTURES VLAN .....	50
5.3	INTEGRATION AVEC UN PROXY WEB D'ENTREPRISE .....	52
5.4	INTEGRATION AVEC UN SERVEUR RADIUS EXTERNE .....	52
5.5	INTEGRATION AVEC UNE ARCHITECTURE PKI .....	52
5.6	INTEGRATION DANS LES ARCHITECTURES UNIVERSITAIRES .....	53
5.6.1	Architecture EDUROAM .....	53
5.6.2	Architecture Shibboleth .....	54
5.7	COUPLAGE AVEC UN PRODUIT TIERS .....	55
5.7.1	API .....	55
5.7.2	Couplage avec un PMS (Property Management System) .....	56
5.7.3	Couplage avec un PPS (Pre Paid System) .....	57
5.7.4	Couplage avec la solution iPass .....	57
<b>6</b>	<b>ARCHITECTURES RESEAU .....</b>	<b>59</b>
6.1	ARCHITECTURES MONO SITE .....	59
6.2	ARCHITECTURES MULTI SITES .....	61
6.2.1	Architecture centralisée .....	61
6.2.2	Architecture partiellement centralisée .....	62
6.2.3	Architecture distribuée .....	63
6.2.4	Architecture mixte .....	64
6.3	ARCHITECTURE MULTI ZONES .....	64
6.4	ARCHITECTURE CLOUD .....	65
<b>7</b>	<b>HAUTE DISPONIBILITE .....</b>	<b>68</b>
7.1	REDONDANCE .....	68
7.2	REPARTITION DE CHARGE .....	69
<b>8</b>	<b>PLATE-FORME UCOPIA WEB SERVICES .....</b>	<b>70</b>
8.1	EXPLOITATION .....	70
8.1.1	Installation automatique de la licence UCOPIA (ou mise à jour) .....	70
8.1.2	Mise à disposition automatique des mises à jour .....	70
8.1.3	Ouverture automatique d'un tunnel de maintenance .....	70
8.1.4	Contrôle de la validité de la maintenance .....	71
8.2	SUPERVISION ET ADMINISTRATION .....	71
8.3	BUSINESS INTELLIGENCE ET ANALYTIQUE .....	72
8.4	CAMPAGNES MARKETING .....	73
8.5	ARCHITECTURE .....	75
<b>9</b>	<b>GAMMES UCOPIA .....</b>	<b>77</b>
<b>10</b>	<b>PERFORMANCES .....</b>	<b>82</b>

<b>11</b>	<b>APPLIANCES MATERIELLES .....</b>	<b>83</b>
<b>12</b>	<b>APPLIANCES VIRTUELLES.....</b>	<b>88</b>
<b>13</b>	<b>MAINTENANCE .....</b>	<b>89</b>
<b>14</b>	<b>CONCLUSION.....</b>	<b>90</b>
<b>15</b>	<b>ANNEXE 1 : DOCUMENTATION .....</b>	<b>92</b>
15.1	MANUELS .....	92
15.2	APIS.....	92
15.3	COUPLAGE AVEC PRODUITS TIERS .....	93
15.4	CERTIFICATION DE SECURITE .....	93
<b>16</b>	<b>ANNEXE 2 : GLOSSAIRE .....</b>	<b>94</b>
16.1	RESEAU .....	94
16.2	WI-FI.....	94
16.3	AUTHENTIFICATION .....	95
16.4	CHIFFREMENT .....	96
16.5	ANNUAIRE.....	96

## Table des figures

Figure 1: La solution UCOPIA .....	10
Figure 2: Architecture globale de la solution UCOPIA .....	10
Figure 3: Page d'accueil du portail UCOPIA .....	13
Figure 4: Affichage des services autorisés depuis le portail UCOPIA.....	14
Figure 5: Authentification par réseaux sociaux.....	15
Figure 6: Authentification Shibboleth.....	16
Figure 7: Architecture VLAN UCOPIA .....	18
Figure 8: Portail UCOPIA avec Ruckus DPSK .....	20
Figure 9: Le modèle de mobilité UCOPIA.....	21
Figure 10 : Conditions BYOD.....	22
Figure 11: Edition du portail UCOPIA .....	25
Figure 12: Portail UCOPIA avec encarts publicitaires.....	25
Figure 13: Application UCOPIA pour Smartphones.....	26
Figure 14: Portail "One Click Button" .....	27
Figure 15: Portail avec auto-enregistrement par formulaire (libre).....	28
Figure 16: Portail avec auto-enregistrement par SMS .....	28
Figure 17: Portail avec auto-enregistrement par mail .....	29
Figure 18 : Portail avec auto-enregistrement par impression de ticket .....	29
Figure 19: Auto-enregistrement avec parrainage .....	30
Figure 20: Portail de délégation – Gestion de la validité .....	31
Figure 21: Portail de délégation – Gestion des utilisateurs .....	32
Figure 22: Portail avec paiement en ligne et choix de forfaits .....	33
Figure 23: Définition d'un profil utilisateur.....	35
Figure 24: Journal des sessions utilisateurs.....	36
Figure 25: Journal d'activité pour un utilisateur .....	37
Figure 26: Journal d'activité (URLs visitées par un utilisateur) .....	38
Figure 27: Visualisation de statistiques .....	39
Figure 28: Exemple de rapport au format PDF .....	40
Figure 29: Architecture UCOPIA.....	43
Figure 30: Architecture du contrôleur UCOPIA .....	44
Figure 31: Architecture des outils d'administration UCOPIA.....	46
Figure 32: Processus de connexion d'un utilisateur.....	48
Figure 33: Configuration d'un annuaire externe d'authentification .....	49
Figure 34: Authentification avec cascade d'annuaires .....	49
Figure 35: Configuration du contrôleur (annuaires d'authentification) .....	50
Figure 36: Configuration IP/VLAN par défaut du contrôleur UCOPIA .....	50
Figure 37: Politiques d'adressage en fonction du profil utilisateur.....	51
Figure 38: Politiques d'adressage et VLANs de sortie .....	51
Figure 39: Configuration RADIUS .....	52
Figure 40: Architecture EDUROAM avec UCOPIA .....	53
Figure 41 : Architecture Shibboleth avec UCOPIA .....	55
Figure 42: Couplage avec un produit tiers .....	56
Figure 43: Couplage avec un PMS.....	57
Figure 44: Architecture globale iPass/UCOPIA.....	58
Figure 45: Architecture iPass .....	58
Figure 46: Architecture UCOPIA mono site (cas 1) .....	59
Figure 47: Architecture UCOPIA mono site (cas 2) .....	60
Figure 48: Architecture multi sites centralisée .....	62
Figure 49: Architecture multi sites partiellement centralisée .....	63
Figure 50: Réplication d'annuaire UCOPIA en architecture distribuée .....	64

Figure 51: Architecture multi zones .....	65
Figure 52: Architecture Cloud.....	66
Figure 53: Architecture de redondance UCOPIA .....	69
Figure 54: Architecture de répartition de charge UCOPIA.....	69
Figure 55: Statistiques globales en fonction des numéros de version .....	71
Figure 56: Nombre de connexions simultanées sur un contrôleur .....	72
Figure 57: Exemple de tableau de bord analytique .....	73
Figure 58: Exemple de campagne marketing .....	74
Figure 59: Exemple de campagne marketing (suite).....	75
Figure 60: Architecture de la plate-forme UCOPIA Web Services .....	76
Figure 61: Contrôleur format "US250" .....	83
Figure 62: Contrôleur format "US2000" .....	83
Figure 63: Contrôleur format « US5000RDP ».....	83
Figure 64 : Contrôleur format « US10000RDP ».....	84

# 1 Introduction

---

Selon IDC, il y a 75 Millions de professionnels nomades en Europe, qui passent 70% de leur temps de travail hors de leur bureau. Par ailleurs, le nombre d'employés ne disposant pas d'un bureau atteint 46 Millions et augmente de 4,4% par an (Gartner). Tous ces nomades ont besoin d'accéder à Internet et au Système d'information de l'entreprise, dans leur bureau, en salle de réunion, à l'hôtel, chez leurs clients et leurs fournisseurs. Dès lors qu'un accès nomade est proposé, les employés se connectent 1h45 de plus chaque jour, ce qui contribue à une amélioration de la productivité de 22% (Source NOP World). Autrement dit, la mobilité donne plus de souplesse et plus d'utilisation donc plus d'efficacité. Selon Forrester, 38% des entreprises fournissent chaque mois à 20 visiteurs au moins un accès réseau et 11% de ces entreprises dépassent les 200 visiteurs connectés.

Les entreprises disposent déjà d'infrastructures IP sur lesquelles circulent les flux générés par les applications données et voix et continuent à les étendre avec notamment la technologie sans fil Wi-Fi. Le déploiement d'un accès nomade consiste donc à mutualiser cette infrastructure pour répondre à tous les utilisateurs (visiteurs, clients, fournisseurs, employés,) et tous les usages (du simple accès Internet jusqu'à un accès aux applications de l'entreprise).

Par ailleurs, l'essor des terminaux mobiles bouleverse les usages. D'ici 2016, le nombre de Smartphones devrait atteindre 480 millions, et 65% d'entre eux seront utilisés dans le cadre du BYOD (*Bring Your Own Device*) (Source Analyse firm IDC).

Dans ce contexte, la sécurité est un enjeu essentiel : authentification des utilisateurs et des terminaux, contrôle des accès en fonction de l'identité de l'utilisateur, de son rôle mais aussi de son terminal, du lieu et de l'heure de connexion, traçabilité des connexions et des usages pour répondre aux exigences légales en vigueur. La simplicité de l'usage et la gestion des utilisateurs (ouverture de compte, gestion des droits d'accès, assistance technique, etc.) conditionnent l'efficacité des accès nomades et le retour sur investissement.

Au-delà de la sécurité, les organisations veulent transformer leur investissement Wi-Fi en une opportunité de revenus (services à la carte, revenus publicitaires, etc.). Selon Gartner, le marché du Wi-Fi va croître de 3.7B\$ en 2011 à 9.7B\$ en 2017 soit une croissance annuelle de 57% pour les opérateurs et de 17% pour les entreprises.

La solution UCOPIA permet aux employés, clients, fournisseurs ou visiteurs de se connecter dans les environnements professionnels et d'accéder très simplement aux ressources de l'Intranet, de l'Internet ou de l'Extranet avec la double garantie de sécurité et de qualité de service. UCOPIA apporte également une réponse aux organisations qui souhaitent un retour sur investissement de leur infrastructure Wi-Fi grâce à ses services d'Analytique et de campagne marketing.

UCOPIA développe et commercialise deux gammes de produits : UCOPIA Advance et UCOPIA Express. UCOPIA Advance est destinée aux grands projets (nombreux utilisateurs, plusieurs sites, intégration fine avec le LAN) des entreprises, des campus, des administrations, des centres de congrès ou des stades. UCOPIA Express vise les projets plus petits (mono site, quelques dizaines ou centaines de connexions simultanées) mais privilégie la simplicité de la mise en œuvre et de l'exploitation. UCOPIA Express est parfaitement adaptée aux besoins des collèges, des hôtels, des cliniques et des PME en général.

Ce livre blanc décrit la solution UCOPIA dans son ensemble, toutes gammes de produits confondues. Il présente dans un premiers temps les composants de l'offre et ses principales fonctionnalités. Une deuxième partie est consacrée à l'architecture de la solution, le rôle et le fonctionnement de chaque composant et module sont présentés de façon détaillée. Une troisième partie est consacrée à la façon dont la solution UCOPIA s'intègre dans les architectures réseau existantes. Une quatrième partie décrit les différentes architectures UCOPIA (mono site, multi sites, etc.). La cinquième partie aborde les architectures de haute disponibilité (redondance et répartition de charge). La suite du document présente la plate-forme UCOPIA Web Services et ses nombreuses fonctions, puis finalement, les différentes

gammes de l'offre UCOPIA sont présentées avec pour chacune d'elle leurs objectifs et leurs fonctionnalités.



## 2 Présentation générale de la solution UCOPIA

---

La solution UCOPIA est une solution sécurisée dédiée à la gestion de la mobilité dans les réseaux sans fil Wi-Fi et filaires. Les principaux avantages d'UCOPIA sont les suivants.

- **La Sécurité de l'entreprise et des utilisateurs:** UCOPIA propose une authentification forte construite sur une architecture 802.1x et un serveur RADIUS. Une fois authentifié, l'utilisateur bénéficie d'un chiffrement WPA ou WPA2 afin de garantir la confidentialité de ses communications. Un mode d'authentification basé sur HTTPS et un portail Web (*login* et mot de passe) est également proposé afin d'accueillir sans contraintes les visiteurs. UCOPIA permet de définir puis de contrôler finement les droits d'accès en prenant en compte l'identité de l'utilisateur, la nature du service demandé, le type d'équipement, le lieu et l'heure de la demande. De plus, UCOPIA assure une parfaite traçabilité du trafic des utilisateurs afin de garantir la conformité aux lois anti-terroristes.
- **Le confort et la productivité des utilisateurs :** quiconque a utilisé son PC hors de son bureau ou de son entreprise a pu constater la difficulté à y retrouver ses applications même les plus courantes : accès Internet nécessitant la reconfiguration du navigateur pour prendre en compte un éventuel Proxy, impossibilité d'envoyer des messages sous son compte professionnel et difficulté à utiliser une imprimante. UCOPIA résout tous ces problèmes automatiquement : accès zéro configuration, sans assistance technique, avec une qualité de service contrôlée et prévisible.
- **L'intégration dans les infrastructures de communication et de sécurité :** les entreprises disposent d'une infrastructure réseau (DHCP, VLAN, VPN, annuaire, etc.). Le Wi-Fi doit s'intégrer dans cet existant en souplesse. UCOPIA grâce à son approche modulaire et ouverte apporte des réponses à toutes ses questions et permet aux entreprises de déployer du Wi-Fi sans remettre en cause son existant.
- **La simplicité de la mise en œuvre et de l'administration:** le contrôleur UCOPIA s'installe et se configure très simplement grâce à ses outils d'administration conviviaux. La création des profils et des comptes utilisateurs est à la portée d'un non spécialiste. UCOPIA combine ainsi une sécurité professionnelle à une simplicité de mise en œuvre exceptionnelle.
- **Le retour sur investissement des infrastructures mises en place :** les organismes déployant des réseaux Wi-Fi souhaitent un retour sur investissement de leur infrastructure. Le service d'Analytique UCOPIA va permettre aux organisations de mieux appréhender les usages et de mieux connaître leurs utilisateurs. Utilisé en conjonction avec le service de Campagnes Marketing Web, il est alors possible de proposer aux utilisateurs des services à valeur ajoutée générateur de revenu, et/ou de monétiser les accès par l'ajout de publicités ciblées.

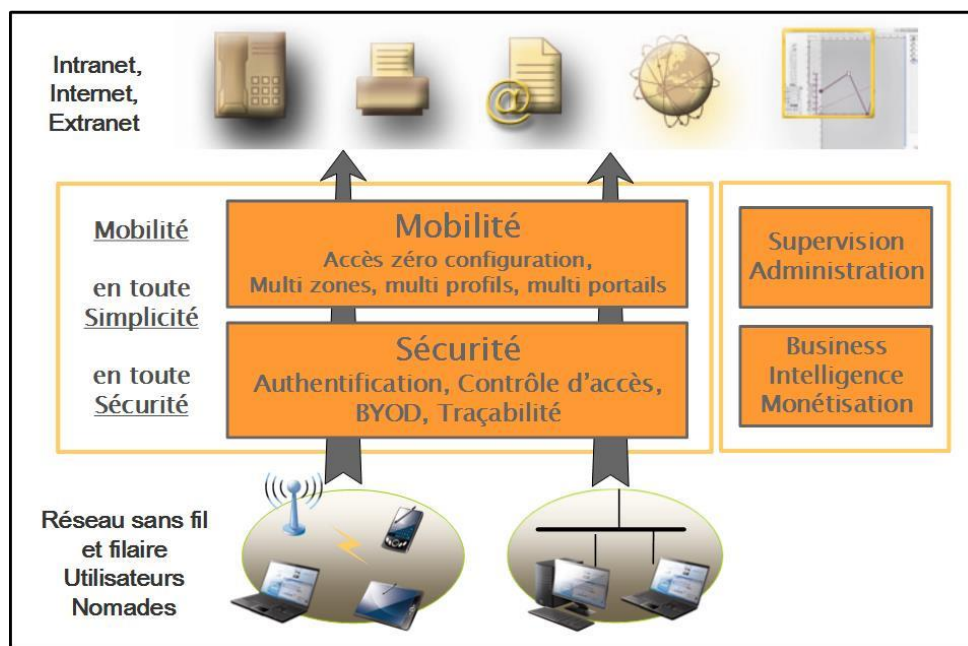


Figure 1: La solution UCOPIA

## 2.1 Architecture globale de la solution UCOPIA

La solution UCOPIA se présente sous la forme d'une Appliance matérielle (ou virtuelle), et vient se greffer sur une infrastructure Wi-Fi ou filaire. Cette infrastructure est connectée au réseau local d'entreprise à travers le contrôleur UCOPIA qui joue le rôle de passerelle et de contrôleur comme décrit dans le schéma ci-dessous.



Figure 2: Architecture globale de la solution UCOPIA

D'autres architectures sont possibles, notamment des architectures dans le Cloud, voir Section 6.4.

Deux composants principaux constituent le contrôleur UCOPIA :

- **Le contrôleur** implémente l'authentification basée soit sur un portail captif HTTPS, soit sur une architecture 802.1x et un serveur RADIUS, le contrôle d'accès par filtrage des flux utilisateurs, la détection et la correction automatique des flux mal configurés, la qualité de service et la traçabilité du trafic des utilisateurs.
- **L'outil d'administration** permet d'administrer l'ensemble de la solution UCOPIA, configuration du contrôleur, définition des politiques de sécurité et de mobilité de l'entreprise, supervision. De plus l'outil d'administration permet de déléguer à des utilisateurs habilités un droit d'administration limitée (par exemple provisionnement de comptes pour accueillir des visiteurs dans une entreprise ou les clients d'un hôtel).

## 3 Fonctionnalités UCOPIA

---

### 3.1 Sécurité

---

La sécurité est un élément essentiel pour un utilisateur nomade, UCOPIA offre les moyens de mettre en œuvre les mécanismes de sécurité indispensable dans un contexte de mobilité, il permet notamment d'installer un climat de confiance mutuelle entre le nomade et son environnement d'accueil.

La solution UCOPIA permet à un utilisateur de se connecter en toute sécurité grâce à ses mécanismes d'authentification. L'utilisateur, une fois authentifié, ne peut accéder qu'aux applications autorisées par son ou ses profils. Les profils peuvent dépendre du lieu ou de l'heure de connexion, voire de l'équipement de l'utilisateur. UCOPIA utilise les architectures VLAN pour renforcer le cloisonnement des différentes populations d'utilisateurs.

#### 3.1.1 Certification de sécurité CSPN

Le produit UCOPIA a obtenu une certification CSPN délivré par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Cela consiste à attester que le produit a subi avec succès une évaluation par un centre d'évaluation agréé par l'ANSSI dans un temps et une charge constraints conduisant à une certification.

Les travaux d'évaluation ont eu pour objectifs :

- de vérifier que le produit est conforme à ses spécifications de sécurité (authentification, contrôle d'accès par profil, traçabilité, etc.) ;
- de coter les mécanismes de façon théorique, de recenser les vulnérabilités connues de produits de sa catégorie ;
- de soumettre le produit à des tests de vulnérabilité visant à contourner ses fonctions de sécurité.

Voir le site de l'ANSSI pour consulter les éléments de certification.

[http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat\\_cspn\\_2010\\_01.html](http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat_cspn_2010_01.html)

#### 3.1.2 Authentification

UCOPIA propose plusieurs modes d'authentification, allant d'une authentification de type portail Web captif basée sur HTTPS jusqu'à une authentification forte basée sur le protocole 802.1x/EAP. Ces différents modes d'authentification cohabitent dans un même réseau, éventuellement sous différents réseaux logiques (VLAN), chacun correspondant à différentes catégories d'utilisateurs. Par exemple, une entreprise peut proposer à ses employés une authentification forte basée sur des certificats en EAP/TLS et peut réserver l'authentification par *login* et mot de passe depuis un portail Web à ses visiteurs. Dans chaque mode d'authentification, la clé d'authentification a une durée limitée dans le temps.

##### 3.1.2.1 Authentification depuis le portail Web captif

Ce mode d'authentification est comparable d'un point de vue ergonomique à celui utilisé par les hotspots. L'utilisateur, à l'ouverture de son navigateur Web, se voit automatiquement redirigé vers une page Web d'authentification hébergée par le contrôleur UCOPIA ou éventuellement externe à celui-ci. La page lui propose de s'authentifier en utilisant un couple *login*/mot de passe (mode standard), une fois l'authentification réussie, les services autorisés s'affichent dans la fenêtre et l'utilisateur peut en faire usage.

La copie d'écran suivante montre la page d'accueil du portail UCOPIA permettant une authentification par *login* et mot de passe (mode standard) ainsi que de l'auto-enregistrement par email et par formulaire libre.



**Figure 3: Page d'accueil du portail UCOPIA**

Une fois l'utilisateur authentifié, les services autorisés par son profil s'affichent dans la fenêtre.



**Figure 4: Affichage des services autorisés depuis le portail UCOPIA**

### ***Réauthentification automatique***

Par défaut, UCOPIA propose un mécanisme permettant de renforcer la sécurité pour le mode d'authentification par portail en mettant en oeuvre une authentification qui est rejouée périodiquement et de façon transparente pour l'utilisateur. Dans ce cas, il faudra que l'utilisateur conserve la fenêtre du portail ouverte pour que sa connexion reste active. Il est néanmoins possible de désactiver cette option par configuration, l'utilisateur sera alors déconnecté quand il éteindra son poste ou désactivera sa connexion réseau. L'activation ou la désactivation de ce mécanisme s'effectue au niveau du profil utilisateur. Le temps de déconnexion sur inactivité est configurable.

### ***Utilisation d'un même couple d'identifiants pour plusieurs connexions simultanées***

Par défaut, le même *login*/mot de passe ne peut être utilisé pour deux connexions simultanées, et ce pour des raisons de traçabilité et de sécurité. Cette option peut toutefois être désactivée pour autoriser plusieurs postes utilisateurs (PC, Smartphone) à se connecter avec le même couple d'identifiants. Il est possible de contrôler le nombre de connexions simultanées pour un profil utilisateur donné.

### ***Redirection vers un portail d'entreprise***

Il est possible de rediriger l'utilisateur vers un portail externe à UCOPIA. Ce fonctionnement peut être intéressant pour, par exemple, alimenter une base de données Marketing. Concernant l'authentification de l'utilisateur, deux modes sont proposés, (1) revenir sur le portail UCOPIA, (2) rester sur le portail d'entreprise qui devra alors être enrichi avec le dialogue d'authentification UCOPIA. Pour ce dernier cas, UCOPIA fournit une API permettant de réaliser le dialogue d'authentification.

#### **3.1.2.2 Authentification par réseaux sociaux**

Afin de ne pas multiplier le nombre d'identifiants pour un utilisateur et ainsi de simplifier l'usage, l'utilisateur peut utiliser les identifiants d'un de ses réseaux sociaux (Facebook, Twitter, Google ou LinkedIn) pour s'authentifier sur le portail captif.



**Figure 5: Authentification par réseaux sociaux**

Les informations propres à l'utilisateur seront enregistrées dans les journaux utilisateurs à des fins de traçabilité et/ou de marketing.

L'organisation déployant UCOPIA pourra développer sa propre application réseau social afin de faire apparaître une page à ses couleurs lors de la saisie par l'utilisateur de ses identifiants.

### **3.1.2.3 Authentification RADIUS/802.1x**

Un serveur RADIUS est embarqué dans le contrôleur UCOPIA permettant de jouer le rôle du serveur d'authentification de l'architecture 802.1x.

#### ***Authentification par login/mot de passe et protocole 802.1x***

Les protocoles tels que PEAP ou TTLS peuvent être utilisés pour l'authentification par *login*/mot de passe.

#### ***Authentification par certificats et protocole 802.1x***

L'authentification par certificat repose sur le protocole 802.1x/EAP-TLS qui s'appuie sur une infrastructure de type PKI. Le serveur RADIUS et le client du réseau sont munis de certificats délivrés par une autorité de certification commune. UCOPIA s'appuie sur des certificats émis par un tiers de confiance.



### 3.1.2.4 Authentification automatique par adresse MAC

Après une première authentification de type portail réussie, UCOPIA peut enregistrer l'adresse MAC de l'utilisateur. Il sera ainsi possible de connecter de façon transparente l'utilisateur lorsqu'il se représente et ce grâce à la reconnaissance automatique de son adresse MAC.

Ce mécanisme permet de rendre le parcours client plus fluide en ne présentant le portail d'authentification que pour la première connexion. L'activation de ce mécanisme s'effectue au niveau du profil de l'utilisateur et peut s'appliquer à tout type de portail.

De plus, il est possible de verrouiller l'accès pour un équipement donné (ou plusieurs) à partir de son adresse MAC. Ceci permet d'éviter le partage des identifiants entre plusieurs utilisateurs utilisant différents équipements.

### 3.1.2.5 Authentification par adresse MAC ou adresse IP fixe

UCOPIA propose une authentification basée sur des adresses MAC ou adresses IP fixes. Les adresses doivent être renseignées depuis l'outil d'administration. Ce mode peut s'avérer utile pour authentifier des équipements IP qui n'auraient pas la capacité à s'authentifier avec des protocoles plus élaborés tel que 802.1x.

### 3.1.2.6 Authentification en environnement Windows

UCOPIA permet de réaliser, en environnement Windows, une authentification machine avant l'authentification de l'utilisateur. L'objectif de l'authentification machine, au-delà de sa fonction première d'authentification, va permettre de déclencher sur le serveur Windows des scripts (type Netlogon), qui vont par exemple monter des lecteurs réseaux, exécuter des scripts de mise à jour antivirus, démarrer certains utilitaires spécifiques, etc.

### 3.1.2.7 Authentification Shibboleth

Shibboleth est un mécanisme de propagation d'identité déployé plus particulièrement en environnement universitaire. L'objectif est que l'utilisateur puisse s'authentifier avec ses identifiants Shibboleth à partir du portail captif UCOPIA. Pour cela, il est redirigé sur une page lui permettant tout d'abord de sélectionner son établissement d'appartenance puis d'entrer ses identifiants de connexion. Une fois authentifié l'utilisateur se voit attribuer un profil qui est déduit à partir de son affiliation et de son site d'appartenance (voir Section 5.6.2 pour l'architecture technique).



Figure 6: Authentification Shibboleth



### 3.1.3 Contrôle d'accès par profil utilisateur

Le contrôle d'accès des utilisateurs doit s'exercer de manière fine, en fonction de l'utilisateur et de ses droits. Pour ce faire le contrôleur UCOPIA utilise un mécanisme de filtre basé sur des règles et construit à partir du profil de l'utilisateur. Le filtre est installé sur le contrôleur dès qu'un utilisateur est authentifié. Il sera supprimé lors de sa déconnexion.

Le profil de l'utilisateur décrit les droits d'accès aux applications, la durée et le mode de connexion, les plages horaires et les zones autorisées de connexion, etc. Un même utilisateur peut avoir plusieurs profils dépendant de différents critères (lieu, temps, équipement).

Le filtre peut proposer de nombreuses autres fonctionnalités que l'on peut mettre en œuvre dans un réseau Wi-Fi. La sécurité en est un exemple, mais d'autres applications tout aussi importantes peuvent également être intégrées à cet environnement. Dans le cadre de la solution UCOPIA, le filtrage est utilisé notamment pour gérer la qualité de service.

### 3.1.4 Traçabilité

UCOPIA enregistre et sauvegarde deux types d'information : les informations de sessions des utilisateurs (qui s'est connecté quand) et les informations de trafic (qui a fait quoi). **En effet, dès lors qu'une organisation accueille des visiteurs, elle a l'obligation légale de conserver le trafic Internet des visiteurs qui se connectent au réseau (loi du 23 janvier 2006 sur le terrorisme et la traçabilité) (voir Section 3.5.3).**

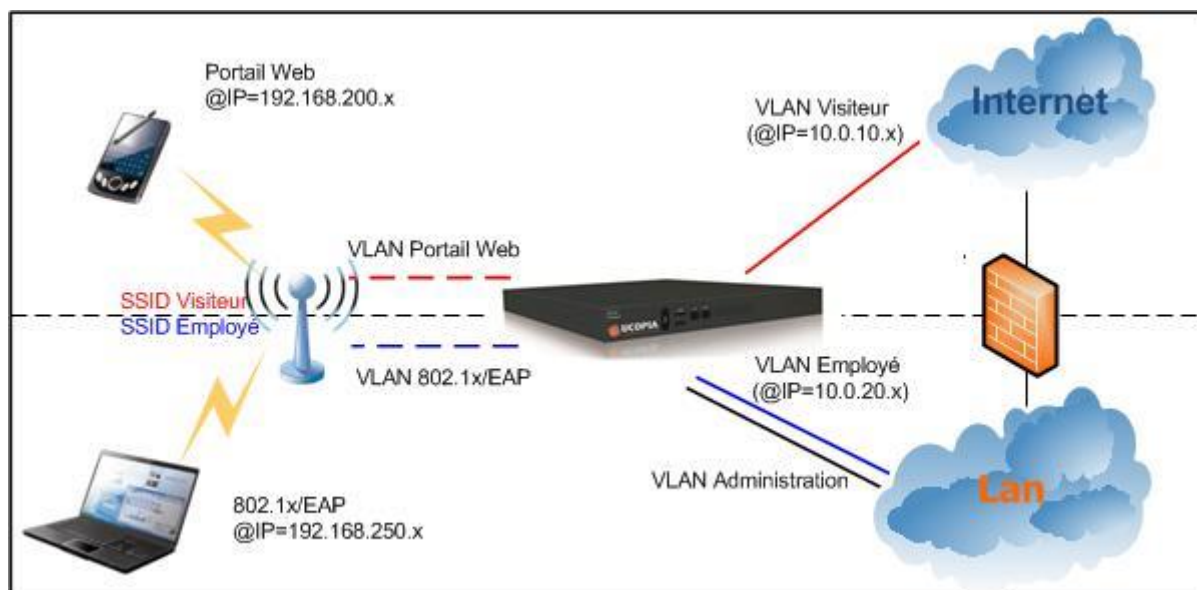
### 3.1.5 Organisation en réseaux virtuels (VLAN)

UCOPIA offre la possibilité d'utiliser des VLAN en entrée et en sortie du contrôleur UCOPIA. En effet, très souvent les entreprises architecturent leur réseau en VLAN et il est important en installant UCOPIA de pouvoir continuer à bénéficier des mécanismes d'isolation réseau mis en place sur le réseau existant.

Considérons le cas d'un déploiement Wi-Fi, à chaque SSID configuré sur les points d'accès Wi-Fi est associé un VLAN, ces VLANs se retrouvent en entrée du contrôleur UCOPIA. Le contrôleur UCOPIA alloue des plages d'adresses IP distinctes pour chacun des VLANs. Par défaut UCOPIA fonctionne en mode NAT mais peut être configuré en mode routage au niveau de chaque VLAN de sortie en fonction du profil de l'utilisateur (voir Section Adressage IP et architectures VLAN).

Par ailleurs, en fonction de son profil, le flux d'un utilisateur pourra être réinjecté en sortie du contrôleur UCOPIA dans un VLAN particulier.

Le schéma ci-dessous illustre une architecture VLAN pour deux types de populations, des visiteurs et des employés d'une entreprise. Les visiteurs s'authentifient en mode portail Web et les employés en 802.1x. Chacune des populations est redirigée dans son VLAN d'appartenance côté réseau d'entreprise.



**Figure 7: Architecture VLAN UCOPIA**

### 3.1.6 Filtrage d'URLs

UCOPIA propose nativement une fonction de filtrage d'URLs qui peut s'activer par profil utilisateur. Différentes catégories d'URLs (Adulte, Agressif, etc.) peuvent être filtrées permettant par exemple de différencier un profil « Enfant » d'un profil « Adulte ».

Les catégories disponibles sont les suivantes.

Achat en ligne	Sites d'achat en ligne.
Adulte	Sites adultes allant de l'érotique à la pornographie.
Agressif	Sites faisant la promotion de la violence et de la haine.
Banque	Sites de banque en ligne.
Blog	Sites d'hébergement de blogs.
Chat	Sites de dialogue et conversation en ligne.
Drogue	Sites faisant la promotion de la drogue.
Hameçonnage	Faux sites de banque ou incitant à donner des informations personnelles frauduleusement.
Hébergement	Sites d'hébergement de fichiers.
Jeux d'argent	Sites de jeux d'argent.
Jeux en ligne	Sites de jeux en ligne ou de distribution de jeux.
Messagerie	Sites de messagerie en ligne.

Piratage	Sites de piratage.
Presse	Sites de presse en ligne.
Publicité	Sites proposant de la publicité.
Redirecteur	Sites permettant de contourner le filtrage des URLs.
Rencontre	Sites de rencontre en ligne.
Réseaux sociaux	Réseaux sociaux.
Vidéo	Sites d'hébergement de contenu audio et/ou vidéo.
Virus	Tout site qui injecte des programmes malveillants.
Warez	Annuaire de liens pour téléchargement de fichiers.

Il est également possible d'utiliser un produit de filtrage tiers grâce à une redirection des flux HTTP ou à travers le protocole ICAP.

La solution basée sur la redirection de flux HTTP est réalisée grâce au proxy Web embarqué dans le contrôleur UCOPIA. Il permet de rediriger les flux vers le produit en charge du filtrage d'URLs. Les identifiants de l'utilisateur peuvent être passés au produit tiers afin qu'il puisse appliquer différentes politiques en fonction de l'utilisateur.

### 3.1.7 DPSK (*Dynamic Pre Share Key*) Ruckus

La solution Wi-Fi Ruckus<sup>1</sup> propose un mécanisme innovant de distribution dynamique de clé de chiffrement, la clé étant unique par utilisateur. DPSK est un compromis idéal entre 802.1x et une simple *passphrase*.

Le portail captif UCOPIA peut être associé à ce mécanisme DPSK afin de renforcer la sécurité du portail tout en conservant la simplicité d'usage.

L'utilisateur va tout d'abord s'associer à un SSID « ouvert » et s'enregistrer sur le portail UCOPIA avec l'une des méthodes d'auto-enregistrement à sa disposition. La clé va lui être octroyée et communiquée en même temps que ses identifiants. Un utilitaire peut être téléchargé depuis le portail pour automatiser la configuration de la clé sur son équipement. L'utilisateur peut ensuite se connecter sur le portail avec ses identifiants, il sera associé à un SSID sécurisé et son trafic sera chiffré.

---

<sup>1</sup> [www.ruckuswireless.com](http://www.ruckuswireless.com)



**Figure 8: Portail UCOPIA avec Ruckus DPSK**

### 3.1.8 Détection d'intrusion

UCOPIA permet de détecter et de contrer des attaques consistant à usurper l'identité d'un utilisateur. L'usurpation s'effectue sur le même réseau Ethernet en falsifiant des adresses ARP (MAC) pour des adresses IP données. Ce type d'attaque est plus sensible en cas d'utilisation d'un mode d'authentification par portail moins sécurisé qu'un mode 802.1x qui ne délivre pas d'adresse IP avant authentification de l'utilisateur. Dans ce type d'attaque, le poste ciblé par l'attaque mettra à jour sa table ARP avec une fausse adresse MAC et ne pourra plus communiquer avec le contrôleur UCOPIA.

UCOPIA, une fois l'attaque détectée, se charge en temps réel de remettre dans un état cohérent les tables ARP des postes attaqués.

### 3.1.9 Politiques de mot de passe

Des politiques de mot de passe peuvent être définies pour chaque profil utilisateur. Il est ainsi possible de définir la longueur du mot de passe ainsi que les caractères qui entrent dans sa composition. L'association d'une politique de mot de passe au profil permet de répondre à différents usages, par exemple l'application d'une politique fortement sécurisée pour des employés d'entreprise accédant à des ressources du réseau, et une politique simplifiée pour des visiteurs s'auto-enregistrant par SMS.

### 3.1.10 Contrôle du mot de passe et quarantaine

Un utilisateur entrant plusieurs fois consécutives un mot de passe erroné peut être mis en quarantaine.

Le nombre de tentatives ainsi que le temps de quarantaine sont configurables.

### 3.1.11 Sécurité Radio

La confidentialité des données transmises est assurée par les équipementiers qui commercialisent les cartes IEEE 802.11 et les points d'accès. Cette sécurité est de type WPA (Wireless Protected Access)

ou WPA2 qui offre les fonctions de chiffrement TKIP ou AES, utilisant des clefs dynamiques. UCOPIA est bien sûr compatible avec ces protocoles. UCOPIA est plus généralement compatible 802.11i.

### 3.1.12 Journal d'audit

A des fins de sécurité et de traçabilité, toutes les opérations d'administration sont notées au format Syslog. Cela concerne les opérations effectuées depuis l'outil d'administration, le portail de délégation et la CLI Web.

## 3.2 Mobilité

La gestion de la mobilité consiste à définir quelles sont les politiques de mobilité de l'entreprise d'une part et à les mettre en œuvre d'autre part. Par ailleurs, il faut que l'utilisateur nomade puisse accéder en tout lieu aux services autorisés de façon simple et transparente et lui garantir la Qualité de Service nécessaire à la bonne exécution de ses applications.

### 3.2.1 Modèle de mobilité

UCOPIA a défini un modèle de mobilité prenant en compte plusieurs dimensions, le « Qui », « Quoi », « Quand », « Où » et « Comment ». Le « Qui » identifie les utilisateurs du réseau et leurs matériels, le « Quoi » les applications accessibles depuis ce réseau. La plupart des systèmes traitant de sécurité sur les réseaux sans fil s'arrêtent à ces deux dimensions. UCOPIA prolonge ce modèle, le « Quand » introduit la notion de temps, par exemple, les employés d'une entreprise peuvent se connecter à toute heure alors que les visiteurs uniquement aux heures d'accueil de l'entreprise. Le « Où » va conditionner les droits d'accès de l'utilisateur, en effet, les droits peuvent être différents en fonction du lieu sur lequel il se connecte. Cette dimension de lieu va introduire une dernière dimension qui est le « Comment », en effet, le fait d'être sur des sites différents peut amener à utiliser un mode d'authentification particulier.

Exemple : un utilisateur se trouvant au siège de son entreprise utilisera une authentification forte de type 802.1x, accèdera sans restrictions au LAN d'entreprise, et ce à toute heure de la journée. Quand il se trouvera sur une filiale de l'entreprise, il utilisera un mode d'authentification de type portail Web et ses droits d'accès seront limités à la fois en terme de services (accès Internet ou VPN d'entreprise) et en termes de plages horaires (de 9h à 18h).

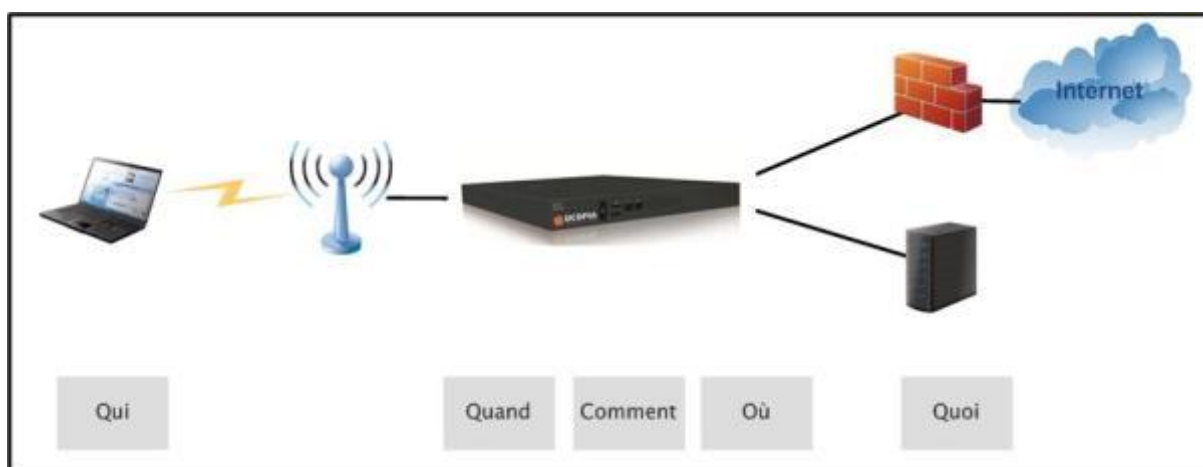


Figure 9: Le modèle de mobilité UCOPIA

### 3.2.2 Profils adaptables

La mise en œuvre du modèle de mobilité UCOPIA s'appuie sur la notion de profil utilisateur adaptable. En effet, UCOPIA, dans sa gamme Advance, permet d'adapter automatiquement le profil du nomade en fonction de différents critères : le lieu de connexion (site, zone), l'heure de connexion, voire l'équipement avec lequel le nomade se connecte.

Grâce aux profils adaptables, il est aisé de spécifier les configurations suivantes :

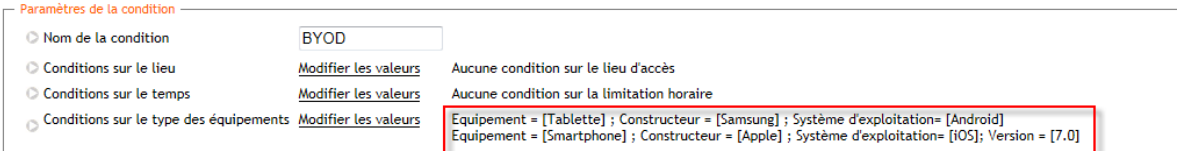
1. Les étudiants qui se connectent dans la zone « Amphithéâtre » pendant la période d'examens voient leurs droits d'accès modifiés (pas d'Internet, accès uniquement aux serveurs pédagogiques).
2. Les étudiants qui se connectent dans la zone « Bibliothèque » se connectent avec un crédit temps de 2 heures par jour, ils n'ont pas de limite de temps sur la zone « Résidence Universitaires ».
3. Les employés d'une entreprise se connectent en authentification forte (802.1x) sur le siège social et peuvent accéder au LAN sans restrictions, ils s'authentifient en mode portail sur une filiale et voient leurs droits d'accès restreints (Internet, VPN d'entreprise).
4. Les clients d'un hôtel qui se connectent dans les chambres ont une connexion illimitée, ils ont un crédit temps dans les zones restaurant et accueil.

### 3.2.3 BYOD (Bring Your Own Device)

Le profil adaptable peut s'appliquer au type de matériel de l'utilisateur et ainsi permettre de mettre en œuvre des politiques de sécurité et de mobilité propres à un type de matériel. Cette fonctionnalité peut être utilisée dans les entreprises pour gérer le BYOD et ainsi appliquer un traitement particulier aux équipements personnels des employés.

Par exemple, les téléphones mobiles et les tablettes ne pourront se connecter qu'aux jours et heures ouverts avec des droits d'accès restreints.

Lors de la définition du profil, la condition BYOD pourra s'exprimer de la façon suivante :



**Figure 10 : Conditions BYOD**

Si la condition est satisfaite, le profil s'adaptera pour mettre en œuvre les droits d'accès et les horaires de connexion appropriés.

Il est à noter que les conditions permettant de sélectionner les équipements peuvent faire intervenir le constructeur et le système d'exploitation (nom et version).

### 3.2.4 Transparence d'accès ou « Zéro configuration »

L'objectif de la transparence d'accès est de permettre à des utilisateurs ne connaissant pas l'infrastructure d'accueil de pouvoir utiliser leur terminal et leurs applications sans besoin de configuration ou d'installation particulière.

La transparence d'accès gérée par UCOPIA est basée sur la technologie de filtrage. Puisque le filtre est capable de reconnaître le type d'application et l'utilisateur émetteur et récepteur, il peut déterminer que l'application est inadaptée au contexte présent. Par exemple, un client visiteur d'une entreprise se connectant sur le réseau sans fil et qui souhaite émettre un message ou bien imprimer un document, ne peut effectuer ces travaux parce qu'il ne possède pas le droit ou plus simplement parce qu'il n'a pas les

drivers nécessaires. Le filtre est capable de détecter ces problèmes et de proposer des solutions. En voici quelques exemples.

- **Adressage IP** : la configuration réseau du terminal de l'utilisateur importe peu. En effet, qu'il soit configuré en adressage IP fixe ou en adressage DHCP, le contrôleur UCOPIA se charge d'établir la connexion de façon transparente pour l'utilisateur.
- **Accès Internet**: beaucoup d'entreprises mettent en place des proxy Internet pour des raisons de sécurité et les navigateurs des employés de ces entreprises sont configurés en conséquence afin d'utiliser le proxy. Si un tel utilisateur tente d'accéder à Internet dans un environnement sans proxy Web ou avec un autre proxy, cela ne fonctionne pas : il doit modifier la configuration de son navigateur. UCOPIA assure le bon fonctionnement du navigateur de l'utilisateur indépendamment de sa configuration et il redirige si besoin est vers le proxy d'entreprise.
- **Email**: envoyer un email depuis un environnement qui n'est pas son environnement habituel généralement échoue car les réseaux des entreprises sont construits pour se protéger de ce type de message qui pourrait par exemple servir de couverture à des mécanismes de « spam ». UCOPIA détecte les messages sortants de type SMTP et redirige automatiquement les paquets vers le serveur SMTP local de l'entreprise si bien sûr l'utilisateur est autorisé à envoyer un message. L'utilisateur ne modifie pas sa configuration de client de messagerie et le mail peut partir en toute transparence.
- **Impression** : imprimer un document dans un environnement qui n'est pas le sien relève très souvent du défi. Il faut connaître le type d'imprimante, savoir quel est son driver, où il se trouve, comment l'installer. UCOPIA apporte la réponse à ce type de problème, le contrôleur embarque un serveur d'impression dont le rôle est de mettre à disposition de façon transparente le driver de l'imprimante.

UCOPIA est également compatible avec la solution AirPrint<sup>2</sup> pour imprimer de façon transparente en environnement Wi-Fi et Apple.

L'ensemble de ces mécanismes de transparence d'accès mis en œuvre par UCOPIA garantit à l'utilisateur final productivité et confort d'utilisation. Il réduit de façon spectaculaire la charge de travail de l'assistance technique car il n'est plus nécessaire de la solliciter lors d'une connexion dans un environnement d'accueil.

### 3.2.5 Qualité de Service

UCOPIA peut différencier les flux traversant les contrôleurs UCOPIA et ainsi gérer des priorités de flux en fonction des choix de l'administrateur.

Deux niveaux de gestion de la Qualité de Service sont proposés :

- **Au niveau des services**
- **Au niveau des utilisateurs**

#### 3.2.5.1 QoS par service

Pour chaque service, il est possible de définir :

- **La priorité de traitement des services**

Les services définis dans le contrôleur UCOPIA peuvent avoir deux niveaux de priorité : temps réel ou normal. Les flux de type de temps réel sont traités en priorité.

---

<sup>2</sup> AirPrint est une technologie proposée par Apple qui permet d'imprimer des documents de haute qualité, et ce à l'aide de l'architecture d'impression sans pilotes d'Apple.



#### ■ Le débit garanti des services

Par défaut, les services se partagent la bande passante disponible. UCOPIA permet de configurer chaque service afin de garantir un débit pour chacun d'eux.

Le débit garanti est exprimé en kilo bit par secondes (Kbps).

#### ■ La limitation de bande passante

La limitation de bande passante s'applique à un service et est exprimée en Kbps. Les paquets d'un flux dépassant cette limite sont éliminés.

### 3.2.5.2 QoS par utilisateur

Une limitation du débit ascendant et descendant peut être définie par utilisateur au niveau du profil utilisateur. Chaque utilisateur ayant ce profil se verra attribuer ces limitations. Le débit descendant correspond au flux allant de la carte Ethernet IN vers OUT, le débit ascendant correspond à l'inverse.

### 3.2.6 Quota de volume de données

Afin de contrôler l'usage qui est fait du réseau, un quota de volume de données transférées peut être défini au niveau du profil de l'utilisateur. Ce quota peut être fixé pour le débit ascendant, descendant ou la somme des deux. En cas de dépassement du seuil, des règles peuvent s'appliquer pour soit bloquer l'utilisateur, soit limiter sa bande passante.

### 3.2.7 Multi portails

Les différents modes de portails peuvent cohabiter, en effet, à chaque zone (voir Section 6.3) en entrée du contrôleur UCOPIA, il est possible d'associer un portail fonctionnant dans un mode particulier. Par exemple, dans un hôtel, les clients du restaurant s'auto-enregistrent sur le portail (mode SMS) et ont une durée de connexion limitée à 30 minutes, les clients de l'hôtel disposent d'un compte utilisateur créé lors de leur inscription et peuvent se connecter sans limite de temps.

### 3.2.8 Personnalisation du portail

Le portail UCOPIA reconnaît le type de terminal utilisé (PC, smartphone ou tablette) et peut ainsi proposer un portail dont le format est approprié au terminal.

Le portail est personnalisable grâce à un mode « Edition » permettant de changer le fond d'écran, le logo, d'ajouter des images, du texte, des URLs accessibles sans authentification, etc. Chaque format de portail (PC, smartphone et tablette) peut ainsi être personnalisé.

La copie d'écran ci-dessous montre le portail en mode « Edition ».





**Figure 11: Edition du portail UCOPIA**

Pour une personnalisation plus avancée, le code HTML du portail peut être exporté, retravaillé et réimporté dans le contrôleur UCOPIA.

### 3.2.9 Portail captif et contenu dynamique

Le portail UCOPIA peut afficher du contenu dynamique à partir d'un serveur de contenu.

Il est ainsi possible de proposer un contenu publicitaire sur le portail en provenance d'une régie, le contenu pouvant changer à chaque rafraîchissement de portail.

La copie d'écran ci-dessous montre un exemple de portail personnalisé affichant un encart publicitaire.



**Figure 12: Portail UCOPIA avec encarts publicitaires**

### 3.2.10 Application mobile pour smartphones et tablettes

Une application mobile UCOPIA pour Smartphones est disponible. L'objectif de l'application est double, d'une part simplifier le parcours utilisateur et donc la connexion à un réseau UCOPIA, d'autre part permettre à un administrateur délégué de créer très simplement un compte utilisateur.

L'application propose un mode d'auto-enregistrement. Ce mode évite d'avoir à créer son compte depuis le portail captif. Son fonctionnement consiste à proposer à la première connexion le renseignement d'un formulaire d'identification, les autres connexions seront alors transparentes. Le formulaire peut éventuellement être supprimé pour une complète transparence d'utilisation.

L'application mémorise les identifiants de l'utilisateur, ils sont rejoués automatiquement en présence d'une demande d'authentification et en fonction du contrôleur UCOPIA sur lequel l'application se connecte

Les comptes utilisateur peuvent être créés directement à partir des contacts du répertoire du Smartphone, les tickets de connexion peuvent être envoyés à l'utilisateur depuis le Smartphone par SMS ou par email.

L'application pourra être personnalisée aux couleurs du client (hôtel, entreprises, ...). Changement du logo, texte, etc.).

L'application UCOPIA est gratuite et disponible en français et en anglais.



Figure 13: Application UCOPIA pour Smartphones

### 3.2.11 Compatibilité iPass

iPass<sup>3</sup> est une solution permettant à des utilisateurs nomades de se connecter à leur environnement professionnel de façon sécurisée depuis une infrastructure Wi-Fi. iPass s'utilise depuis un PC, un smartphone ou une tablette.

UCOPIA est compatible iPass, il permet ainsi de prendre en charge tout utilisateur iPass de façon transparente. C'est un avantage pour toute organisation (hôtel, centre de congrès, etc.) qui veut attirer et fidéliser une population d'utilisateurs professionnels (voir Section 5.7.4 pour l'architecture).

<sup>3</sup> [www.ipass.com](http://www.ipass.com)

### 3.3 Provisionnement de comptes utilisateur

Les comptes peuvent être créés de différentes façons, soit par l'administrateur depuis l'outil d'administration, soit depuis le portail de délégation par un administrateur délégué, soit par l'utilisateur final à travers les méthodes d'auto-enregistrement du portail captif.

#### 3.3.1 Auto-enregistrement depuis le portail captif

Différents modes d'auto-enregistrement sont proposés, ces modes sont disponibles depuis le portail captif et peuvent éventuellement cohabiter. Il est par exemple possible de présenter un portail qui combine le mode standard (*login*/mot de passe) avec un ou plusieurs modes d'auto-enregistrement (SMS, email, ...).

L'avantage du provisionnement de compte par auto-enregistrement est de ne demander aucune intervention de l'administration puisque le compte de l'utilisateur est automatiquement créé par l'action d'auto-enregistrement. Pour renforcer la sécurité, il est possible d'ajouter un mot de passe préalable pour accéder au portail, ce mot de passe sera le même pour tous les utilisateurs du portail.

##### 3.3.1.1 Auto-enregistrement « One Click Button »

Le portail "One Click Button" a été conçu pour apporter une grande facilité d'usage. Un seul bouton de connexion pour accéder aux services. Une acceptation de charte ou un formulaire à renseigner peut venir compléter ce portail.



Figure 14: Portail "One Click Button"

##### 3.3.1.2 Auto-enregistrement libre (formulaire)

L'utilisateur s'enregistre sur le portail en indiquant son nom, prénom et éventuellement son email et son numéro de téléphone. Il reçoit ses identifiants directement sur le portail. L'avantage de ce mode est de privilégier la simplicité d'usage.



Figure 15: Portail avec auto-enregistrement par formulaire (libre)

### 3.3.1.3 Auto-enregistrement par SMS

L'utilisateur s'auto-enregistre sur le portail en indiquant son nom, prénom et numéro de téléphone mobile. Il reçoit son mot de passe par SMS sur son téléphone, son login sera son numéro de téléphone. Pour mettre en œuvre ce type de portail, il faudra que l'organisation utilisant la solution UCOPIA s'abonne à une des plates-formes de SMS proposées par UCOPIA. La traçabilité est garantie grâce au numéro de téléphone mobile.



Figure 16: Portail avec auto-enregistrement par SMS

### 3.3.1.4 Auto-enregistrement par email

L'utilisateur s'auto-enregistre sur le portail en indiquant son nom, prénom et adresse email. Il reçoit ses identifiants par email. Pour mettre en œuvre ce type de portail, l'administration devra « ouvrir » tout ou

partie du réseau pendant un laps de temps donné afin que l'utilisateur puisse consulter sa messagerie. La traçabilité est garantie grâce à l'email de l'utilisateur. Ce mode présente l'avantage d'être gratuit en comparaison du mode SMS qui a le coût d'envoi du SMS.



**UCOPIA**  
TURN YOUR WI-FI UP

BIENVENUE WELCOME  
WELKOM BENVENIDOS  
HERZLICH WILLKOMMEN  
BENVENUTI BEM-VINDO

**Enregistrement par email**

Renseignez l'ensemble des champs obligatoires pour vous enregistrer. Une fois l'enregistrement effectué, vous aurez quelques minutes pour vérifier votre messagerie et ainsi obtenir vos identifiants. Ce temps écoulé, vous devrez vous enregistrer de nouveau.

**Attention : votre adresse email doit être valide car elle sera utilisée pour envoyer votre ticket de connexion.**

Nom   
Prénom   
Adresse email

\* Champs obligatoires

[Retour](#) [S'enregistrer](#)

Figure 17: Portail avec auto-enregistrement par mail

### 3.3.1.5 Auto-enregistrement par impression de ticket

L'utilisateur s'enregistre sur le portail en renseignant un formulaire et demande l'impression d'un ticket sur lequel se trouveront ses identifiants de connexion. Le ticket s'imprime à l'accueil de l'organisation où la personne se présente. Ce mode présente l'avantage d'apporter un gain de temps substantiel pour le réceptionniste (pas d'information à saisir) et une connexion sécurisée (l'utilisateur doit se présenter à l'accueil pour récupérer ses identifiants, un contrôle d'identité peut éventuellement être réalisé).



**UCOPIA**  
TURN YOUR WI-FI UP

BIENVENUE WELCOME  
WELKOM BENVENIDOS  
HERZLICH WILLKOMMEN  
BENVENUTI BEM-VINDO

**Imprimez vos identifiants**

Renseignez l'ensemble des champs obligatoires pour vous enregistrer. Vos identifiants seront disponibles sur un ticket de connexion imprimé.

Nom   
Prénom

\* Champs obligatoires

[Retour](#) [S'enregistrer](#)

**Bienvenue au centre des congrès**

Identifiant	jdurant
Mot de passe	WSD2fgMu
Nom	Durant
Prénom	Jean

Figure 18 : Portail avec auto-enregistrement par impression de ticket


### 3.3.2 Parrainage

Afin de renforcer la sécurité pour les modes d'auto-enregistrement, il est possible de faire valider la demande d'enregistrement par un tiers, un parrain.

Ainsi lors de l'auto-enregistrement sur le portail, l'utilisateur renseigne l'email de son parrain auquel sera envoyée la demande d'enregistrement. Le parrain reçoit un email avec deux liens lui permettant d'accepter ou de refuser la demande.

L'utilisateur est notifié de la décision sur le portail.

Ce mode par parrainage peut être utilisé pour les modes d'auto-enregistrement par email, SMS et formulaire.



The screenshot shows the UCOPIA 'Enregistrement libre' (Free Registration) form. At the top is the UCOPIA logo and a row of flags representing various languages. Below the logo, the text 'Enregistrement libre' is followed by instructions: 'Renseignez l'ensemble des champs obligatoires pour vous enregistrer. Vos identifiants s'afficheront directement sur le portail. Votre demande sera envoyée à votre sponsor pour validation. Vous serez informé une fois votre compte activé.' The form contains several input fields: 'Nom \*', 'Prénom \*', 'Adresse email', 'Numéro de téléphone' (with a dropdown for 'Préfixe' and a text field for 'Numéro de téléphone'), 'Nom de l'entreprise \*', and 'Adresse email du parrain \*'. A note at the bottom right states '\* Champs obligatoires'. At the bottom are two buttons: 'Retour' and 'S'enregistrer'.

Figure 19: Auto-enregistrement avec parrainage

### 3.3.3 Portail de délégation

L'administrateur peut déléguer à une ou plusieurs personnes le droit de créer des comptes utilisateurs. Pour ce faire, un portail de délégation est mis à disposition de ces personnes habilitées. Ce portail est plus particulièrement utilisé pour accueillir des visiteurs dans une entreprise ou des clients dans un hôtel. Le portail de délégation ne nécessite aucune compétence technique, il s'agit d'un outil Web très simple d'utilisation.

Les administrateurs délégués peuvent être définis localement dans l'annuaire UCOPIA où appartenir à un annuaire d'entreprise externe (Active Directory par exemple).

Le portail de délégation est disponible en plusieurs langues.

#### 3.3.3.1 Prérogatives des administrateurs délégués

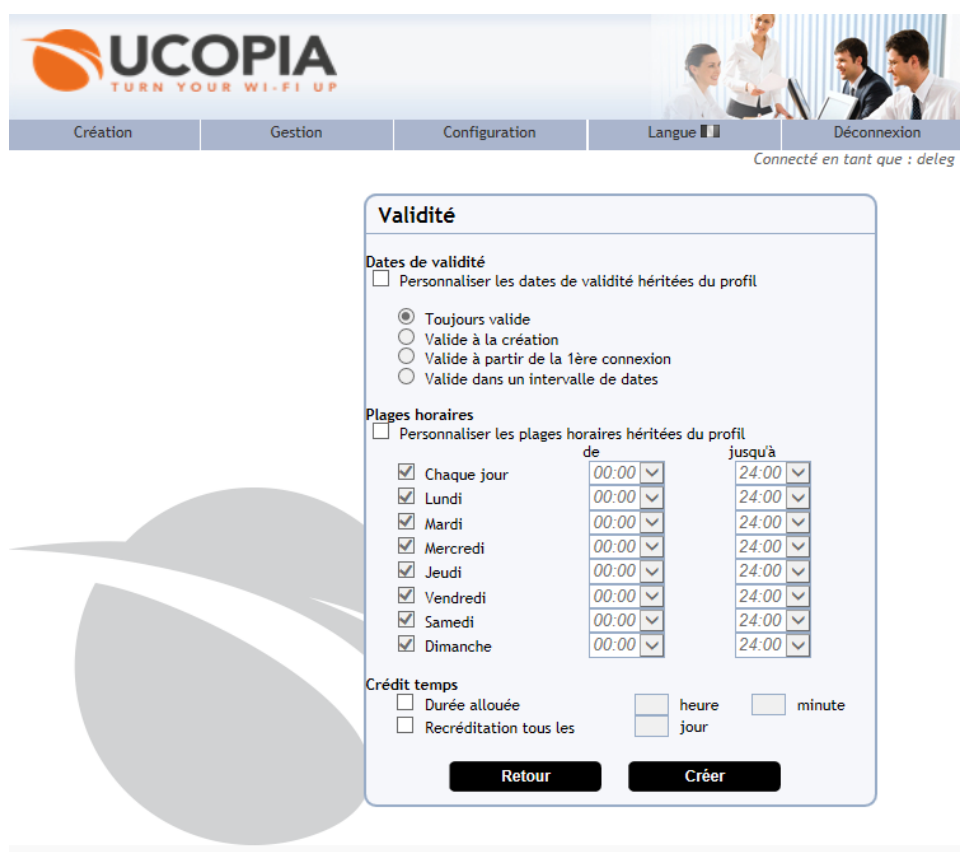
L'administrateur UCOPIA peut adapter le portail de délégation en fonction des usages et des utilisateurs. L'administrateur peut en conséquence créer différents profils ayant plus ou moins de prérogatives. Le portail de délégation s'adaptera alors automatiquement en fonction des prérogatives de son utilisateur.

Par exemple, pour un usage simplifié, l'outil pourra être réduit à sa plus simple expression en générant un ticket de connexion à partir des seules informations de nom et prénom de l'utilisateur. Pour un usage plus avancé, l'administrateur délégué sera à même de créer un compte en allouant un profil, une plage horaire, il pourra éventuellement modifier le compte après création, rééditer un ticket de connexion, régénérer un mot de passe, détruire le compte, etc.

Voici à titre d'exemple, une utilisation du portail de délégation.

1. Choix d'un profil parmi un ensemble de profils prédéfinis
2. Renseignement des informations nominatives de l'utilisateur
3. Choix de plages horaires et/ou de crédit temps
4. Génération d'un ticket de connexion résumant les informations permettant à l'utilisateur de se connecter (*login*, mot de passe, restrictions horaires, etc.)
5. Le ticket peut être imprimé, envoyé par email ou par SMS suivant les possibilités de l'UCOPIA en place.

Les copies d'écran ci-dessous montrent respectivement la sélection d'une plage horaire de connexion et/ou d'un crédit temps depuis le portail de délégation ainsi que la gestion des comptes utilisateur.



**Validité**

Dates de validité

☐ Personnaliser les dates de validité héritées du profil

☒ Toujours valide

☐ Valide à la création

☐ Valide à partir de la 1ère connexion

☐ Valide dans un intervalle de dates

Plages horaires

☐ Personnaliser les plages horaires héritées du profil

	de	jusqu'à
<input checked="" type="checkbox"/> Chaque jour	00:00	24:00
<input checked="" type="checkbox"/> Lundi	00:00	24:00
<input checked="" type="checkbox"/> Mardi	00:00	24:00
<input checked="" type="checkbox"/> Mercredi	00:00	24:00
<input checked="" type="checkbox"/> Jeudi	00:00	24:00
<input checked="" type="checkbox"/> Vendredi	00:00	24:00
<input checked="" type="checkbox"/> Samedi	00:00	24:00
<input checked="" type="checkbox"/> Dimanche	00:00	24:00

Crédit temps

☐ Durée allouée

☐ Recréditation tous les

heure minute

jour

**Retour** **Créer**

Figure 20: Portail de délégation – Gestion de la validité





**Figure 21: Portail de délégation – Gestion des utilisateurs**

### 3.3.3.2 Personnalisation du portail de délégation

Le portail de délégation est personnalisable grâce à un mode « Edition » permettant de changer le fond d'écran, le logo, d'ajouter des images, du texte, etc.

### 3.3.3.3 Multi zones

A l'instar du portail d'authentification, le portail de délégation peut se décliner par zone. Par exemple, dans le cadre d'une architecture centralisée, une chaîne d'hôtels pourra proposer pour chacune de ses enseignes un portail de délégation aux couleurs de l'enseigne.

### 3.3.3.4 Génération de comptes en masse

Le portail de délégation autorise la génération de comptes « en masse », cette fonctionnalité s'avérant très pratique lors d'événements tels que séminaires ou congrès. La création en masse peut s'effectuer en important un fichier au format CSV afin d'obtenir les informations nominatives des utilisateurs. Les tickets de connexion peuvent être imprimés ou envoyés par mail ou SMS.

## 3.4 Paiement et facturation

UCOPIA permet la mise en œuvre de solution de paiement d'accès Internet, paiement en ligne depuis le portail captif ou connecteur avec des outils de facturation.

### 3.4.1 Paiement en ligne

L'utilisateur peut acheter un temps de connexion ou crédit temps en réalisant un paiement en ligne. L'utilisateur est invité à choisir un forfait sur le portail UCOPIA puis est redirigé vers le site Paypal ou Ogone suivant la configuration du portail UCOPIA. Il peut payer soit en utilisant son compte Paypal soit en utilisant sa carte de paiement (PayPal ou Ogone). Une fois la transaction effectuée avec succès, l'utilisateur peut se connecter sur le portail UCOPIA en utilisant le login et mot de passe délivrés par



UCOPIA sur le portail. Optionnellement les identifiants peuvent être délivrés par SMS. La traçabilité est assurée car UCOPIA récupère les informations nominatives de l'utilisateur depuis le site PayPal ou Ogone. Pour mettre en œuvre ce type de portail l'organisation utilisant UCOPIA doit posséder un compte PayPal ou Ogone afin de se voir rétribuée des achats des utilisateurs.



Figure 22: Portail avec paiement en ligne et choix de forfaits

### 3.4.2 Connexion avec outil de facturation (PMS)

UCOPIA fonctionne en association à des outils de facturation de type PMS (*Property Management System*). Comme le paiement en ligne, le couplage UCOPIA/PMS utilise une notion de forfait. Le forfait est défini par l'administrateur UCOPIA. Cela peut être un forfait 1h, 3h, ou forfait « emails », ou forfait « Tous les jours ouvrés de 16h à 18h », etc. Les forfaits sont proposés au choix de l'utilisateur sur le portail UCOPIA après authentification.

### 3.4.3 Connexion avec serveur de cartes prépayées (PPS)

UCOPIA peut fonctionner avec un serveur de cartes prépayées de type PPS (Pre Paid System). A chaque carte est associé un temps de connexion. L'utilisateur s'authentifie sur le portail captif avec l'identifiant de sa carte et un captcha code. Le temps octroyé par la carte et le temps consommé s'affichent sur le portail après authentification.

### 3.4.4 Gestion d'événements

Pour répondre aux besoins des environnements de type centres d'exposition, UCOPIA propose une gestion d'événement. Un événement se matérialise par un forfait nommé et une date de validité, par exemple « Le salon de l'auto du 4 au 12 avril ».

Un exposant peut acheter sur le portail captif (via Ogone) une extension de son forfait pour plusieurs connexions simultanées, pour par exemple offrir un accès Internet à ses visiteurs ou collaborateurs.

Un prix dégressif peut être appliqué pour les achats de connexions supplémentaires. Un récapitulatif des paiements (sous la forme d'un document PDF) peut être obtenu par l'exposant depuis le portail captif.

## 3.5 Administration

---

L'outil d'administration est dédié à l'administrateur réseau, il permet de gérer les politiques de mobilité de l'entreprise, l'ensemble de la configuration UCOPIA ainsi que les aspects supervision et journalisation.

L'administration peut déléguer à des personnes habilitées mais non spécialistes réseau des droits d'administration limités, notamment la création de comptes utilisateur. Le délégué dispose d'un portail dit de délégation pour créer ou modifier des comptes utilisateur (voir Section 3.3.3).

L'outil d'administration ainsi que le portail de délégation sont accessibles à travers une interface Web sécurisée en HTTPS.

### 3.5.1 Profils d'administration

Différents profils d'administration peuvent être créés afin d'octroyer plus ou moins de prérogatives aux administrateurs. Par exemple, un administrateur sera habilité à effectuer des modifications de configuration réseau alors qu'un autre ne pourra que modifier les profils utilisateurs ou les portails d'authentification.

### 3.5.2 Administration des politiques de sécurité et de mobilité

L'outil d'administration UCOPIA va permettre de définir les services qui seront accessibles depuis le réseau d'accueil, les profils utilisateurs (droits d'accès, plages horaires, zones, QoS, filtrage d'URLs, etc.) et les utilisateurs. Par défaut un utilisateur hérite des propriétés de son profil mais il est possible de redéfinir pour un utilisateur certaines propriétés telles que sa durée de validité ou les plages horaires de connexion.

Les services sont caractérisés par différents paramètres tels que les numéros de ports, les adresses IP des serveurs impliqués dans le service, les protocoles réseau, etc. UCOPIA est livré avec un ensemble de services prédéfinis (Web, Mail, Transfert de fichier, VPN, etc.), ces services sont bien sûr personnalisables.

Les catégories d'URLs devant être filtrées et donc interdites peuvent être spécifiées au niveau de chaque profil d'utilisateur.


La copie d'écran ci-dessous montre la création d'un profil utilisateur avec sélection des droits d'accès, des heures de connexion et des URLs autorisées.


 contrôleur  
 V2401175 - 5.0 (build 14061607)  
 Connecté en tant que : admin

Configuration Administration Supervision Exploitation

Accès CLI Documentation Redémarrer Arrêter

Utilisateurs  
 Profils  
 Services  
 Délégation  
 Zones  
 Forfaits  
 Contraintes de champ  
 Récupération de mot de passe  
 Administrateurs

Choisissez votre langue  


Déconnexion

### Gestion des profils

Modification du profil Visiteur

Défaut Ajouter condition

Paramètres du profil

ID de profil Visiteur

Droits d'accès

Services du profil

Services disponibles

Administration  
 File\_Transfer  
 Full\_Access  
 Instant\_Messaging  
 Microsoft\_Network  
 Printers  
 Remote\_Access  
 SSH  
 Telnet  
 VPN

<<< Ajouter  
 Supprimer >>>

Validité

Dates de validité

Toujours valide  
 Valide à la création  
 Valide à partir de la 1ère connexion  
 Valide dans un intervalle de dates

Crédit temps :

Durée allouée : heure et minute  
 Recrédition tous les jour

Plages horaires

Chaque jour de 00:00 jusqu'à 24:00  
 Lundi de 00:00 jusqu'à 24:00  
 Mardi de 00:00 jusqu'à 24:00  
 Mercredi de 00:00 jusqu'à 24:00  
 Jeudi de 00:00 jusqu'à 24:00  
 Vendredi de 00:00 jusqu'à 24:00  
 Samedi de 00:00 jusqu'à 24:00  
 Dimanche de 00:00 jusqu'à 24:00

Zones

Cette section permet de définir les zones d'entrée et de sortie.

Reconnaissance d'équipements utilisateur

Cette section permet de définir les options de reconnaissance des équipements et les actions associées.

Traffic web

Activer la redirection vers le proxy web pour les ports 8080, 3128.  
 Pour configurer la liste des ports : Configuration de la liste des ports

Appliquer Google SafeSearch.

Activer le filtrage des URLs.

Catégories filtrées

Catégories disponibles

Adulte  
 Agressif  
 Vidéo  
 Banque  
 Blog  
 Chat  
 Rencontre  
 Drogue  
 Hébergement  
 Jeux d'argent

Politiques de mot de passe

Cette section permet de définir des politiques de mot de passe en fonction de différentes sources de modification pour ce profil.

Limitation de bande passante et quotas

Cette section permet de définir une limitation de bande passante ainsi que des quotas de données pour chaque équipement de l'utilisateur.

Options avancées

Cette section permet de définir les options d'authentification avancée.

\* Champs obligatoires

Valider

Figure 23: Définition d'un profil utilisateur

### 3.5.3 Supervision, traçabilité

UCOPIA gère des journaux de sessions et de trafic, ces journaux sont créés localement sur le contrôleur UCOPIA et sont accessibles depuis l'outil d'administration UCOPIA.

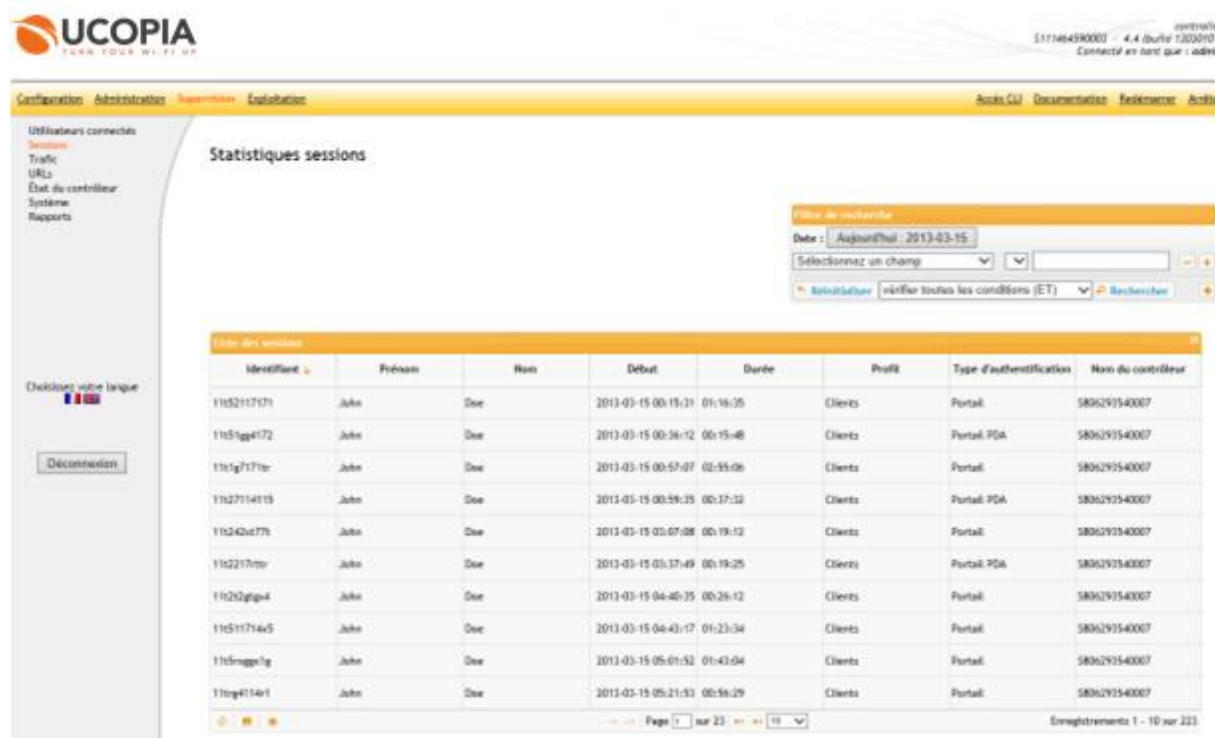
#### ■ Les journaux de sessions

Concernant les journaux de sessions, les informations sauvegardées sont les suivantes :

- Le *login*, nom et prénom de l'utilisateur
- Les adresses IP et MAC de l'utilisateur
- Le sous-réseau d'entrée sur lequel l'utilisateur se trouve
- Le type d'authentification : 802.1x ou mode portail Web
- Les horaires de connexion : heure à laquelle l'utilisateur s'est connecté, heure à laquelle il s'est déconnecté
- Le profil de l'utilisateur

- Les champs additionnels ajoutés par l'administrateur, par exemple email, nom de société, numéro de carte d'identité.

La figure suivante montre le journal des sessions depuis l'outil d'administration UCOPIA.



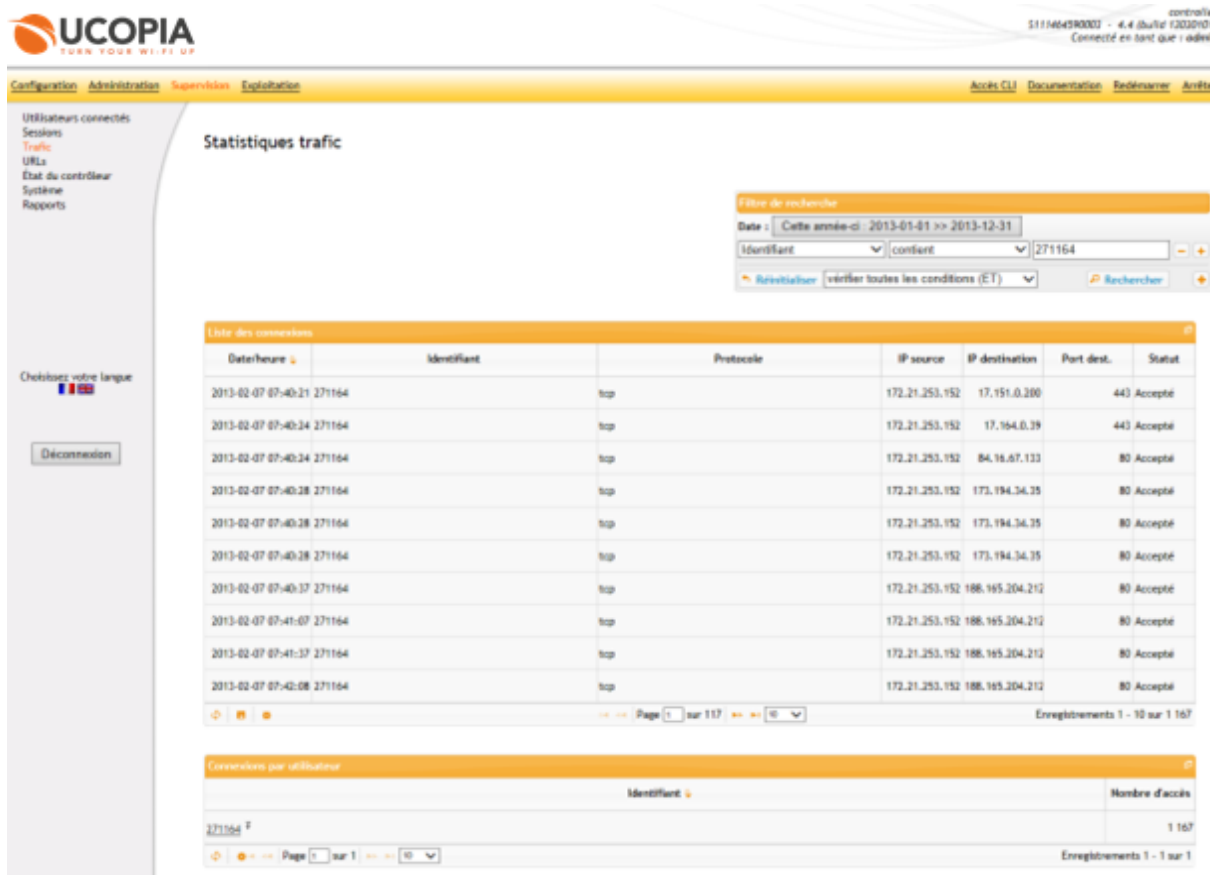
**Figure 24: Journal des sessions utilisateurs**

#### ■ Les journaux d'activité ou de trafic

Concernant les journaux d'activité, les informations sauvegardées sont les suivantes :

- Les types de services utilisés, la fréquence d'utilisation de chacun d'eux
- Les adresses IP sources et destinations
- Les numéros de ports
- Les URLS

La figure suivante montre le journal des sessions depuis l'outil d'administration UCOPIA.

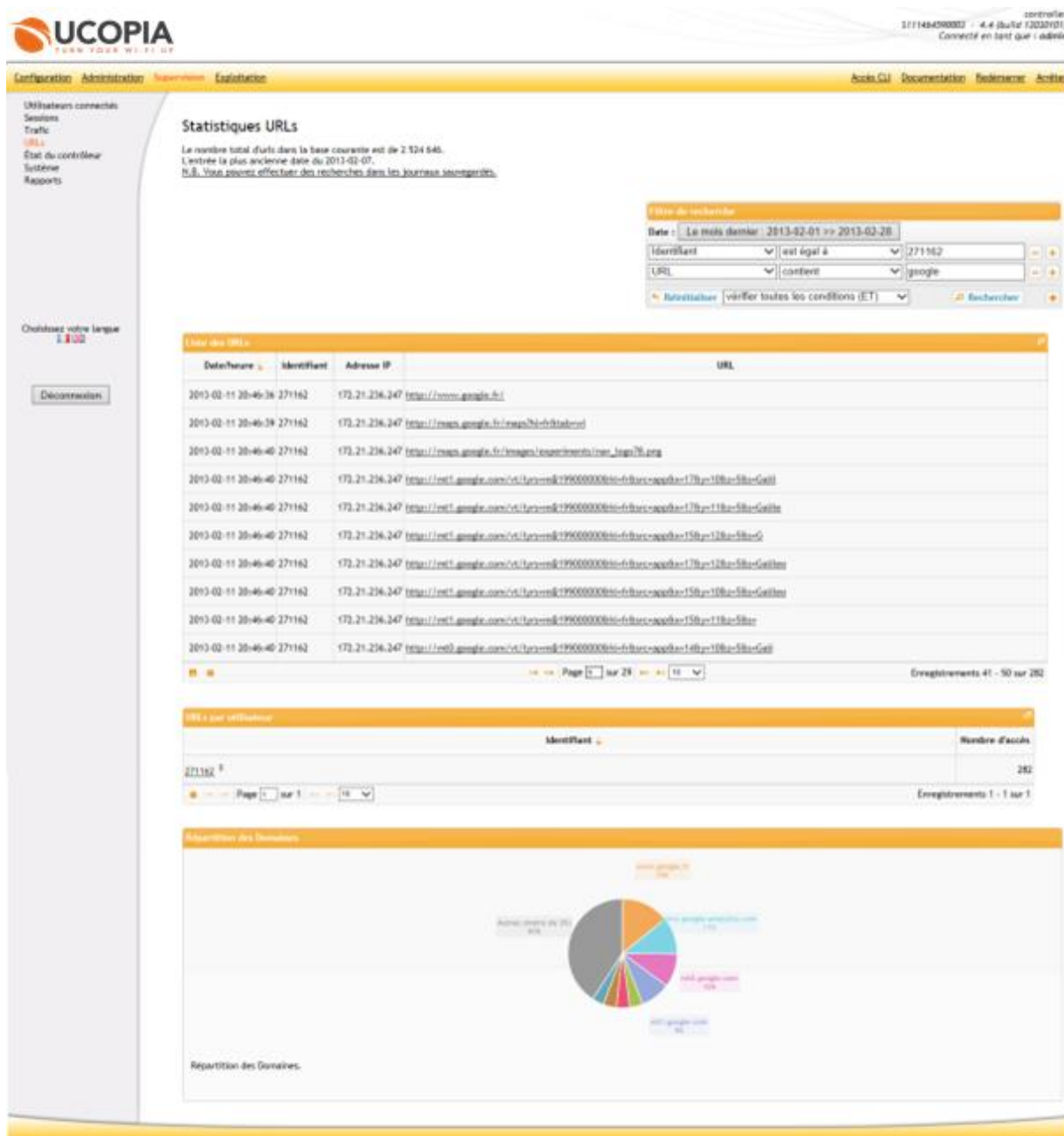


The screenshot displays the UCOPIA management interface. The top navigation bar includes links for Configuration, Administration, Supervision, and Exploitation. The left sidebar shows a menu with options like Utilisateurs connectés, Sessions, Traffic, URLa, État du contrôleur, Système, and Rapports. The main content area is titled 'Statistiques trafic' and features a search filter section. The filter is set to search for the identifier '271164' in the 'contient' field. Below the filter is a table titled 'Liste des connexions' showing a list of connections for the selected user. The table has columns for Date/heure, Identifiant, Protocole, IP source, IP destination, Port dest., and Statut. The connections listed are all for the user 271164, with various IP addresses and ports, and all are marked as 'Accepté'. At the bottom, there is a section titled 'Connexions par utilisateur' showing the total number of connections for the selected user, which is 1167.

Date/heure	Identifiant	Protocole	IP source	IP destination	Port dest.	Statut
2013-02-07 07:40:21	271164	tcp	172.21.253.152	17.151.0.200	443	Accepté
2013-02-07 07:40:24	271164	tcp	172.21.253.152	17.154.0.39	443	Accepté
2013-02-07 07:40:24	271164	tcp	172.21.253.152	84.16.67.133	80	Accepté
2013-02-07 07:40:28	271164	tcp	172.21.253.152	173.194.34.35	80	Accepté
2013-02-07 07:40:28	271164	tcp	172.21.253.152	173.194.34.35	80	Accepté
2013-02-07 07:40:28	271164	tcp	172.21.253.152	173.194.34.35	80	Accepté
2013-02-07 07:41:37	271164	tcp	172.21.253.152	188.165.204.212	80	Accepté
2013-02-07 07:41:37	271164	tcp	172.21.253.152	188.165.204.212	80	Accepté
2013-02-07 07:41:37	271164	tcp	172.21.253.152	188.165.204.212	80	Accepté
2013-02-07 07:42:08	271164	tcp	172.21.253.152	188.165.204.212	80	Accepté

**Figure 25: Journal d'activité pour un utilisateur**

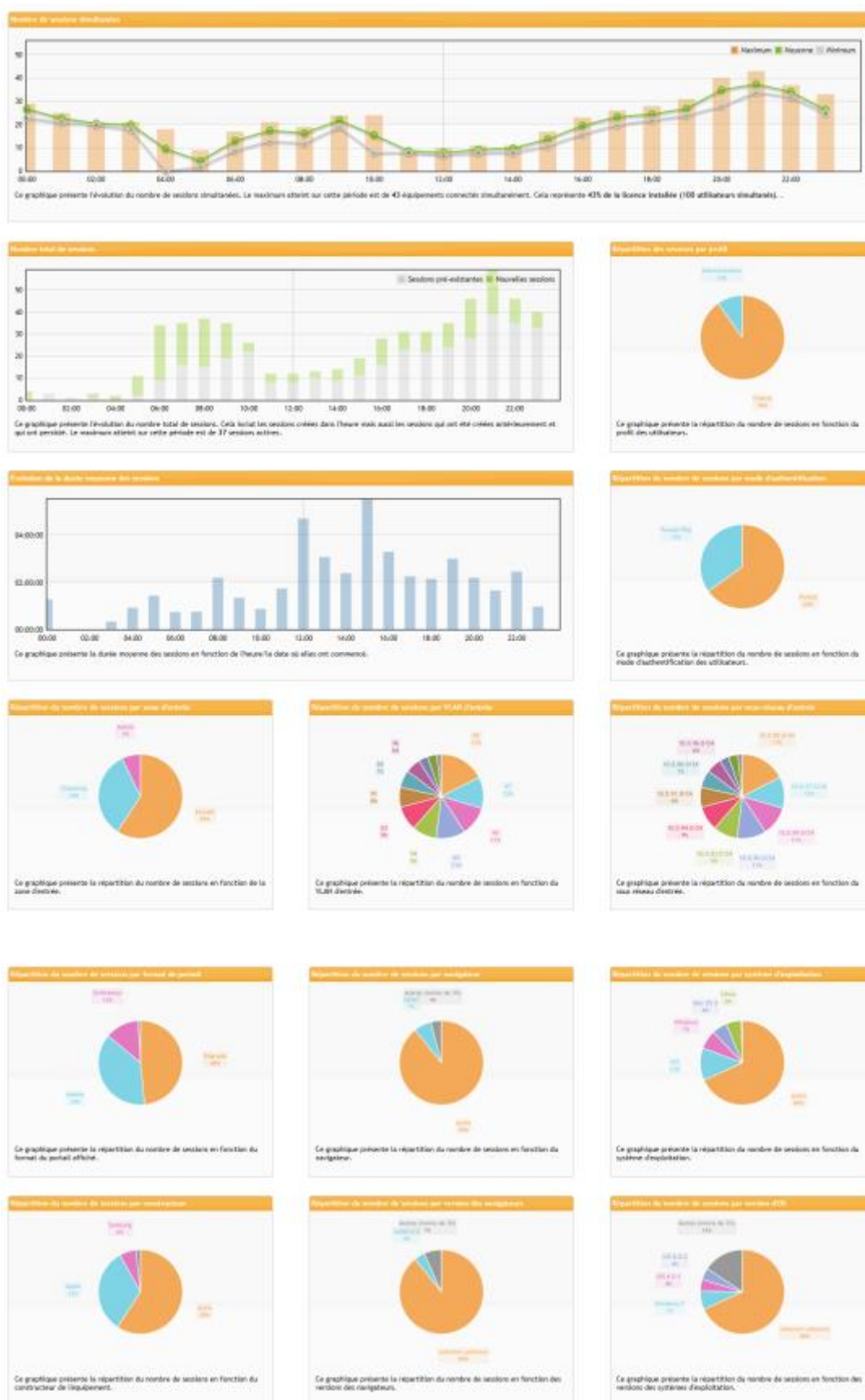
La recherche d'un utilisateur à partir d'une information est particulièrement simple. Par exemple, la copie d'écran ci-dessous montre le résultat de la demande « qui a visité l'URL [www.google.com](http://www.google.com) dans un intervalle de temps défini ». UCOPIA retrouve le ou les utilisateurs répondant à ces critères, l'ensemble des pages visitées est présenté.



**Figure 26: Journal d'activité (URLs visitées par un utilisateur)**

Les journaux sont compressés dynamiquement afin d'optimiser la place sur le disque dur du contrôleur UCOPIA. Les journaux peuvent également être exportés, manuellement ou automatiquement (via FTPS), vers une machine tierce.

Les journaux peuvent être également utilisés à des fins de statistiques pour notamment mieux appréhender l'usage qui est fait du contrôleur UCOPIA. Pour cela, UCOPIA propose différentes vues statistiques préconfigurées.



**Figure 27: Visualisation de statistiques**

La connaissance de l'ensemble de ces données d'exploitation du réseau d'accueil permet à l'administrateur UCOPIA d'optimiser sa gestion en déterminant par exemple si le réseau est



correctement dimensionné pour répondre aux besoins des utilisateurs. Il permet également de savoir quels sont les utilisateurs qui se connectent régulièrement sur le réseau, quels sont les services qui sont sollicités, les ressources déployées pour ces demandes, etc.

### 3.5.4 Reporting

Un rapport de statistiques des sessions utilisateurs au format PDF peut être généré automatiquement et périodiquement (par jour, par semaine, etc.). Le rapport est envoyé par email à un ou plusieurs destinataires ou déposé sur un serveur FTP.

Les rapports peuvent être générés par zone.

Le rapport inclut des statistiques telles que :

- **Nombre de sessions simultanées**
- **Nombre total de sessions**
- **Durée moyenne des sessions**
- **Répartition du nombre de sessions par mode d'authentification, par profil utilisateur**
- **Répartition du nombre de sessions par sous-réseau d'entrée, par zone**
- **Répartition du nombre de sessions par constructeurs d'équipement, par système d'exploitation**
- **Liste des utilisateurs les plus consommateurs en bande passante**
- **etc.**

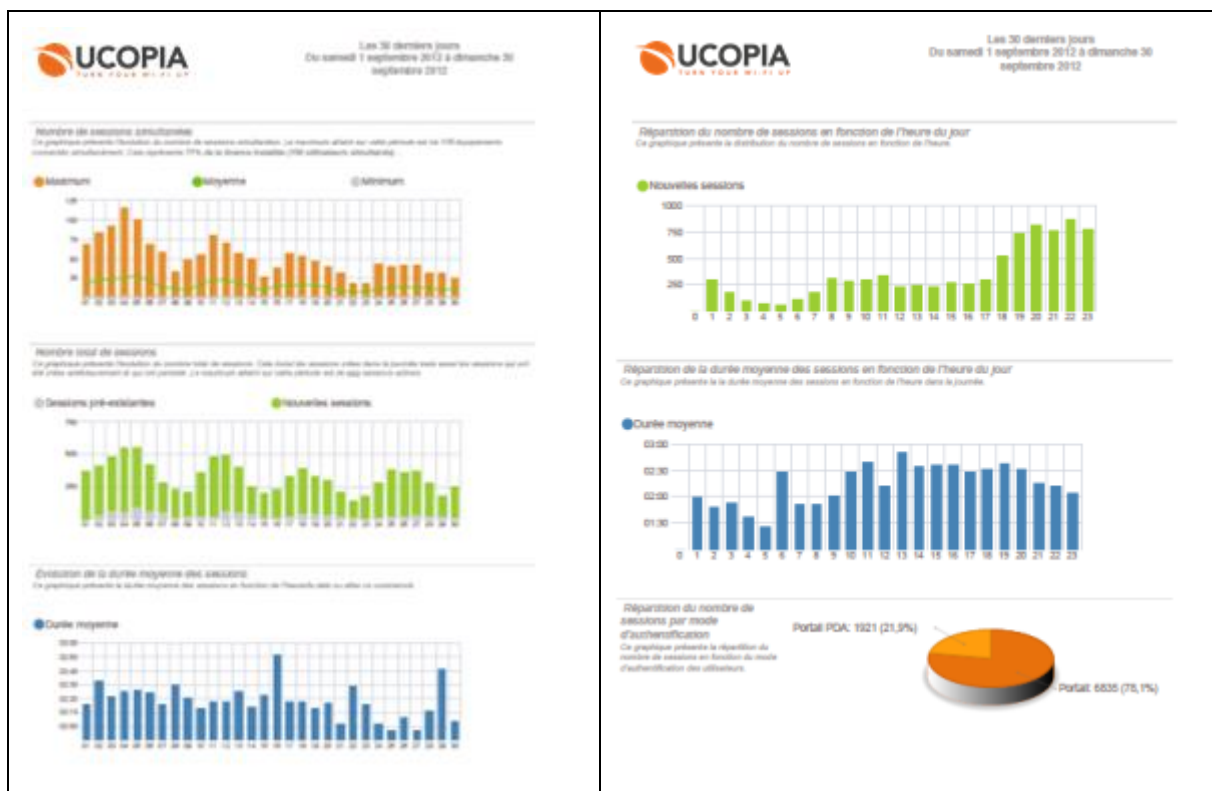


Figure 28: Exemple de rapport au format PDF



### 3.5.5 Configuration du contrôleur UCOPIA

A travers l'outil d'administration, l'administrateur UCOPIA va pouvoir spécifier le paramétrage global du contrôleur (paramètres réseau, VLAN, etc.) et effectuer des configurations plus spécifiques telles que cascade d'annuaires ou configuration du RADIUS en mode proxy.

### 3.5.6 Exploitation du contrôleur UCOPIA

L'exploitation du contrôleur consiste à gérer les sauvegardes de l'ensemble de la configuration (configuration réseau, personnalisation, annuaire UCOPIA, journaux), mettre à jour le contrôleur UCOPIA avec les dernières Releases, mettre en place un tunnel pour autoriser la télémaintenance (tunnel entre le contrôleur et les serveurs de maintenance UCOPIA), etc.

Les sauvegardes de configuration peuvent être faites automatiquement sur un serveur FTP.

### 3.5.7 Administration centralisée

Dans le cas d'architecture multi sites, plusieurs contrôleurs UCOPIA peuvent être déployés (voir Section Architecture ). Dans ce cas, un contrôleur sera configuré comme étant « Principal », il sera alors en charge de l'administration centralisée de tous les autres contrôleurs.

### 3.5.8 Administration SNMP

Le contrôleur UCOPIA intègre un agent SNMP, lui permettant ainsi d'être supervisé depuis un outil de supervision du marché compatible SNMP.

UCOPIA propose une MIB standard MIB-2 afin de permettre le dialogue entre l'outil de supervision et l'agent UCOPIA. De plus, des *traps* SNMP peuvent être déclenchés afin de surveiller les différents services actifs du contrôleur (DHCP, RADIUS, SQL, etc.).

### 3.5.9 Administration via CLI

Une CLI (*Command Line Interface*) est disponible. L'objectif est de permettre certaines opérations d'administration avancée.

La CLI est accessible depuis l'outil d'administration graphique. Depuis la CLI, Il est par exemple possible de visualiser les différents journaux internes d'un contrôleur UCOPIA (DHCP, RADIUS, etc.), de lancer des commandes réseau (*nslookup*, *tcpdump*, etc.), de redémarrer ou de visualiser le statut des services (DHCP, RADIUS, proxy, LDAP, etc.).

### 3.5.10 Exportation Syslog

Le fichier Syslog UCOPIA qui centralise les journaux d'événements peut être exporté d'un contrôleur UCOPIA afin d'être pris en charge par un serveur Syslog. Les événements envoyés peuvent être filtrés par catégorie (DHCP, RADIUS, ...).

### 3.5.11 Administration multi sites

Dans le cas d'une architecture multi sites centralisée, il est intéressant de pouvoir dédier des opérations d'administration à chaque site. Pour cela, sur le contrôleur central, une zone d'entrée peut être associée à un site. Il sera alors possible d'administrer au niveau de la zone, par exemple en allouant une licence par zone, un portail, un compte Ogone, etc. Les rapports de statistiques peuvent également être générés par zone.

### 3.5.12 Gestion de compte par l'utilisateur

L'administrateur peut donner la possibilité à l'utilisateur de gérer son propre compte utilisateur depuis le portail captif. L'utilisateur pourra ainsi modifier ses informations personnelles (nom, prénom, email, ...) et gérer sa liste d'équipements. En effet, dans le cas où les équipements de l'utilisateur sont enregistrés par le contrôleur UCOPIA, ceux-ci seront visibles depuis la page d'administration de compte. L'utilisateur aura alors la possibilité d'intervenir, par exemple pour supprimer un équipement qui n'existe plus.

## 4 Architecture UCOPIA

Nous décrivons dans cette section les différents modules constituant l'architecture UCOPIA ainsi que les protocoles utilisés lors des interactions entre ces modules.

En règle générale, l'ensemble du trafic en provenance des utilisateurs est redirigé vers le contrôleur UCOPIA qui est en coupure logique (ou physique) entre un réseau d'accueil (Wi-Fi et/ou filaire) et le LAN de l'organisation.

Les protocoles d'authentification entre les postes des utilisateurs et le contrôleur UCOPIA sont soit 802.1x/EAP ou HTTPS. Le serveur RADIUS et les outils d'administration UCOPIA dialoguent avec le ou les annuaires LDAP à travers le protocole sécurisé LDAPS. La traçabilité est assurée par une base de données des journaux au format SQL. L'administration s'effectue en mode Web HTTPS.

Le contrôleur UCOPIA est basé sur une architecture Linux.

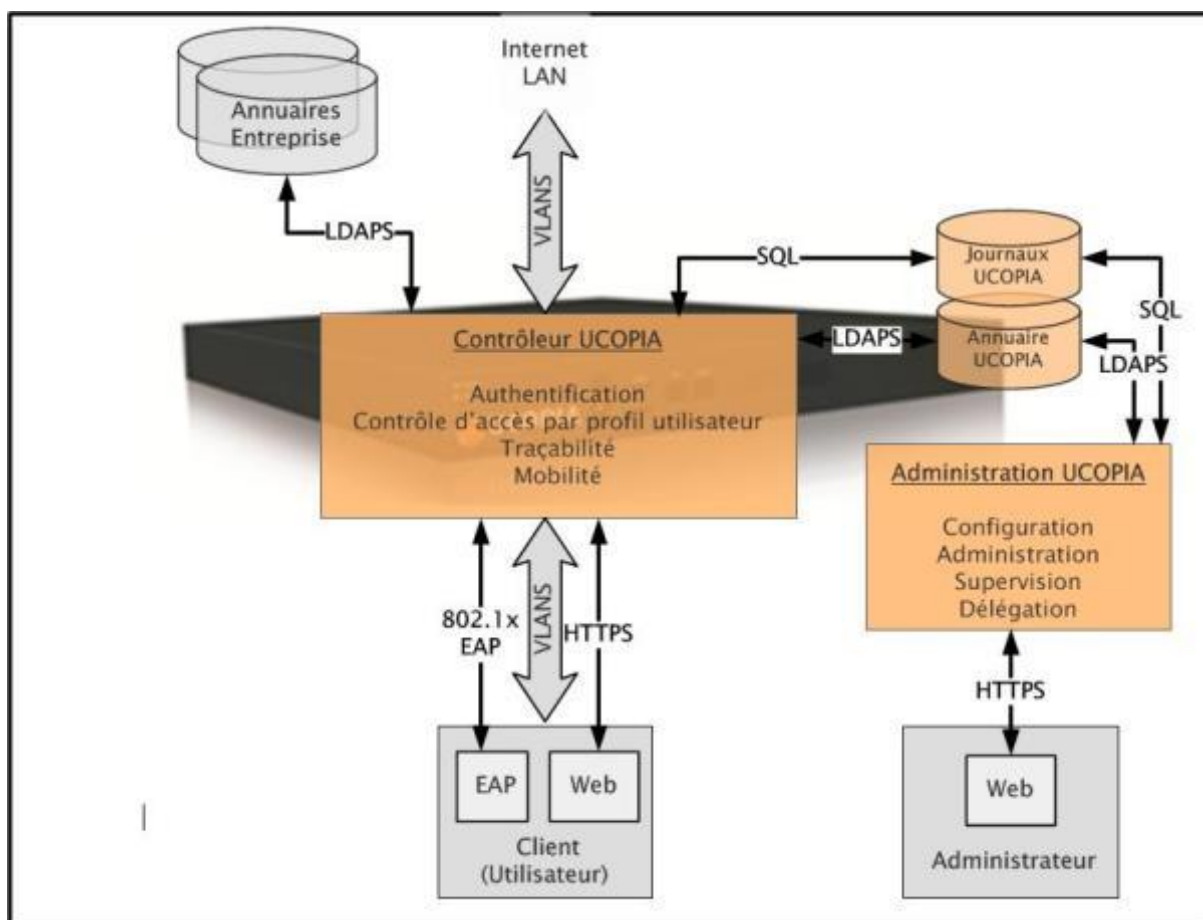
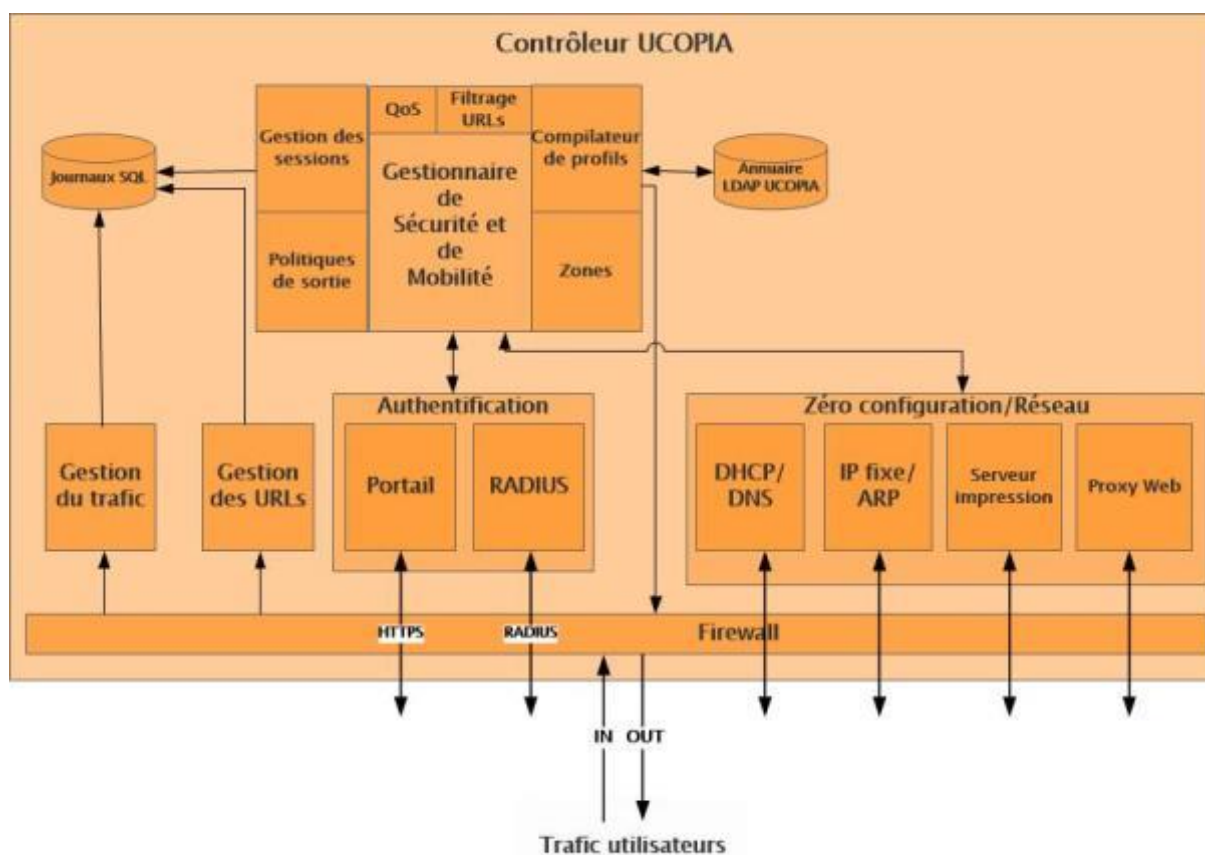


Figure 29: Architecture UCOPIA

### 4.1 Contrôleur UCOPIA

Le contrôleur est le cœur de l'architecture UCOPIA, il est en charge de mettre en œuvre les politiques de sécurité et de mobilité définies depuis l'outil d'administration. Le contrôleur comprend plusieurs modules en charge de l'authentification, du contrôle d'accès par profil utilisateur, de la Qualité de Service, du filtrage d'URLs, de l'accès transparent aux services, etc. Le module « **Gestionnaire de sécurité et de mobilité** » orchestre l'ensemble des modules.



**Figure 30: Architecture du contrôleur UCOPIA**

Le contrôleur est basé sur une technologie de filtrage qui permet de filtrer et de classer les paquets afin de mettre en œuvre respectivement le contrôle d'accès par profil utilisateur et la qualité de service. Le filtrage assure également la détection des flux correspondant à des configurations erronées. Le filtrage se base sur les adresses IP des utilisateurs mais aussi sur les adresses MAC, les numéros de ports, les types de protocoles, etc.

- **Authentification**: le contrôleur embarque un **serveur RADIUS** qui est le serveur d'authentification de l'architecture 802.1x. Ce serveur implémente différents algorithmes d'authentification (PEAP, TTLS ou TLS). Le **portail UCOPIA** propose une authentification par *login*/mot de passe et protocole HTTPS. Ce mode d'authentification peut également être utilisé via RADIUS, cette solution est utile pour les architectures à base d'interconnexions de serveurs RADIUS avec mécanisme de proxy. UCOPIA interroge l'annuaire LDAP UCOPIA et/ou un ou plusieurs annuaires externes pour réaliser l'authentification.
- **Contrôle d'accès** : une fois l'utilisateur authentifié, le module « **Compilateur de profil** » recherche le profil de l'utilisateur dans l'annuaire LDAP UCOPIA et le compile en règles de filtrage qu'il installe dynamiquement au niveau du contrôleur. Ces règles sont retirées lorsque l'utilisateur se déconnecte.
- **Qualité de Service** : le contrôleur UCOPIA reconnaît le flot et le marque pour que les paquets du flot soient traités d'une certaine façon. La classification des flux et la gestion de priorité sont implémentées par le module « **QoS** ». Les paquets sont dispatchés dans des files d'attente afin de mettre en œuvre la gestion de priorités.
- **Filtrage d'URLs** : le module « **Filtrage d'URLs** » permet de filtrer les URLs en provenance du trafic utilisateur et de ne rendre accessibles que celles autorisées. Le filtrage s'opère à

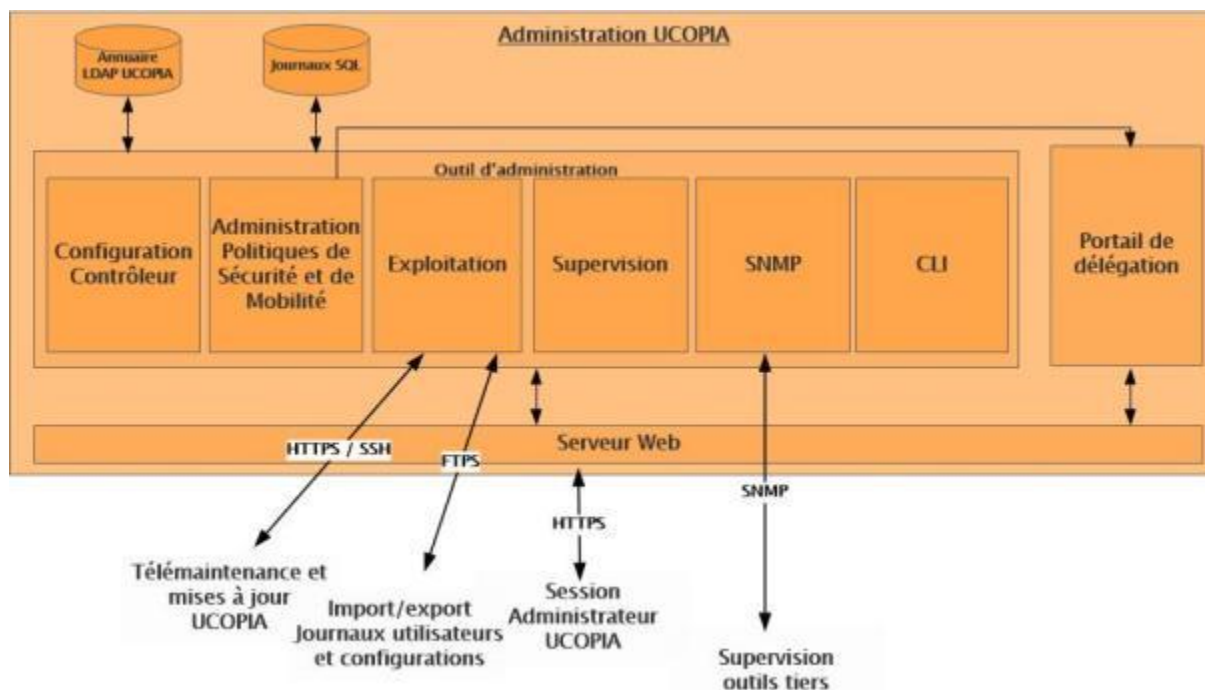
partir de catégories prédéfinies. La base des URLs est embarquée dans le contrôleur UCOPIA.

- **Accès transparent** : le module « **Zéro Configuration/Réseau** » est basé sur le mécanisme de filtrage des flux et permet de rectifier dynamiquement les erreurs de configuration par rapport à l'environnement d'accueil. Les techniques utilisés sont soit de la redirection de flux vers les serveurs appropriés (ex : mail ou proxy Web) soit de la mise à disposition automatique et transparente de composants nécessaires à l'exécution du service (ex : pilote d'imprimante). Pour réaliser la mise à disposition de pilotes d'imprimantes, un serveur d'impression est intégré au module « zéro configuration ». Par ailleurs, ce module délivre des @IP en mode DHCP mais permet également de prendre en charge des postes utilisateur configurés en @IP fixe.
- **Zones** : le module « **Zones** » implémente des zones logiques qui peuvent représenter des lieux ou des sites et qui s'implémentent en VLANs ou en sous-réseaux en fonction de la couche réseau mise en oeuvre (niveau 2 ou 3).
- **Rédirection VLAN** : Le module « **Politiques de sortie** » permet de router en sortie du contrôleur UCOPIA le flux d'un utilisateur dans un VLAN en fonction de son profil (au lieu de l'adresse de destination du flux). Ce module présente donc des fonctionnalités de routage évolué et utilise notamment le standard 802.1q pour la gestion des VLAN. Le flux de l'utilisateur peut également sortir du contrôleur en mode NAT ou en mode routage, en fonction de la politique.
- **Adressage réseau**: Le contrôleur embarque un **serveur DHCP**, fonctionne en mode NAT ou routage et assure un relais DNS.
- **Traçabilité** : Les journaux sont alimentés par trois sources et stockés dans une base de données SQL : le module '**Gestion des sessions**' enregistre les sessions des utilisateurs (login, nom, prénom, @IP, @Mac, etc.), le module « **Gestion du trafic** » enregistre le trafic des utilisateurs (entêtes de paquets IP), le module « **Gestion des URLs** » enregistre les URLs accédées par les utilisateurs.

## 4.2 Administration UCOPIA

---

L'outil d'administration UCOPIA est composé de plusieurs modules assurant la configuration du contrôleur UCOPIA, l'administration des politiques de mobilité et de sécurité, la supervision de l'activité du contrôleur, l'exploitation et les fonctions de délégation.



**Figure 31: Architecture des outils d'administration UCOPIA**

- **Configuration** : ce module permet de configurer les propriétés réseau du contrôleur UCOPIA ainsi que les mécanismes d'authentification, de zéro configuration et de redondance/répartition de charge. La personnalisation du portail UCOPIA et des tickets de connexion est également prise en charge par ce module. La configuration du contrôleur est traduite au niveau système en fichiers de configuration Linux.
- **Administration des politiques de sécurité et de mobilité** : ce module permet d'administrer les services, les profils utilisateurs et les utilisateurs. Il se repose sur un modèle de mobilité implémenté sous la forme d'un schéma LDAP afin d'assurer la persistance des informations, ce schéma LDAP prend place dans l'annuaire LDAP embarqué dans le contrôleur UCOPIA. Le protocole sécurisé LDAPS est utilisé pour dialoguer avec l'annuaire.
- **Supervision du contrôleur** : les journaux de sessions et d'activité sont générés par le contrôleur UCOPIA dans une base de données de type SQL. Ce module permet d'interroger cette base de données à travers des requêtes SQL.
- **Exploitation** : ce module a en charge tout ce qui concerne l'exploitation du contrôleur UCOPIA : sauvegarde/restauration des configurations (manuelle ou automatique via le protocole FTPS), sauvegarde/restauration des journaux utilisateurs (manuelle ou automatique via le protocole FTPS), mise à jour du contrôleur UCOPIA avec les nouvelles versions UCOPIA, télémaintenance, etc. Les sauvegardes de configuration sont au format archive (.tar) compressée. Les mises à jour de version doivent être soit téléchargées manuellement depuis le site Extranet UCOPIA, soit automatiquement téléchargées depuis la plate-forme de gestion de parc UCOPIA. La télémaintenance est assurée par un tunnel SSH qui s'établit depuis le contrôleur UCOPIA vers les serveurs de maintenance UCOPIA.
- **SNMP** : agent SNMP, permettant ainsi au contrôleur d'être supervisé depuis un outil de supervision du marché compatible SNMP.
- **CLI** : langage de commandes permettant une administration avancée du contrôleur.
- **Portail de délégation** : le portail est en charge du provisionnement de compte lors de l'accueil de visiteurs, il est accessible depuis une interface Web en HTTPS. Il s'interface

avec l'annuaire LDAP UCOPIA afin de créer les comptes utilisateurs, le protocole utilisé est LDAPS.

### 4.3 Points d'accès Wi-Fi

---

Les prérequis des points d'accès Wi-Fi dépendent des protocoles utilisés notamment lors de l'authentification, par exemple une authentification 802.1x nécessitera que les points d'accès supportent ce protocole. Les points d'accès sont configurés avec plusieurs SSIDs, chaque SSID est encapsulé dans un VLAN. On associe à chaque VLAN une plage d'adresses IP et un mode d'authentification (802.1x ou mot de passe) et ce de manière à isoler les différentes populations d'utilisateurs Wi-Fi.

L'adresse du serveur RADIUS doit être spécifiée dans les points d'accès, ainsi que le secret partagé avec le serveur.

### 4.4 Prérequis des postes utilisateurs

---

Chaque mode d'authentification impose plus ou moins de pré-requis sur le poste de l'utilisateur.

- **Portail Web HTTPS** : la clé d'authentification est un couple *login*/mot de passe qui sera utilisé sur le portail UCOPIA. Aucun pré-requis sur le poste de l'utilisateur n'est demandé. Ce mode est compatible avec tout type de systèmes d'exploitation et de navigateurs Internet.
- **802.1x/PEAP, TTLS** : la clé d'authentification est un couple *login*/mot de passe. L'utilisation du protocole PEAP ou TTLS nécessite un client 802.1x sur le poste de l'utilisateur (en standard sur Windows depuis Windows 2000 Service Pack 4).
- **802.1x/EAP-TLS** : la clé d'authentification est un certificat. Le protocole d'authentification EAP/TLS est basé sur une architecture PKI avec certificats. Les certificats sont de type X509 et installés dans le format PKCS#12 (Personal Information Exchange Syntax Standard) pour le stockage des clés privées. Ils s'installent soit directement sur le poste de l'utilisateur, soit sur une carte à puce dans le format PKCS#12 (Public-Key Cryptography Standards). L'environnement EAP/TLS de Windows est disponible à partir de la version Windows 2000 Service Pack 3. Ce mode d'authentification ne nécessite pas de logiciel client sur le poste de l'utilisateur.

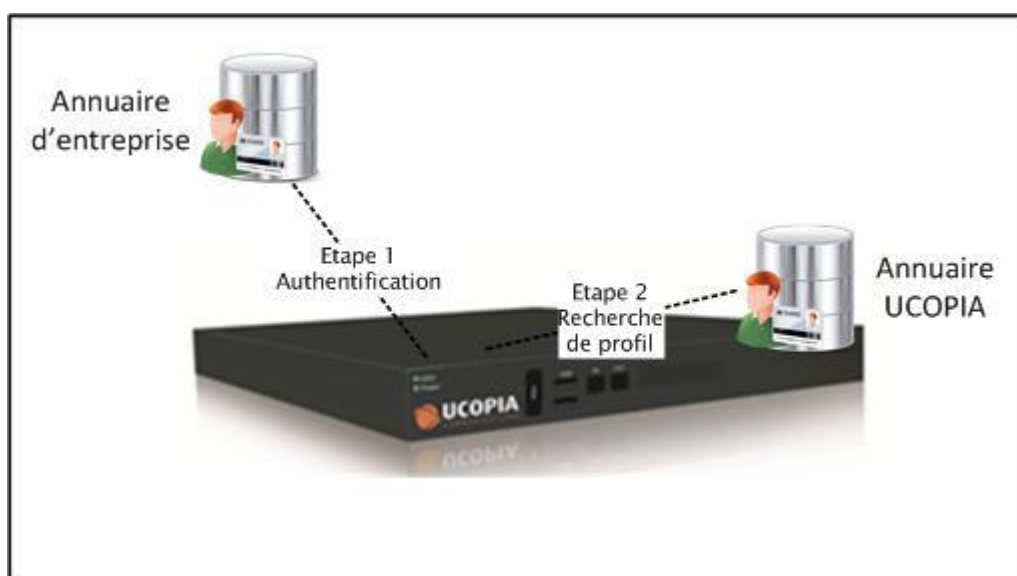


## 5 Intégration UCOPIA dans une infrastructure réseau

La solution UCOPIA inclut l'ensemble des modules nécessaires à son fonctionnement, ce qui lui permet d'être proposée dans un mode « clé en main » très simple de mise en œuvre, ce packaging convenant parfaitement aux petites entreprises ou aux agences déportées d'une grande entreprise, ayant peu de besoin et de moyen d'intégration<sup>4</sup>. A l'inverse, les grandes entreprises ont des infrastructures réseau complexes et souhaitent pouvoir réutiliser les solutions déjà déployées en termes de sécurité et/ou d'organisation réseau. UCOPIA, grâce à son architecture, ouverte et modulaire, peut s'intégrer en souplesse dans les architectures réseau existantes et inter-opérer avec les outils en place (annuaires LDAP, serveur RADIUS, Domaine Windows, PKI, outils tiers, ....)<sup>5</sup>.

### 5.1 Intégration avec un ou plusieurs annuaires d'entreprise

La solution UCOPIA permet de s'interfacer avec tout annuaire d'entreprise compatible LDAP V3. Dans le cas suivant, nous utiliserons deux annuaires, l'annuaire d'entreprise pour réaliser l'authentification des utilisateurs et l'annuaire UCOPIA pour appliquer le profil associé à l'utilisateur. Le fonctionnement lors du processus de connexion d'un utilisateur est alors schématisé par la figure ci-dessous.



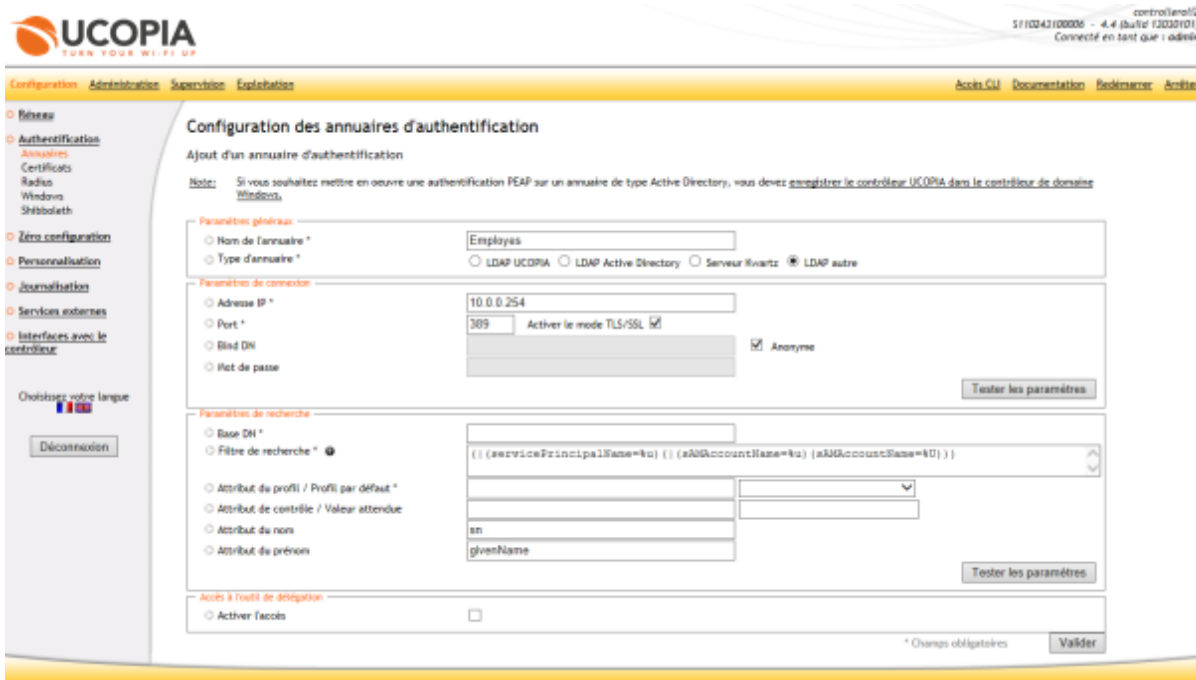
**Figure 32: Processus de connexion d'un utilisateur**

Pour mettre en place ce mécanisme, il faut pouvoir déduire le profil d'un utilisateur se trouvant dans l'annuaire UCOPIA à partir d'informations présentes dans l'annuaire d'entreprise.

La copie d'écran suivante montre comment configurer la connexion à un annuaire externe.

<sup>4</sup> Gamme UCOPIA Express

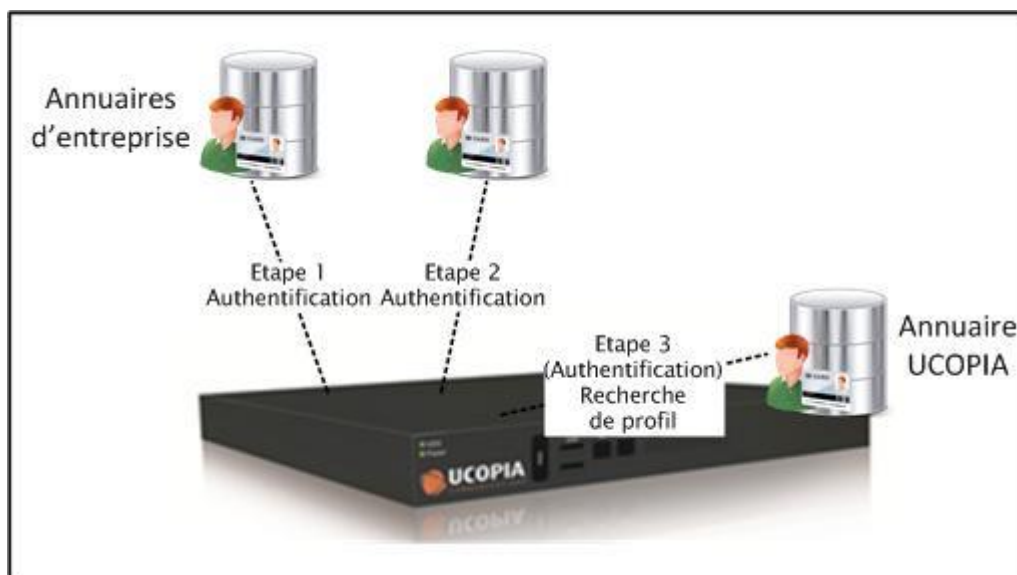
<sup>5</sup> Gamme UCOPIA Advance



**Figure 33: Configuration d'un annuaire externe d'authentification**

Un filtre LDAP de recherche permet d'identifier l'utilisateur, son profil UCOPIA sera déduit de l'attribut de groupe.

Le processus d'authentification UCOPIA fonctionne également avec plusieurs annuaires d'entreprise en cascade. La recherche d'un utilisateur lors d'une demande d'authentification peut se faire dans un premier annuaire puis si cette recherche échoue dans un second annuaire, etc. L'annuaire UCOPIA peut intervenir à la fois dans le processus d'authentification et dans la recherche de profils utilisateurs. L'ordre dans lequel les annuaires sont interrogés est configurable depuis l'outil d'administration UCOPIA.



**Figure 34: Authentification avec cascade d'annuaires**

La copie d'écran suivante présente une configuration avec trois annuaires (Employés, Partenaires, local (ucopia)), l'ordre de la cascade d'annuaires est spécifique à un mode d'authentification. En effet, il est possible de faire une distinction entre le mode d'authentification portail et le mode 802.1x/EAP, par exemple pour le mode portail les trois annuaires interviennent dans un ordre particulier, pour le mode

802.1x, seulement deux annuaires entrent en jeu (Employés et Partenaires) dans un ordre de cascade différent du mode portail.

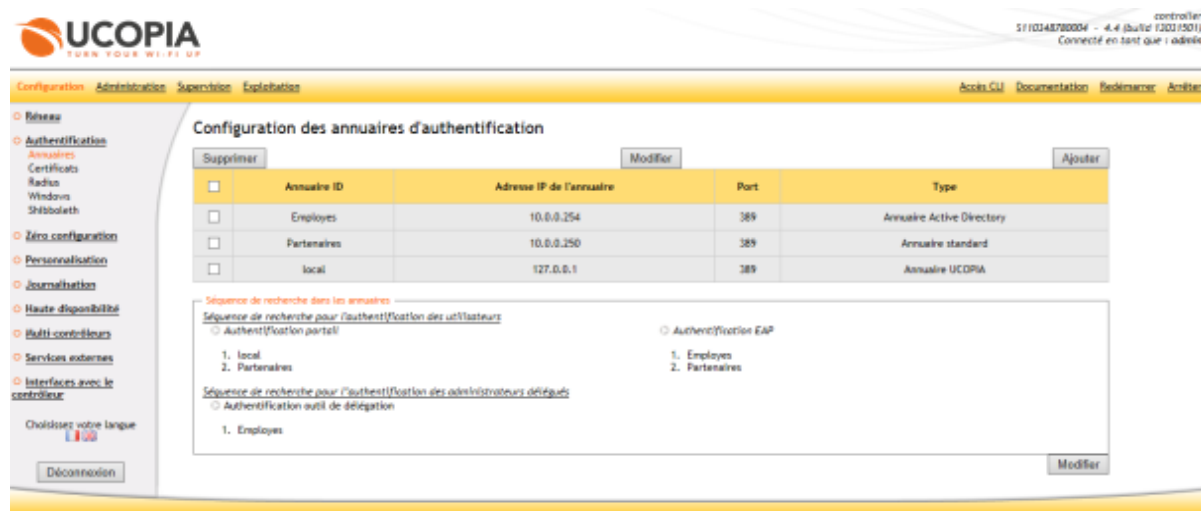


Figure 35: Configuration du contrôleur (annuaires d'authentification)

## 5.2 Adressage IP et architectures VLAN

La solution UCOPIA permet une gestion très fine du mécanisme d'adressage réseau des utilisateurs en fonction de leur profil et de la configuration du contrôleur UCOPIA.

Le contrôleur UCOPIA, se plaçant dans l'architecture réseau en coupure entre le réseau Wi-Fi et le LAN de l'entreprise, est muni de deux cartes Ethernet 802.1q, autorisant ainsi une architecture VLAN en entrée et en sortie du contrôleur.

UCOPIA embarque un serveur DHCP et fonctionne par défaut en mode NAT. Par défaut seul le VLAN natif est configurée en entrée d'UCOPIA, ce VLAN servant généralement à l'administration. Tous les utilisateurs sortent du contrôleur UCOPIA par la même interface native eth0.

La figure suivante montre le fonctionnement par défaut du contrôleur UCOPIA.

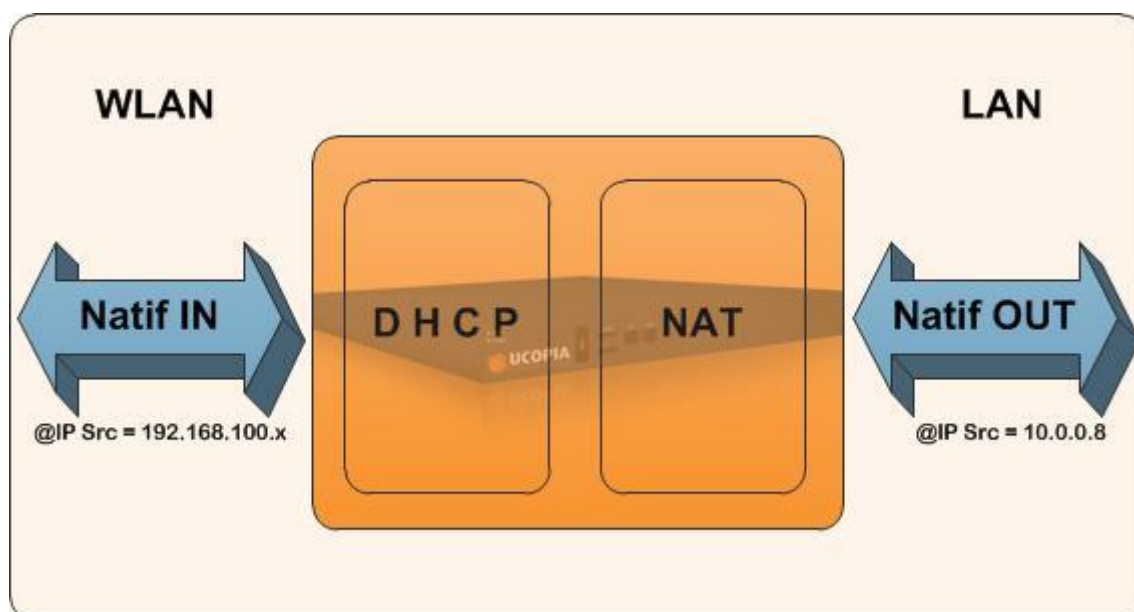
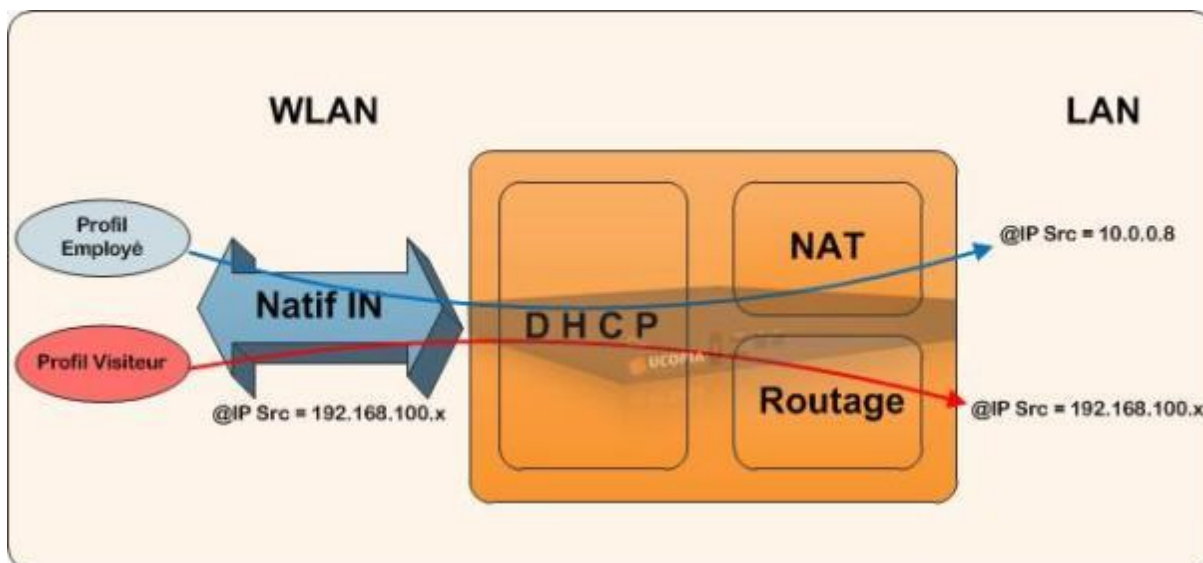


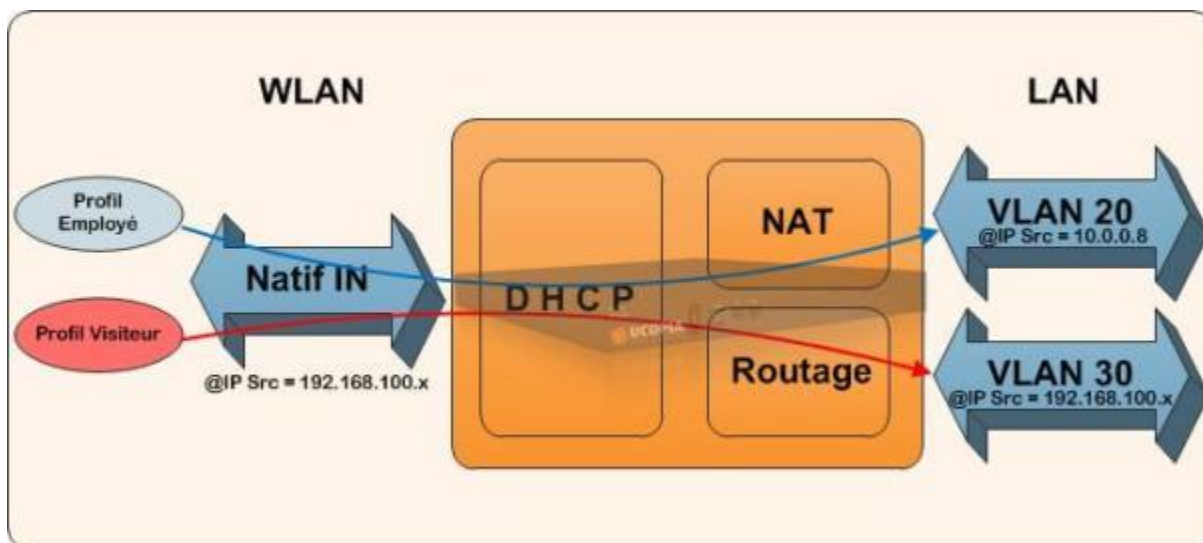
Figure 36: Configuration IP/VLAN par défaut du contrôleur UCOPIA

Le mode d'adressage peut être personnalisé en fonction du profil de l'utilisateur. Par exemple, un utilisateur ayant le profil Visiteur peut être naté alors qu'un Employé sera routé. Ces politiques d'adressage se définissent sur les VLANs de sortie du contrôleur UCOPIA. Le schéma ci-dessous illustre la mise en œuvre de deux politiques de sortie sur le VLAN natif de sortie.



**Figure 37: Politiques d'adressage en fonction du profil utilisateur**

Plusieurs VLANs de sortie peuvent être définis au niveau du contrôleur UCOPIA. En fonction du profil de l'utilisateur il sera alors possible de ré-aiguiller le flux de l'utilisateur dans un VLAN de sortie particulier, le schéma ci-dessous illustre ce type de configuration.



**Figure 38: Politiques d'adressage et VLANs de sortie**

Enfin, il est possible d'associer des zones (accueil, bureaux, bibliothèque) aux VLANs afin d'autoriser ou d'interdire la connexion de l'utilisateur sur ces zones qui sont définies au niveau du profil utilisateur (voir Section 6.3).

Ce mécanisme va également permettre de restreindre le nombre de VLANs par lesquels un utilisateur « entre » dans le contrôleur UCOPIA. Ceci peut être intéressant si l'on souhaite par exemple qu'un Employé utilise toujours le VLAN d'entrée associé à une authentification forte de type 802.1x et qu'il ne puisse pas utiliser le VLAN associé à une authentification de type portail moins sécurisée.

### 5.3 Intégration avec un proxy Web d'entreprise

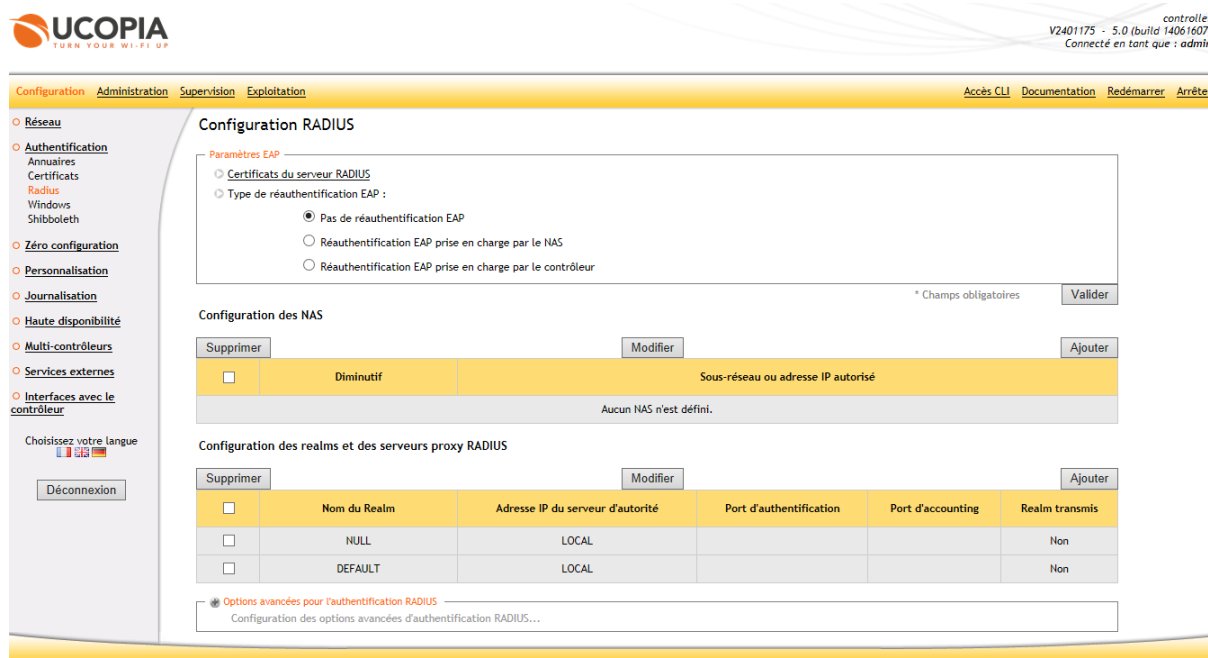
UCOPIA permet de rediriger le trafic HTTP vers un proxy d'entreprise grâce à son proxy Web embarqué. Les informations propres à l'utilisateur (*login* et mot de passe) peuvent être transmises au proxy parent, ceci lui permet d'appliquer des politiques différentes en fonction des utilisateurs.

### 5.4 Intégration avec un serveur RADIUS externe

Le contrôleur UCOPIA embarque un serveur RADIUS utilisé pour différents modes d'authentification UCOPIA basés sur 802.1x/EAP.

Le serveur RADIUS UCOPIA peut-être configuré afin de jouer le rôle de proxy vers un autre serveur d'authentification. Il sera donc possible d'utiliser le serveur RADIUS d'entreprise en place de celui d'UCOPIA pour des besoins d'authentification ou d'*accounting*.

La copie d'écran ci-dessous montre la configuration du mode proxy RADIUS depuis l'outil d'administration UCOPIA.



controleur  
V2401175 - 5.0 (build 14061607)  
Connecté en tant que : admin

Configuration Administration Supervision Exploitation Accès CLI Documentation Redémarrer Arrêter

**Configuration RADIUS**

Paramètres EAP

☐ Certificats du serveur RADIUS

☐ Type de réauthentification EAP :

☒ Pas de réauthentification EAP

☐ Réauthentification EAP prise en charge par le NAS

☐ Réauthentification EAP prise en charge par le contrôleur

\* Champs obligatoires Valider

Configuration des NAS

Supprimer Modifier Ajouter

	Diminutif	Sous-réseau ou adresse IP autorisé
<input type="checkbox"/>		Aucun NAS n'est défini.

Configuration des realms et des serveurs proxy RADIUS

Supprimer Modifier Ajouter

	Nom du Realm	Adresse IP du serveur d'autorité	Port d'authentification	Port d'accounting	Realm transmis
<input type="checkbox"/>	NULL	LOCAL			Non
<input type="checkbox"/>	DEFAULT	LOCAL			Non

Options avancées pour l'authentification RADIUS

Configuration des options avancées d'authentification RADIUS...

Figure 39: Configuration RADIUS

### 5.5 Intégration avec une architecture PKI

La solution UCOPIA s'intègre avec les architectures PKI existantes basées sur le protocole EAP-TLS pour réaliser l'authentification des utilisateurs.

Le certificat produit par l'autorité de certification est un certificat délivré au nom du contrôleur UCOPIA, celui-ci sera installé sur le contrôleur UCOPIA.

Le certificat pour l'utilisateur est installé au format pkcs12 dans le magasin de certificats personnel de l'utilisateur sur son poste de travail ou bien embarqué dans une carte à puce. Ces certificats devront contenir un champ "CN" spécifiant l'identifiant de l'utilisateur tel qu'il est défini dans l'annuaire d'entreprise, afin qu'UCOPIA puisse authentifier l'utilisateur.

De plus, les certificats générés par l'autorité de certification doivent contenir l'extension nécessaire au protocole EAP/TLS.

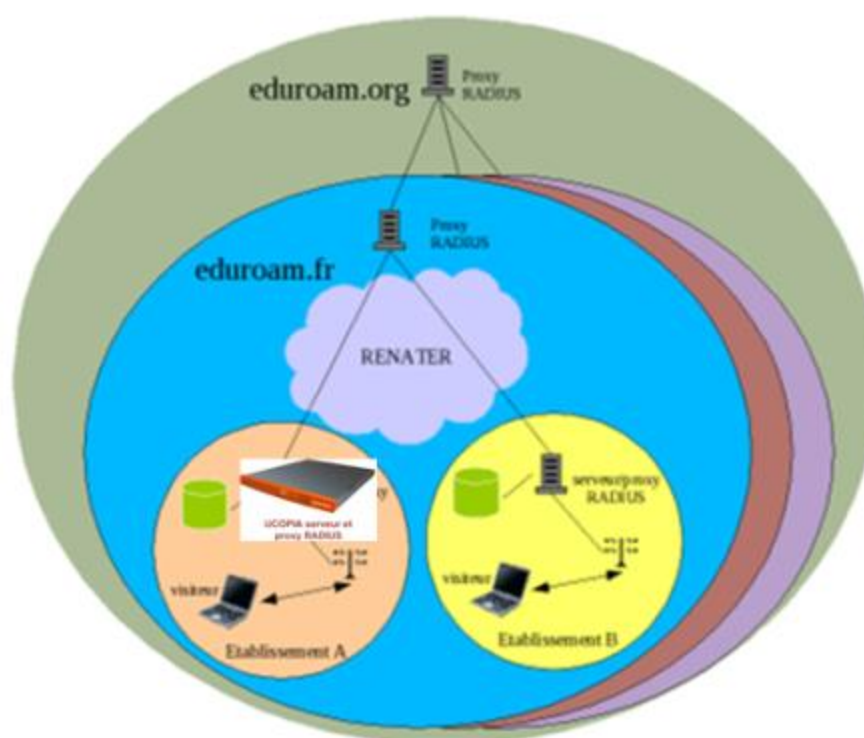
## 5.6 Intégration dans les architectures universitaires

### 5.6.1 Architecture EDUROAM

La capacité du serveur RADIUS UCOPIA à être configuré en mode proxy répond au besoin des architectures d'authentification EDUROAM rencontrées dans le monde universitaire.

EDUROAM est un projet Européen d'architecture d'authentification répartie, utilisant le protocole RADIUS, entre les établissements d'enseignement supérieurs et de recherche français. Cette authentification vise à offrir des accès réseau sans fil aux membres de la communauté concernée en déplacement sur les sites des partenaires avec leur nom et mot de passe habituels.

Les serveurs RADIUS des participants sont connectés à un proxy national, lui-même connecté au proxy international du projet EDUROAM. Les requêtes d'authentifications sont acheminées vers le serveur d'authentification de l'établissement d'appartenance de l'utilisateur par le biais du nom de domaine associé à son identifiant (de la forme [user@etab.fr](mailto:user@etab.fr)).



**Figure 40: Architecture EDUROAM avec UCOPIA**

UCOPIA est compatible avec l'architecture EDUROAM en apportant les fonctions suivantes

1. Proxy RADIUS
2. Analyse du domaine de l'utilisateur par le biais du nom de domaine (ou realm) associé à son identifiant (de la forme [user@etab.fr](mailto:user@etab.fr)). Ceci permet de réaliser l'aiguillage vers le site d'appartenance de l'utilisateur.
3. Authentification 802.1x/RADIUS ou par portail Web couplée à RADIUS. En effet, le mode RADIUS est classiquement le serveur d'authentification de l'architecture 802.1x. UCOPIA



associe la simplicité d'utilisation du mode portail Web avec le mode RADIUS et proxy RADIUS.

### 5.6.2 Architecture Shibboleth

Shibboleth est un mécanisme de propagation d'identités, développé par le consortium Internet2, qui regroupe un grand nombre d'universités et de centres de recherches. L'objectif de la propagation d'identités est double : déléguer l'authentification à l'établissement d'origine de l'utilisateur et obtenir certains attributs de l'utilisateur (pour gérer le contrôle d'accès ou personnaliser les contenus).

Dans l'architecture Shibboleth, UCOPIA joue le rôle de *Service Provider*. UCOPIA permet ainsi à travers son portail de rediriger l'utilisateur vers le service de découverte de la fédération (*Discovery Service*) à partir duquel il peut sélectionner son établissement d'origine. L'utilisateur sera ensuite redirigé vers son fournisseur d'identité pour authentification (*Identity Provider*).

UCOPIA fonctionne par défaut avec le *Discovery Service* de RENATER mais peut-être configuré pour utiliser un autre service.

Le schéma ci-dessous montre les interactions entre les différents composants de l'architecture Shibboleth.



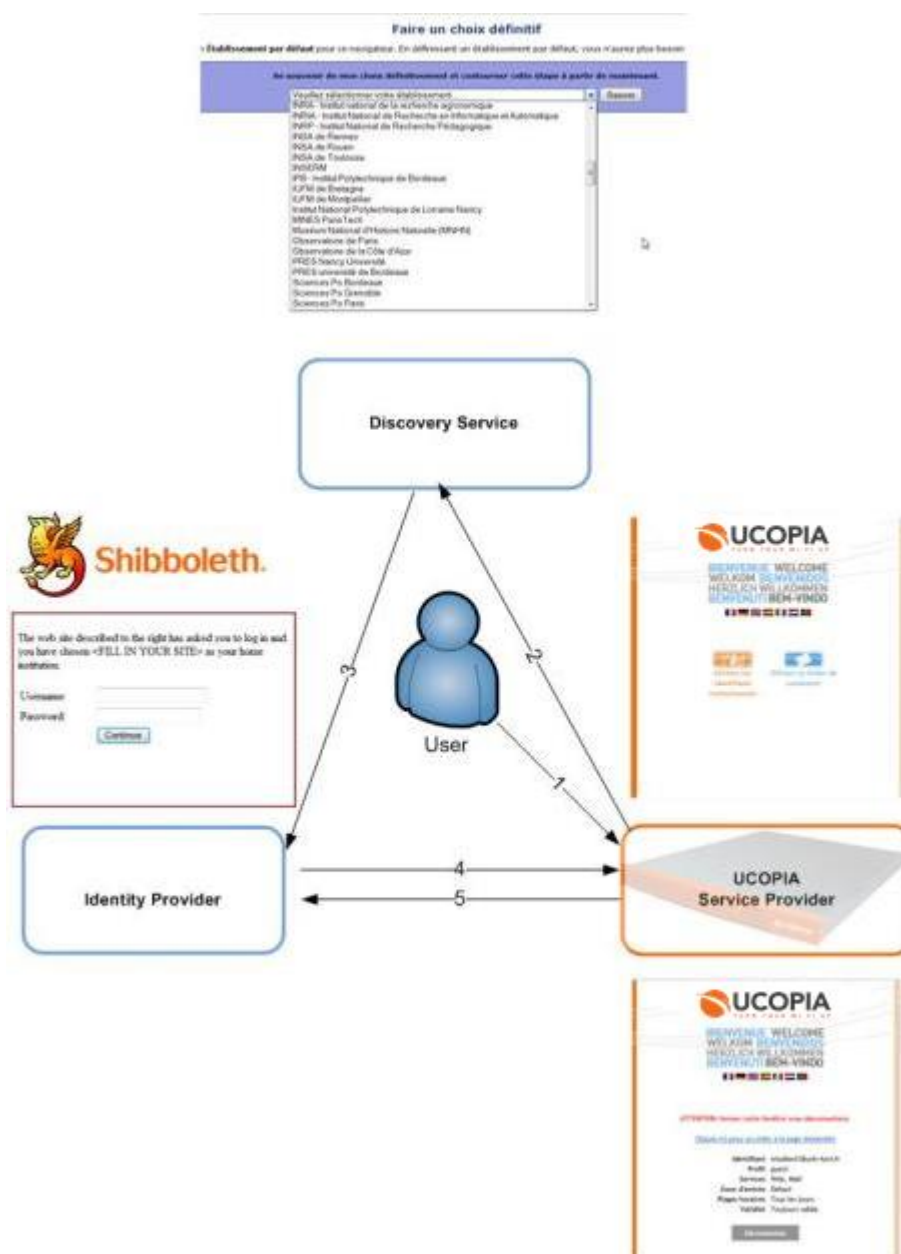


Figure 41 : Architecture Shibboleth avec UCOPIA

## 5.7 Couplage avec un produit tiers

### 5.7.1 API

UCOPIA propose une API générique permettant d'interfacer le contrôleur UCOPIA avec un produit tiers. Ce couplage peut s'avérer intéressant afin d'utiliser UCOPIA en conjonction d'un produit de provisionnement de comptes utilisateurs et/ou de facturation de services. Prenons le cas d'une clinique qui utilise un produit permettant lors de l'enregistrement d'un patient de lui délivrer des services tels que TV, téléphone, accès Internet, et ensuite de les facturer. Dans ce contexte, UCOPIA serait en charge du contrôle de l'accès Internet. Une fois le compte du patient créé dans l'outil tiers, ce même compte sera créé automatiquement dans UCOPIA via l'API afin d'autoriser l'accès Internet pour le patient. Le patient quittant la clinique, UCOPIA sera interrogé via son API pour connaître le temps cumulé de connexion Internet du patient et ainsi procéder à la facturation depuis l'outil tiers.

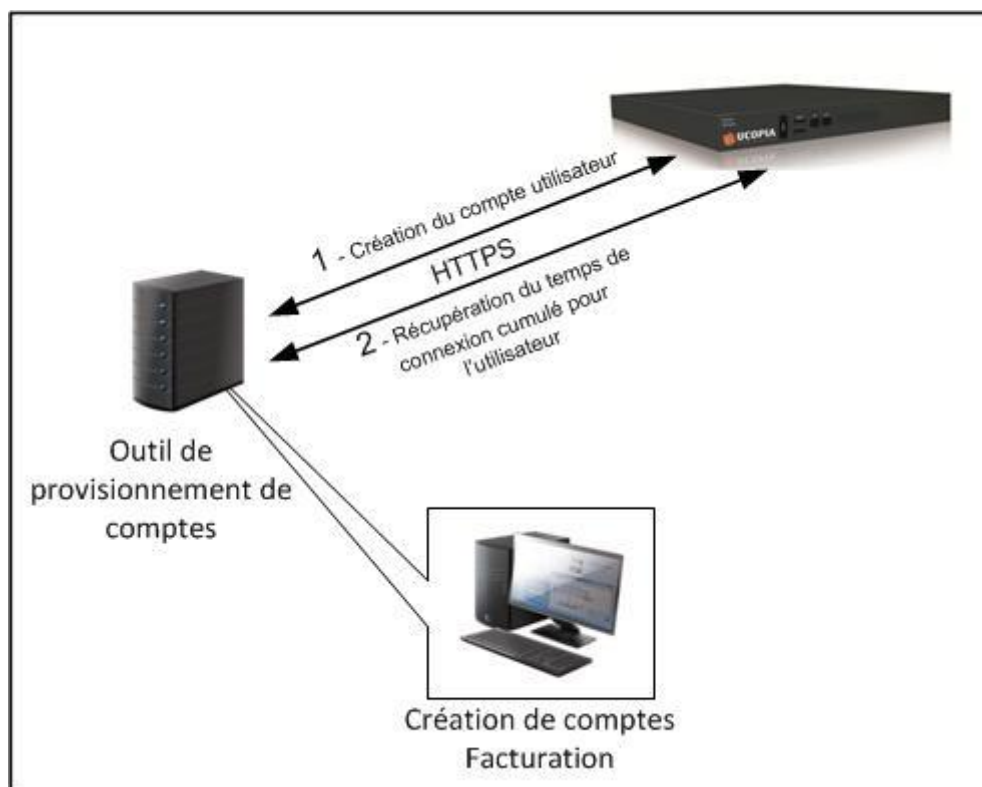
L'API se présente sous la forme de requête http dont la syntaxe est la suivante :

[http://<@IP du contrôleur UCOPIA>/deleg/api\\_admin\\_deleg.php](http://<@IP du contrôleur UCOPIA>/deleg/api_admin_deleg.php)

Par exemple pour créer un compte utilisateur dont le *login* est « jdupond » et le profil « guest »:

[http://10.0.0.1/deleg/api\\_admin\\_deleg.php?deleg\\_id=deleg&deleg\\_pwd=deleg&action=adduser&user\\_id=jdupond&user\\_pwd=dupond&user\\_grp=guest](http://10.0.0.1/deleg/api_admin_deleg.php?deleg_id=deleg&deleg_pwd=deleg&action=adduser&user_id=jdupond&user_pwd=dupond&user_grp=guest)

L'architecture de ce type de couplage est la suivante :



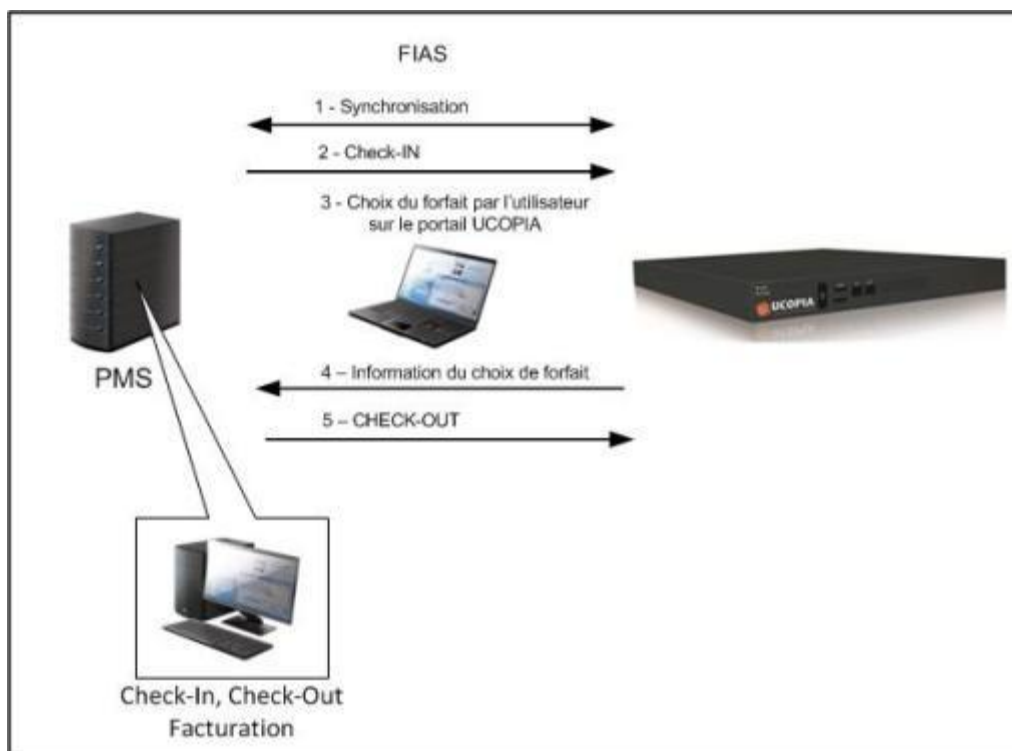
**Figure 42: Couplage avec un produit tiers**

### 5.7.2 Couplage avec un PMS (*Property Management System*)

Le contrôleur UCOPIA propose en plus de son API générique d'interfaçage, une interface dédiée avec des produits de type PMS. Les PMS sont des produits de gestion clients et se rencontrent plus particulièrement dans les environnements hôteliers ou hospitaliers, ils permettent l'enregistrement des clients, la facturation, etc.

Le couplage PMS/UCOPIA repose sur le protocole FIAS et fonctionne avec une notion de forfait. Le forfait est défini par l'administrateur UCOPIA, cela peut être un forfait 1h, 3h, ou forfait « emails », ou forfait « Tous les jours ouvrés de 16h à 18h », etc. Les forfaits sont proposés au choix de l'utilisateur sur le portail UCOPIA. UCOPIA informe le PMS des forfaits choisis afin qu'il puisse opérer la facturation.

L'architecture du couplage UCOPIA/PMS est la suivante :



**Figure 43: Couplage avec un PMS**

### 5.7.3 Couplage avec un PPS (*Pre Paid System*)

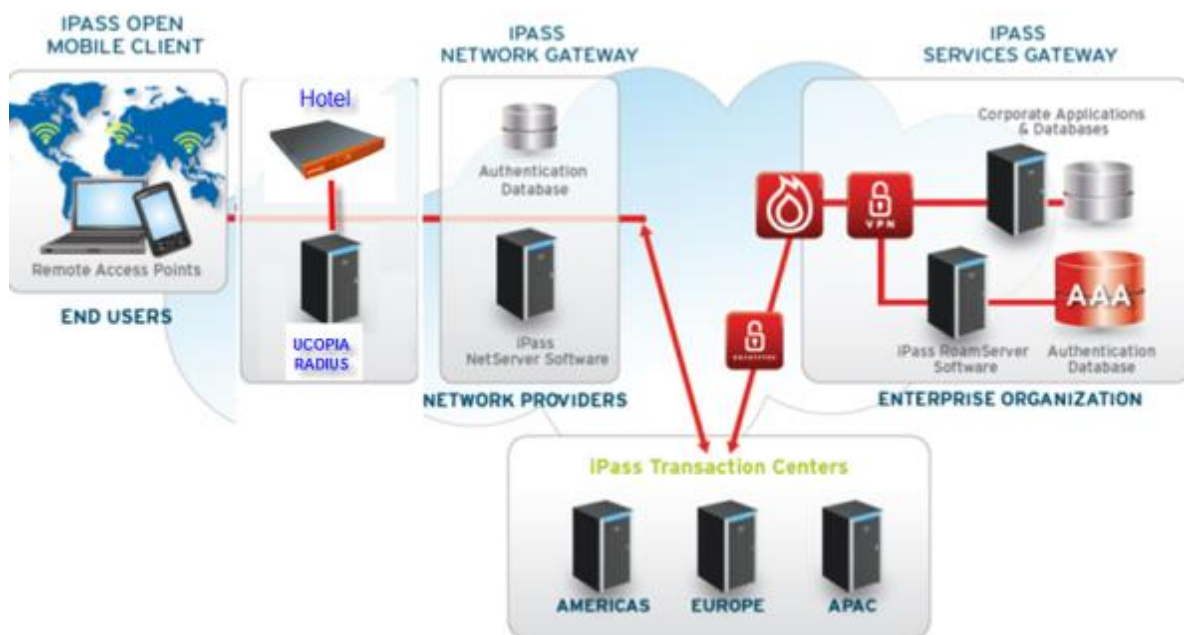
Le contrôleur UCOPIA propose une interface dédiée avec des produits de type PPS fonctionnant avec des cartes prépayées. L'utilisateur s'authentifie sur le portail UCOPIA en renseignant le numéro de carte et le CAPTCHA code. Le numéro de carte permet de faire une demande de crédit temps auprès du serveur PPS. Le PPS alloue du temps par tranche de N minutes renouvelable. Le compte de l'utilisateur est automatiquement créé dans UCOPIA. L'utilisateur visualise sur le portail le temps de connexion associé à la carte et le temps de connexion consommé.

### 5.7.4 Couplage avec la solution iPass

UCOPIA est compatible iPass et permet ainsi à tout utilisateur abonné de se connecter depuis un contrôleur UCOPIA. Pour cela, l'utilisateur iPass installe sur son matériel (PC, Smartphone, ...) une application iPass qui permet une connexion transparente. Cette application utilise un VPN pour assurer la communication avec l'entreprise de l'utilisateur.

UCOPIA est compatible iPass et permet ainsi à tout utilisateur abonné de se connecter depuis un contrôleur UCOPIA.

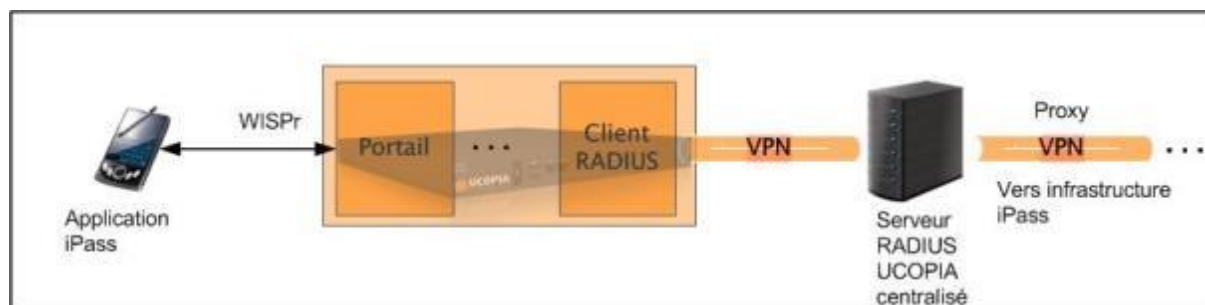
L'architecture UCOPIA/iPass est la suivante.



**Figure 44: Architecture globale iPass/UCOPIA**

Le contrôleur UCOPIA est en relation avec l'application iPass via le protocole WISPr. L'authentification est réalisée en RADIUS. Le RADIUS embarqué dans le contrôleur UCOPIA est le client d'un serveur RADIUS UCOPIA centralisé qui assure l'interaction avec l'infrastructure iPass (en mode proxy). L'ensemble des échanges RADIUS s'effectuent à travers un tunnel VPN.

Le schéma ci-dessous illustre cette architecture.



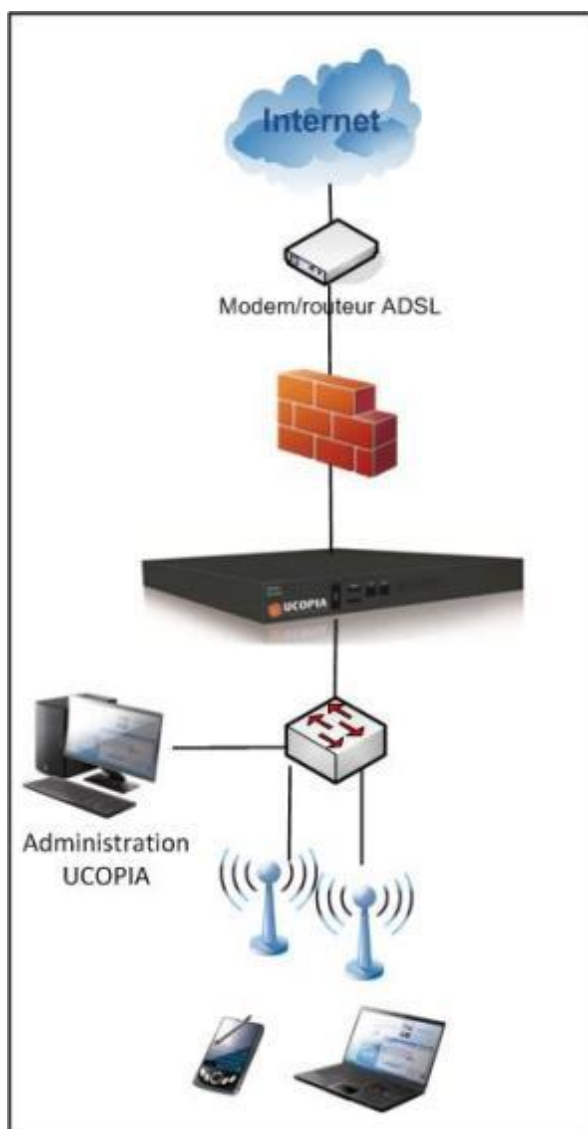
**Figure 45: Architecture iPass**

## 6 Architectures réseau

### 6.1 Architectures mono site

Les architectures mono site se rencontrent plus particulièrement dans les environnements hôteliers ou entreprises de type PME.

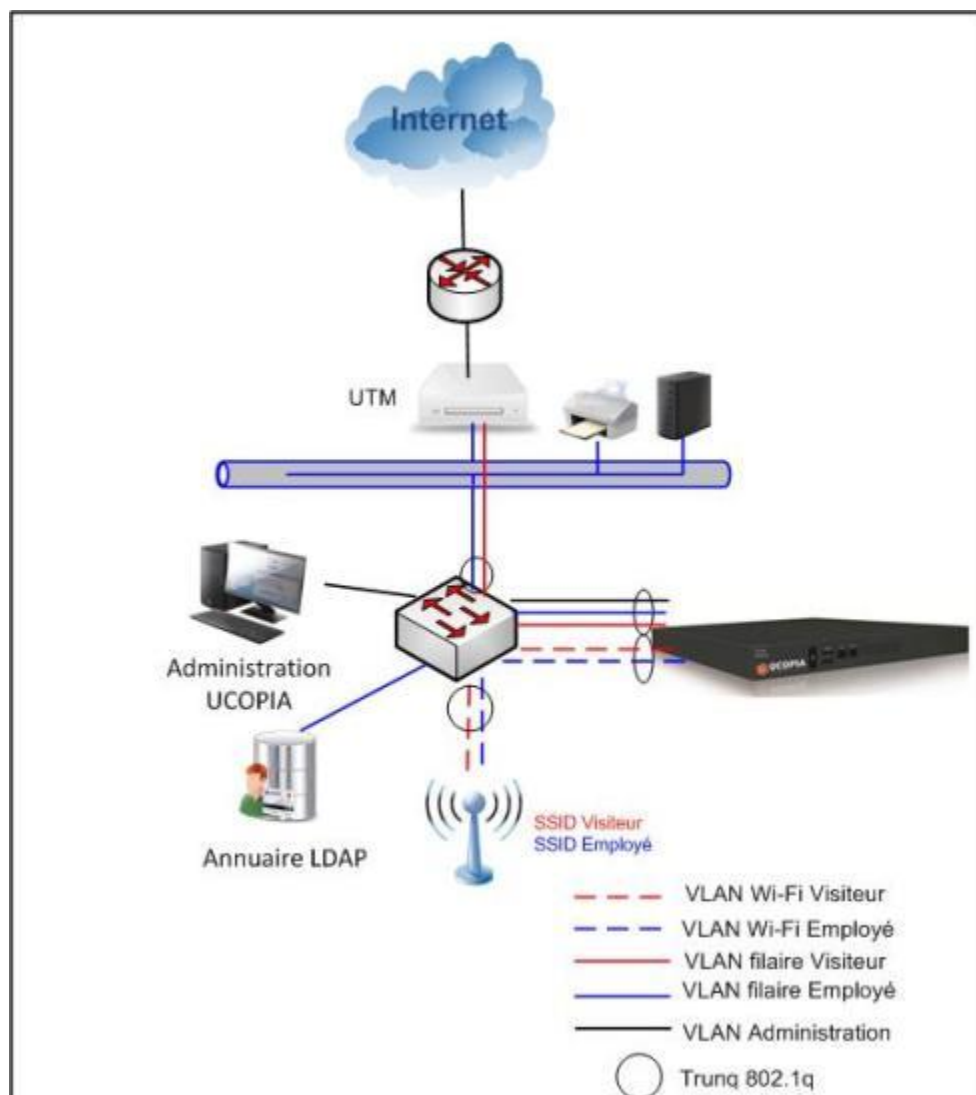
Dans le cas des hôtels, les architectures réseau sont généralement très « dépouillées », l'accès Internet est assuré par un modem/routeur ADSL, un pare-feu assure la sécurité périphérique. UCOPIA se positionne en coupure physique (pas d'organisation en VLANs) entre le réseau d'accueil des clients (Wi-Fi et/ou filaire) et le pare-feu comme l'indique le schéma ci-dessous.



**Figure 46: Architecture UCOPIA mono site (cas 1)**

Concernant les PME, les architectures sont plus élaborées, il n'est pas rare de rencontrer un annuaire dans lequel sont référencés les employés de l'entreprise, une organisation en VLAN et le besoin d'accueillir des visiteurs.

L'architecture UCOPIA type est dans ce cas la suivante :



**Figure 47: Architecture UCOPIA mono site (cas 2)**

Plusieurs couples SSID/VLAN sont définies sur les points d'accès Wi-Fi afin d'isoler les différentes populations d'utilisateurs (visiteurs, employés). Ces VLANs sont également configurés en entrée du contrôleur UCOPIA (carte Ethernet 802.1q). Lors du processus d'authentification d'un utilisateur, le contrôleur UCOPIA peut proposer en fonction de l'utilisateur des modes d'authentification distincts et adaptés, portail Web pour les visiteurs, protocole 802.1x pour les employés. Concernant l'authentification des employés, UCOPIA peut interroger l'annuaire d'entreprise (LDAP, Active Directory). Enfin en sortie du contrôleur UCOPIA, le flux d'un utilisateur peut être redirigé sur un VLAN particulier côté LAN (le choix du VLAN sera fait en fonction du profil de l'utilisateur).

## 6.2 Architectures multi sites

---

Les architectures multi sites se rencontrent le plus souvent dans les grandes organisations ou grandes entreprises (grands comptes, université, CROUS, CHU, etc.) ainsi que dans les réseaux d'agences ou de points de vente.

L'architecture UCOPIA en environnement multi sites peut être réalisée avec un ou plusieurs contrôleurs UCOPIA. Le ou les contrôleurs (s) peuvent être centralisé(s) sur un site ou bien distribués sur différents sites en fonction des contraintes des connexions réseau entre les sites. Le choix de ne pas positionner de contrôleur sur un site distant peut également dépendre du trafic associé à ce site. Les « petits » sites préféreront se référer à un contrôleur central, en revanche les sites plus importants préféreront un contrôleur local afin d'optimiser les performances.

### 6.2.1 Architecture centralisée

Dans une architecture centralisée multi sites, le contrôleur sera centralisé sur l'un des sites et assurera le service pour l'ensemble des sites distants.

Le flux utilisateur sera centralisé afin d'utiliser l'échappement Internet central. La centralisation du flux peut s'opérer de différentes façons. Soit en assurant un routage des flux entre le site distant et le site central, soit en établissent un tunnel (niveau 2 ou 3) entre le site distant et le site central, soit, dans le cas d'une architecture Wi-Fi de type « point d'accès léger », en utilisant les tunnels LWAPP ou CAPWAPP entre les bornes Wi-Fi se trouvant sur le site distant et le contrôleur de bornes sur le site central.

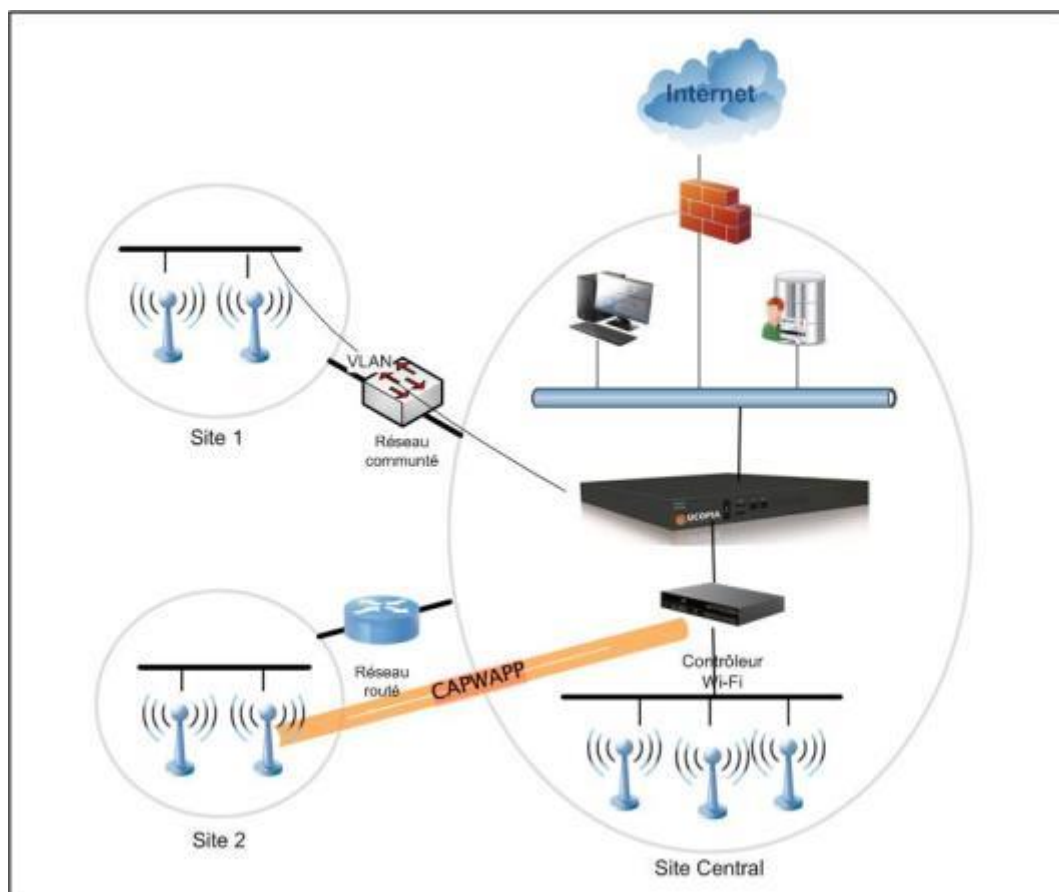
#### **Cas d'une architecture centralisée avec réseau routé (N3) entre les sites distants et le site central**

Si l'on souhaite dans une architecture routée conserver des fonctionnalités UCOPIA nécessitant l'adresse MAC telles que l'authentification automatique par adresse MAC ou l'authentification 802.1x, il faudra qu'un élément en amont d'UCOPIA puisse relayer les requêtes DHCP et bien entendu que le service DHCP soit rendu par le contrôleur UCOPIA.

Il persistera néanmoins pour cette architecture deux restrictions : (1) les postes clients sur le site distant doivent être configurés en DHCP, (2) la répartition de charge nécessite que les éléments de niveau 3 puissent être configurés pour répartir le trafic sur les différents contrôleurs du cluster (ex : source routing). Si ces restrictions ne sont pas souhaitées, il faut alors établir un tunnel de niveau 2 entre le site distant et le site central.

Il est à noter que le contrôleur UCOPIA central peut être configuré pour fonctionner à la fois en communication commutée et routée.





**Figure 48: Architecture multi sites centralisée**

### 6.2.2 Architecture partiellement centralisée

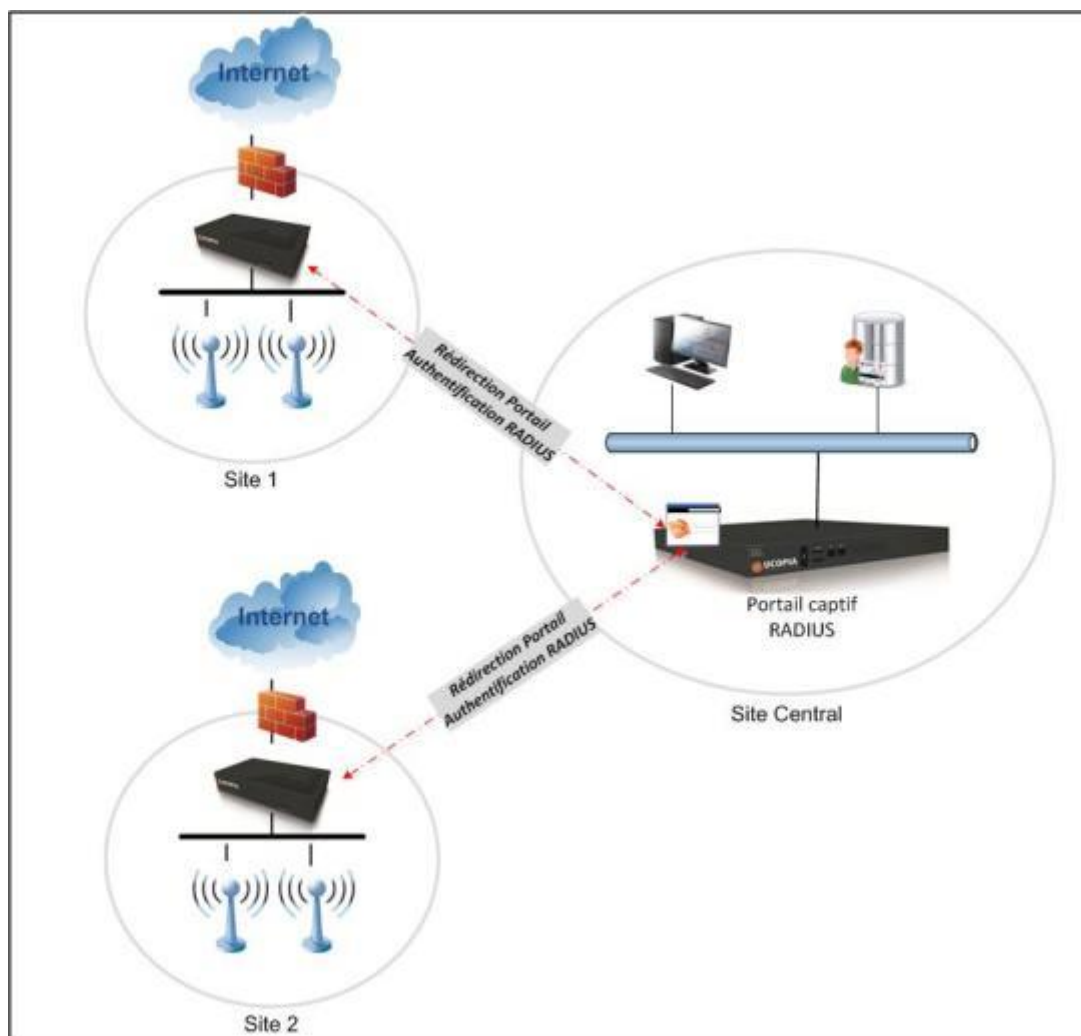
Il est possible de ne centraliser que certains services, en l'occurrence les services de portail et d'authentification. Un contrôleur UCOPIA sera donc présent sur chaque site en charge du contrôle du trafic utilisateur et un contrôleur en central assurera les services de portail et d'authentification.

Dans cette architecture, les flux utilisateurs sont donc gérés localement sur chaque site et l'échappement Internet local à chaque site est utilisé.

Le contrôleur UCOPIA local réalise une redirection de portail vers l'UCOPIA central, l'authentification s'effectue en RADIUS. La base des utilisateurs se trouve sur le contrôleur central.

L'avantage de cette architecture est de pouvoir partager le portail d'authentification et la base des utilisateurs entre tous les sites. Cela simplifie notamment l'administration en cas de mise à jour du portail.

Il est à noter que cette architecture peut fonctionner avec uniquement une infrastructure Wi-Fi sur le site distant (c'est-à-dire sans contrôleur UCOPIA). Il faut néanmoins que la solution Wi-Fi soit compatible avec les protocoles de redirection portail et RADIUS.



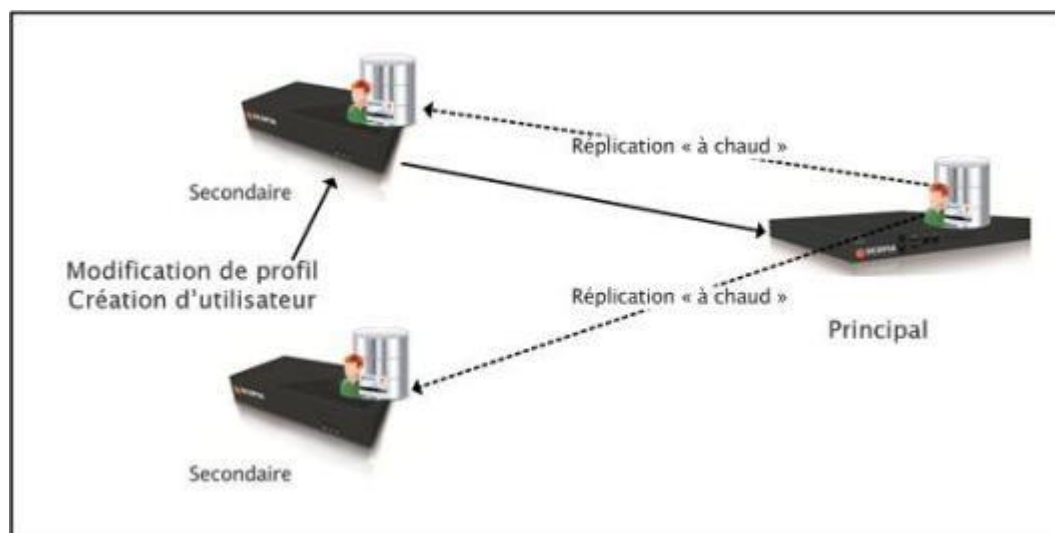
**Figure 49: Architecture multi sites partiellement centralisée**

### 6.2.3 Architecture distribuée

Dans une architecture distribuée, un contrôleur est présent sur chaque site.

Pour assurer une cohérence de l'annuaire UCOPIA à travers les différents sites, il est possible de mettre en œuvre un mécanisme de synchronisation de cet annuaire. Il faut alors définir un contrôleur dit Principal qui aura la charge de cette synchronisation. En conséquence, toute opération effectuée sur un des annuaires UCOPIA du pool de contrôleur s'effectuera en réalité sur le contrôleur Principal qui réplique « à chaud » la modification sur tous les contrôleurs Secondaires. En revanche, l'interrogation d'un annuaire UCOPIA et donc l'authentification des utilisateurs est toujours réalisée en local sur le contrôleur. Ce mécanisme garantit une parfaite homogénéité en termes d'administration des utilisateurs et des profils utilisateur.

Le schéma ci-dessous illustre le mécanisme de réplcation d'annuaire.



**Figure 50: Réplication d'annuaire UCOPIA en architecture distribuée**

Le contrôleur principal doit être absolument de la gamme Advance, en revanche les contrôleurs secondaires peuvent être indifféremment de la gamme Express ou Advance.

#### 6.2.4 Architecture mixte

En multi sites, les architectures précédentes peuvent être combinées et ainsi avoir des sites distants qui se réfèrent à un UCOPIA central alors que d'autres auront leur propre contrôleur local.

### 6.3 Architecture multi zones

UCOPIA propose une notion de zone permettant de décrire un lieu, par exemple dans une entreprise, une zone d'accueil ou de bureaux, dans une université, la bibliothèque ou les amphithéâtres.

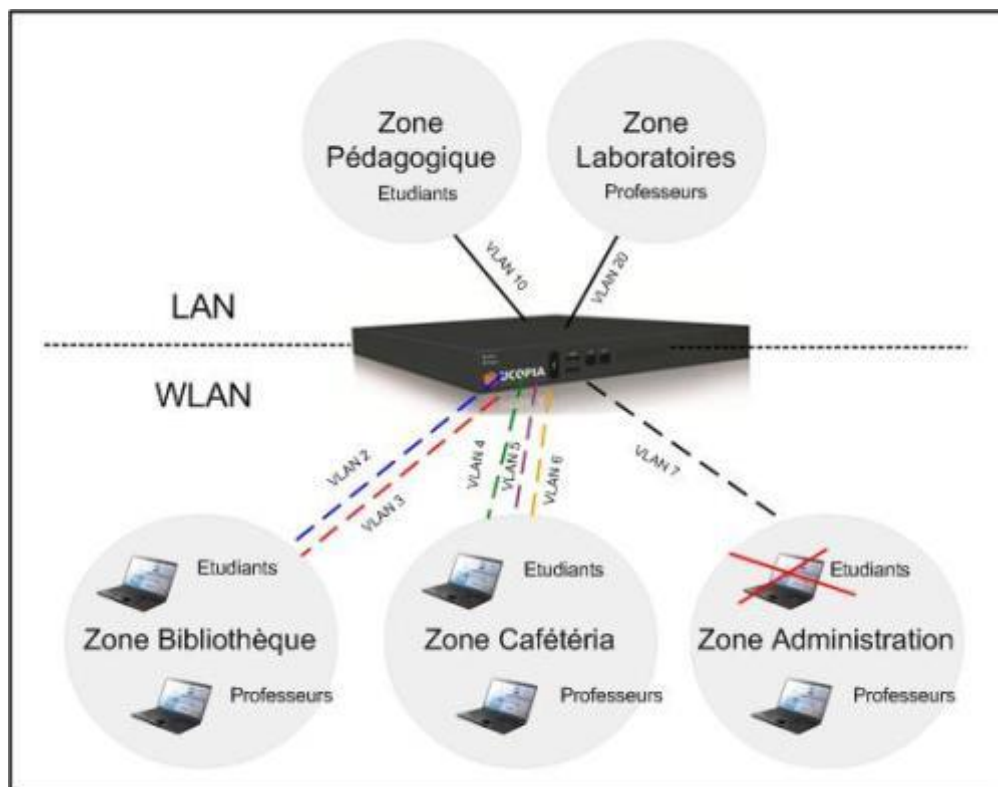
Les zones peuvent être utilisées à des fins de sécurité et/ou de mobilité. Pour renforcer la sécurité, il est possible de spécifier qu'une population d'utilisateurs est autorisée ou interdite à se connecter sur une zone. Par exemple, les visiteurs d'une entreprise ne se connectent pas dans la zone Bureaux mais uniquement dans la zone Accueil. Pour un usage des zones lié à la mobilité, il est possible de proposer un portail captif différent pour chaque zone. Il est également possible de faire varier les prérogatives de l'utilisateur suivant sa zone de connexion. Par exemple, un employé d'une entreprise pourra se connecter dans toutes les zones sans restriction de temps, accepté dans la zone Accueil, où il verra son temps de connexion limité.

Il existe des zones d'entrée et des zones de sortie, l'entrée et la sortie sont relatives au contrôleur UCOPIA et à son architecture en coupure.

D'un point de vue réseau, les zones d'entrée correspondent à des sous-réseaux. Dans une architecture réseau local (niveau 2) les zones correspondront à des VLANs, dans une architecture réseau distant (niveau 3) les zones seront des sous-réseaux. Les zones en sortie correspondront dans tous les cas à des VLANs. La correspondance zone d'entrée/sous-réseaux s'effectue lors de la configuration des réseaux d'entrée au niveau du contrôleur UCOPIA. En sortie, les zones sont associées à un profil utilisateur.

Dans l'exemple ci-dessous, un profil Etudiant sera configuré pour autoriser la connexion sur les zones d'entrées "Bibliothèque" et "Cafétéria". La zone « Administration » sera interdite à la connexion et donc ne sera pas configurée dans le profil. Sur le site ci-dessous, Bibliothèque = vlan 2 + vlan3. Sur au autre site la zone Bibliothèque pourrait être implémentée avec d'autres VLANs.

La zone de sortie est unique, elle correspond d'une part à un VLAN et d'autre part à une politique d'adressage en sortie du contrôleur UCOPIA (NAT ou routage).



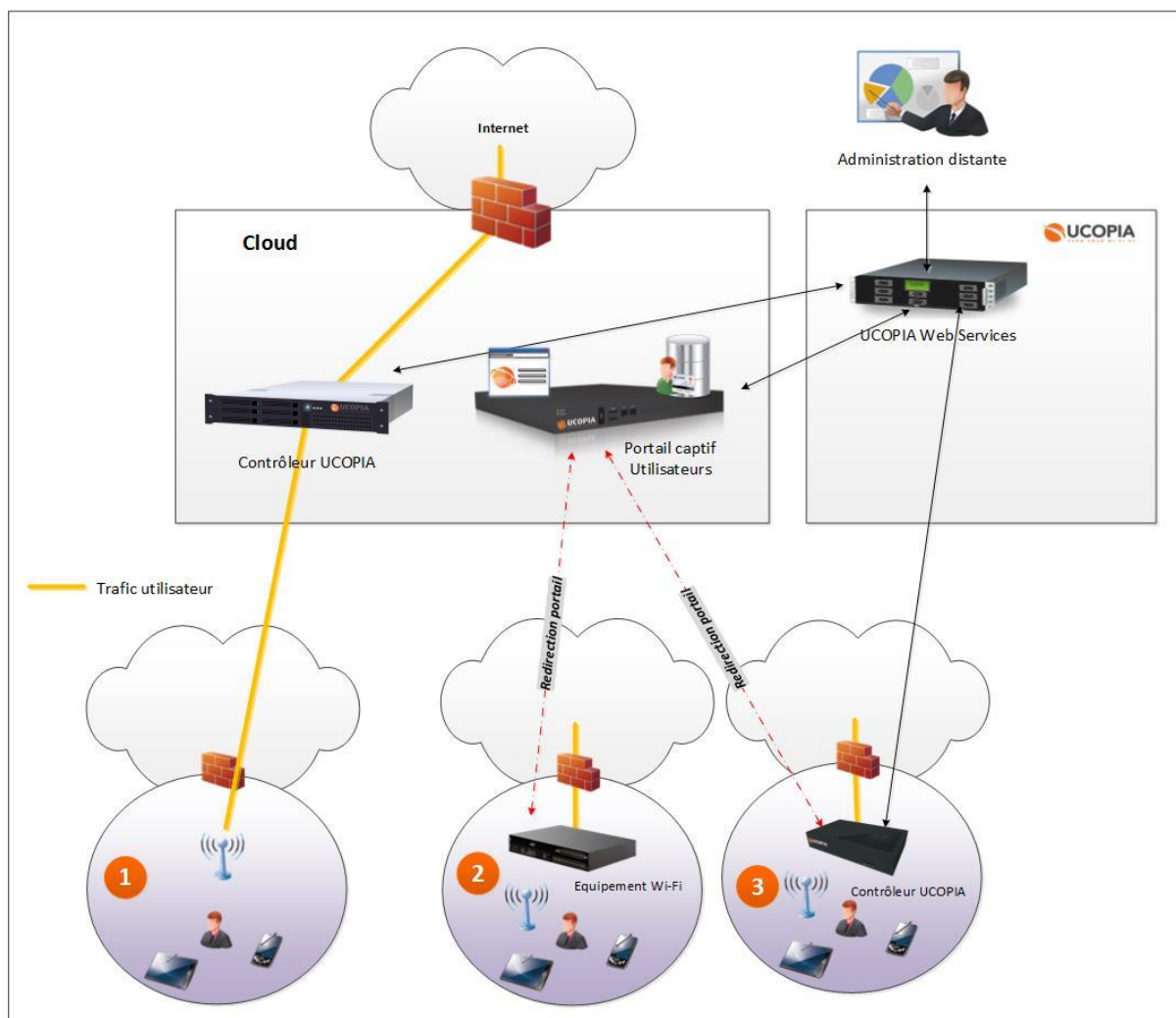
**Figure 51: Architecture multi zones**

Dans une architecture multi sites dont l'administration est centralisée, la notion de zone est globale et s'applique à tous les contrôleurs UCOPIA pouvant être réparties sur les sites. En revanche, la façon dont s'implémentent ces zones est propre à chaque contrôleur. La correspondance zone/VLANs s'effectue lors de la configuration de chaque contrôleur. Toutes les zones ne sont pas systématiquement implémentées sur chaque contrôleur.

## 6.4 Architecture Cloud

UCOPIA propose différentes architectures, centralisées, distribuées ou mixtes (voir Sections précédentes) permettant de déployer des architectures Cloud très flexibles.

Le schéma suivant résume les différentes possibilités d'architectures dans le Cloud.



**Figure 52: Architecture Cloud**

■ Cas N°1 :

Le trafic utilisateur est centralisé dans le Cloud, l'échappement Internet s'effectue au niveau du Cloud. L'ensemble des fonctions UCOPIA est assuré par un (ou plusieurs) contrôleurs UCOPIA du Cloud.

Cette architecture répond aux besoins des opérateurs, des WISP ou des grandes chaînes de magasins.

■ Cas N°2 :

Le portail captif, l'authentification et l'annuaire des utilisateurs sont centralisés dans le Cloud. Cette architecture déporte certaines fonctions du contrôleur UCOPIA dans le Cloud permettant ainsi une administration centralisée de ces fonctions. Un équipement Wi-Fi assure la redirection vers le portail UCOPIA centralisé et l'authentification (échange RADIUS avec le serveur RADIUS UCOPIA en central). Cette architecture présente l'avantage de ne pas nécessiter l'ajout de composants sur le site local en dehors de l'équipement Wi-Fi. En revanche, en termes de traçabilité, seuls les journaux de sessions utilisateur sont disponibles au niveau du Cloud. Cette architecture répond aux besoins des WISP, opérateurs pour le bas/milieu de marché. Ou pour de nombreux petits points de ventes d'une chaîne de magasins.

- Cas N°3:

Il s'agit d'une architecture comparable à l'architecture 2, mais avec un contrôleur UCOPIA sur site local. De part la présence d'un contrôleur UCOPIA sur site, cette architecture permet de fournir l'ensemble des fonctions UCOPIA telles que traçabilité du trafic utilisateur ou filtrage d'URLs.

## 7 Haute disponibilité UCOPIA<sup>6</sup>

---

Une architecture de redondance peut être mise en place afin de ne pas interrompre le service du contrôleur UCOPIA en cas de défaillance de la machine sur laquelle le contrôleur fonctionne. Pour ce faire, il faudra déployer deux contrôleurs ayant la capacité à se suppléer l'un l'autre.

UCOPIA propose également un mécanisme de répartition de charge qui peut permettre à plusieurs contrôleurs UCOPIA de se répartir les connexions des utilisateurs. Redondance et répartition de charge sont deux mécanismes indépendants et complémentaires.

### 7.1 Redondance

---

Le modèle de redondance UCOPIA est un modèle Actif/Passif mettant en œuvre deux contrôleurs UCOPIA, un seul étant actif à un instant donné. Les contrôleurs UCOPIA intervenant dans une architecture de redondance dialoguent entre eux et peuvent par conséquent s'apercevoir de la défaillance de leur confrère.

Le basculement d'un contrôleur UCOPIA à l'autre s'effectue grâce à une adresse IP virtuelle. En effet, à un instant donné, seul un contrôleur dispose de l'adresse virtuelle. En cas de panne du contrôleur actif, le contrôleur de redondance prend connaissance de la panne grâce au protocole VRRP et récupère l'adresse IP virtuelle. Il devient ainsi le nouveau contrôleur actif tout en assurant une totale transparence pour les utilisateurs.

Les contrôleurs UCOPIA dans une architecture de redondance (ou de répartition de charge) obéissent à l'architecture multi contrôleurs UCOPIA, par conséquent nous aurons un contrôleur « Principal » correspondant au contrôleur Actif sur lequel l'administration s'effectuera et nous aurons un contrôleur « Secondaire » correspondant au contrôleur Passif. L'annuaire UCOPIA du contrôleur Actif sera répliqué « à chaud » sur l'annuaire du contrôleur Passif. Ce mécanisme permettra au contrôleur Passif d'être à jour quand il sera sollicité pour passer en mode Actif.

Dans une architecture de redondance, les contrôleurs UCOPIA doivent se trouver sur réseau de niveau 2.

Le schéma ci-dessous illustre l'architecture de redondance.

---

<sup>6</sup> Gamme Advance uniquement



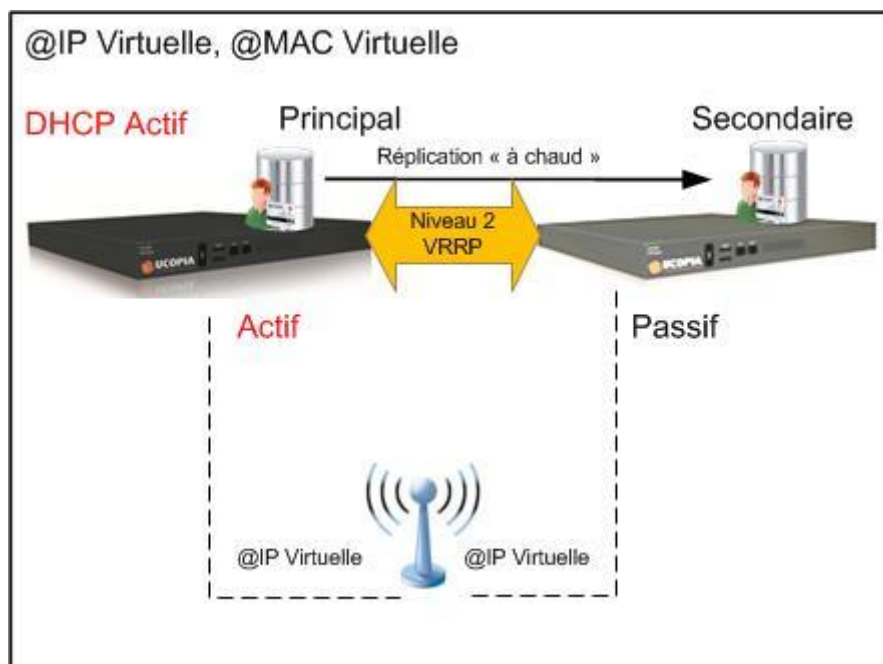


Figure 53: Architecture de redondance UCOPIA

## 7.2 Répartition de charge

La répartition de charge permet de répartir de façon uniforme les connexions des utilisateurs sur les différents contrôleurs. Sur chacun des contrôleurs la charge montera jusqu'à atteindre la limite fixée par les licences des contrôleurs.

Comme la reprise sur panne, la répartition de charge est basée sur un dialogue VRRP entre les contrôleurs UCOPIA et sur le principe d'IP virtuelle. Seul le serveur DHCP du contrôleur Principal est activé.

Les contrôleurs organisés en répartition de charge utilisent le mécanisme de réplication « à chaud » de l'annuaire UCOPIA pour maintenir tous les annuaires à jour en temps réel.

Le schéma ci-dessous illustre un exemple dans lequel trois contrôleurs UCOPIA sont configurés en répartition de charge, un contrôleur passif assure la redondance en cas de panne de l'un des trois contrôleurs actifs.

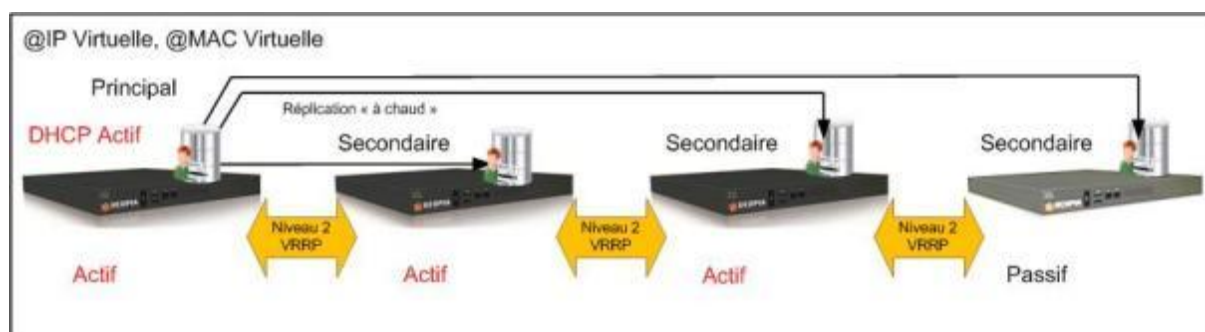


Figure 54: Architecture de répartition de charge UCOPIA

## 8 Plate-forme UCOPIA Web Services

---

La plate-forme UCOPIA Web Services (UWS), hébergée par UCOPIA, est dédiée aux clients et partenaires UCOPIA et propose des fonctions d'exploitation, de supervision et d'administration des contrôleurs UCOPIA, ainsi que des services d'analytique et de marketing.

Pour pouvoir bénéficier de ces services, il faudra que les contrôleurs soient configurés de façon à autoriser le dialogue avec la plate-forme UWS (voir Section Architecture).

### 8.1 Exploitation

---

La plate-forme UWS est en mesure d'apporter les services suivants en termes d'exploitation du contrôleur UCOPIA

#### 8.1.1 Installation automatique de la licence UCOPIA (ou mise à jour)

Avant toute opération, une licence doit être installée sur le contrôleur UCOPIA.

La licence UCOPIA détermine la gamme de contrôleur (Express, Advance) ainsi que le nombre maximum de connexions simultanées (Express 20, Advance 1000, etc.).

La licence une fois attribuée à un contrôleur peut être répartie par l'administrateur en fonction des zones et des profils utilisateur. La répartition par zone peut s'avérer utile pour associer une licence à un lieu ou à un site dans une architecture multi sites. La répartition par profil permet de réserver un nombre de licences pour un type d'utilisateurs donné.

Une fois connecté au réseau, le contrôleur interroge à la demande de l'administrateur la plate-forme centrale. Celle-ci extrait les caractéristiques de la machine (numéro de série, etc.) et vérifie dans son système d'information la validité de la demande. Cette étape de validation effectuée, la licence est générée et installée automatiquement sur le contrôleur UCOPIA.

#### 8.1.2 Mise à disposition automatique des mises à jour

UCOPIA met régulièrement à disposition des mises à jour correctives et évolutives dont l'objectif est d'apporter correctifs, améliorations et nouvelles fonctionnalités.

Grâce à la plate-forme UWS, les mises à jour sont périodiquement téléchargées sur le contrôleur, elles sont prêtes à l'installation. L'administrateur est informé et peut décider de leur installation.

La plate-forme propose également le service d'installation automatique pour les mises à jour correctives.

#### 8.1.3 Ouverture automatique d'un tunnel de maintenance

Le tunnel de maintenance permet au partenaire ou au support technique UCOPIA d'intervenir en télémaintenance sur le contrôleur UCOPIA pour effectuer des analyses et diagnostics. En cas de nécessité, le tunnel sera activé automatiquement sans intervention de l'administrateur. Il est noté que le tunnel de maintenance est établi du contrôleur UCOPIA vers les serveurs de maintenance.

### 8.1.4 Contrôle de la validité de la maintenance

Une alerte prévient l'administrateur quand la validité de la maintenance expire. Par ailleurs, le téléchargement des mises à jour devient impossible une fois la maintenance expirée.

## 8.2 Supervision et administration

La plate-forme UWS fournit des services additionnels dont les partenaires UCOPIA peuvent bénéficier. L'objectif étant qu'ils puissent superviser et administrer l'ensemble des contrôleurs UCOPIA de leur propre parc.

Une des premières fonctions de UWS est de pouvoir réorganiser un parc en fonction de différents critères : par client final, par type de produit, par région, etc. Le parc pourra donc être structuré en sous-ensembles de contrôleurs UCOPIA permettant ainsi une gestion optimale du parc.

Les autres fonctions proposées vont permettre de superviser et d'administrer les contrôleurs UCOPIA soit de façon globale soit individuellement.

Les copies d'écran ci-dessous illustrent quelques fonctions de supervision.

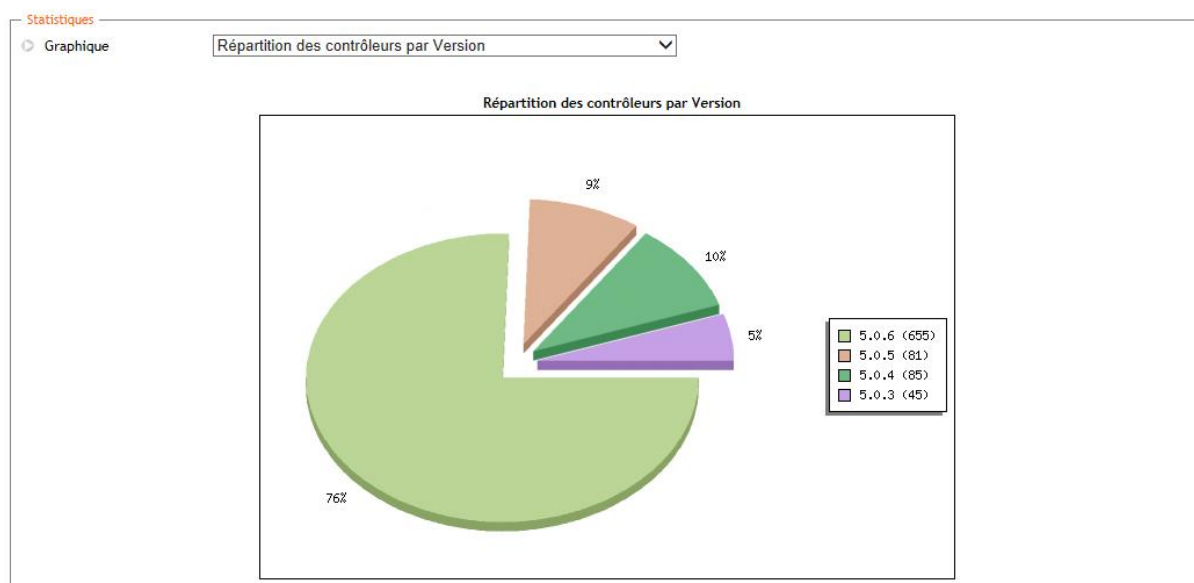
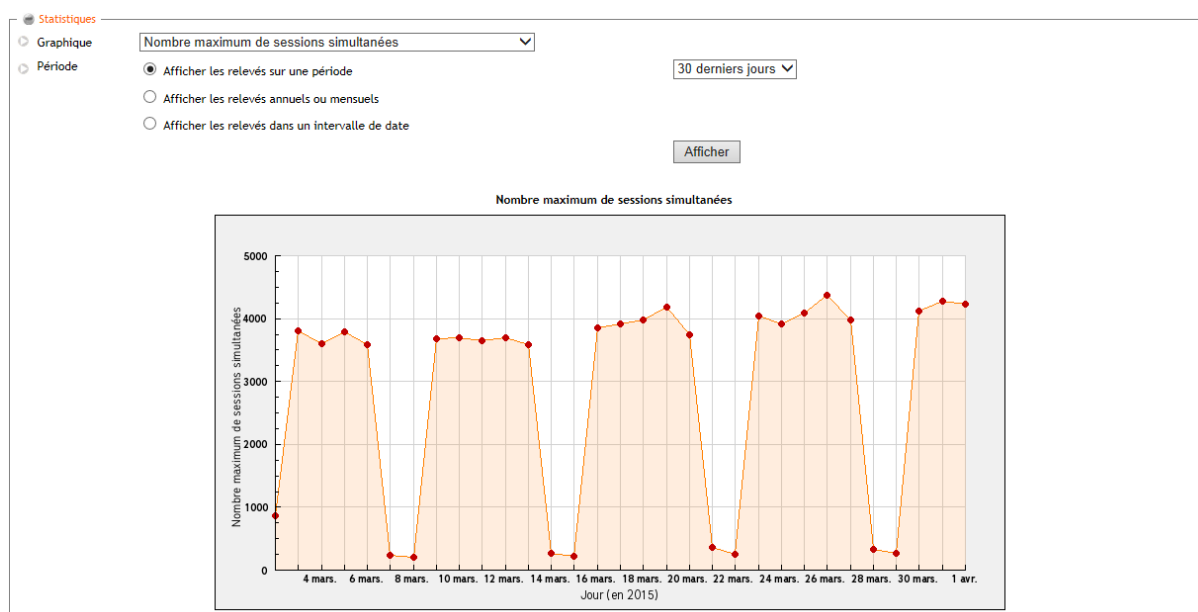


Figure 55: Statistiques globales en fonction des numéros de version



**Figure 56: Nombre de connexions simultanées sur un contrôleur**

Par ailleurs, le partenaire peut avoir accès par un simple clic aux outils d'administration pour vérifier ou modifier une configuration. Il peut également contrôler le niveau de mise à jour des contrôleurs, télécharger des mises à jour et les appliquer sur les contrôleurs.

Des alertes peuvent être déclenchées sur certains types d'événement (contrat de maintenance expiré, disque arrivant à saturation, contrôleur dont la température est anormalement élevée, etc.). Ces alertes peuvent être envoyées par email à l'administrateur.

### 8.3 Business intelligence et analytique

Le contrôleur UCOPIA enregistre et conserve tout un ensemble de données d'usage du service (le nombre de connexions simultanées, le nombre et la durée des sessions, etc.) mais aussi des informations concernant les utilisateurs de la solution (qui sont-ils ? avec quels types d'équipement se connectent-ils ? que font-ils ?). Le portail captif ainsi que les connecteurs aux réseaux sociaux contribuent à enrichir la connaissance des utilisateurs.

Le service «Wi-Fi Analytics» disponible sur UWS va permettre au propriétaire de la solution UCOPIA d'explorer toutes ses données pour bénéficier d'une vue d'ensemble. Il est ainsi possible de saisir n'importe quel mot ou expression, dans n'importe quel ordre, dans la zone de recherche du service d'analytique pour obtenir des résultats à la fois instantanés et associatifs, permettant de visualiser de nouvelles connexions et relations entre les données.

Le service « Wi-Fi Analytics » permet par conséquent de parfaitement appréhender l'usage qui est fait du Wi-Fi et d'exploiter de nombreux KPI (*Key Performance Indicator*). Il propose notamment des vues prédéfinis sur les utilisateurs, leur matériel, leur comportement ainsi que sur les aspects monétisation. Le service permet l'analyse de données personnelles et démographiques nécessaires au marketing digital.

Le service d'analytique facilite la prise de décision et de part sa disponibilité dans le Cloud peut s'utiliser sans impacter la production.

Les associations de données sont présentées graphiquement de façon dynamique et sous forme de tableau de bord.

La page ci-dessous montre un exemple de tableau de bord.



Figure 57: Exemple de tableau de bord analytique

Ce service est dédié aux clients UCOPIA compte-tenu de la confidentialité des données manipulées ou aux revendeurs mandatés par leur client.

## 8.4 Campagnes Marketing

L'objectif du service « Wi-Fi Marketing » disponible sur UWS est de pouvoir mettre en œuvre des campagnes marketing à travers un mécanisme d'injection Web. L'injection Web consiste à injecter du contenu dans les pages Web visitées par l'utilisateur final. Le contenu peut être publicitaire ou des services à valeur ajoutée. Comme le service d'Analytique, ce service est proposé aux clients UCOPIA ou aux revendeurs mandatés par leur client.

Un hôtel pourra par exemple insérer une bannière en bas de page avec son logo permettant à ses clients de découvrir les services de son établissement. L'utilisateur reste ainsi connecté en permanence aux services de l'hôtel et peut y accéder immédiatement sans besoin de revenir sur une page particulière. C'est la garantie pour l'hôtelier d'optimiser la visibilité de ses services et amener ses clients à consommer plus et mieux.

L'ajout de publicité est une autre utilisation de l'injection, permettant de créer du revenu en provenance des annonceurs publicitaires pour l'organisation qui déploie le service.

Dès lors qu'un contrôleur UCOPIA est inscrit à ce service, le trafic Web (HTTP) des utilisateurs est alors redirigé dans le Cloud afin que l'injection puisse se réaliser.

Différents types d'injection sont possible tels que bannière avec ou sans menu, image, vidéo, lien, etc.

L'exemple ci-dessous est celui d'un hôtel qui a incrusté en bas de page une bannière permettant de donner des informations sur son hôtel et de renvoyer l'utilisateur sur le site de l'hôtel.

L'utilisateur recherche un restaurant sur Internet. L'hôtel lui propose par l'intermédiaire de sa bannière de découvrir le restaurant de l'hôtel.

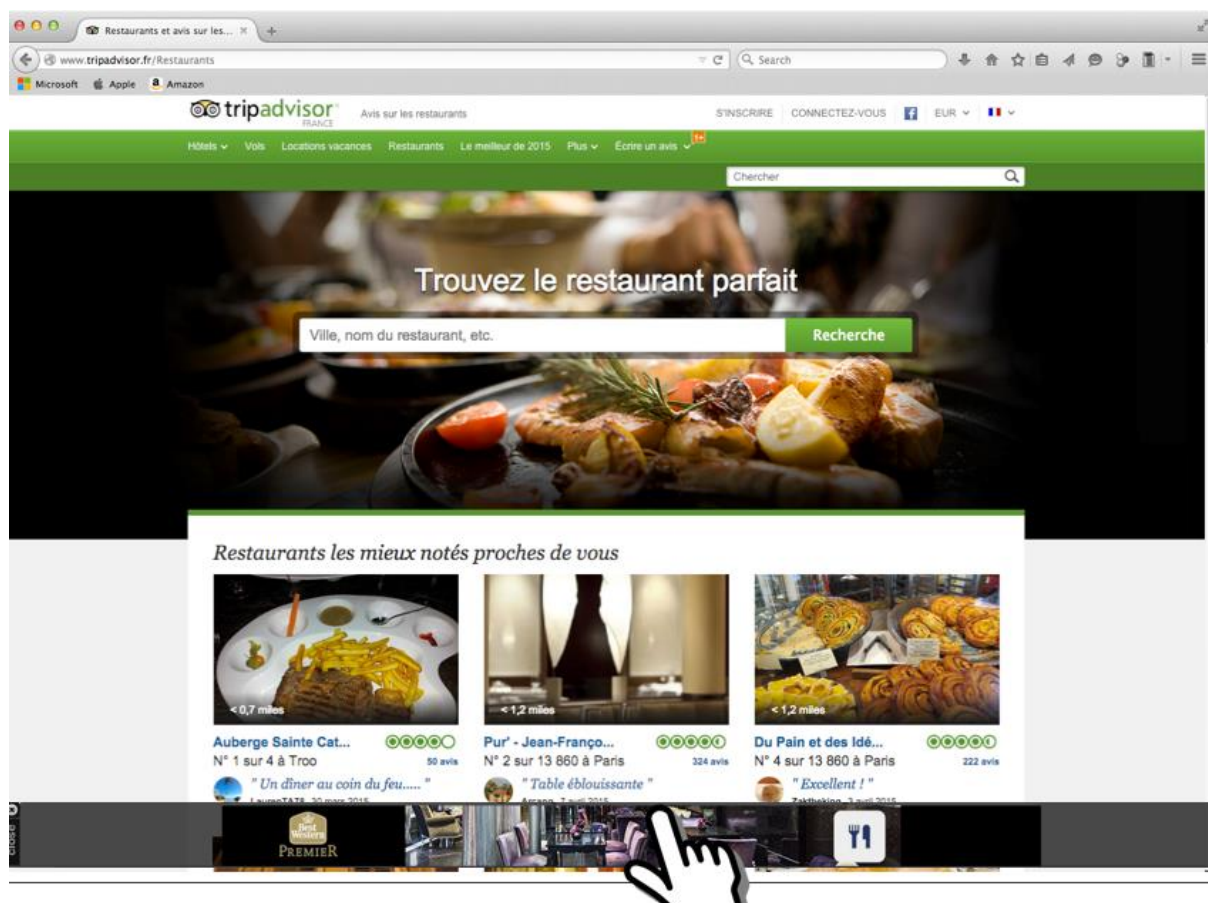


Figure 58: Exemple de campagne marketing

Une popup s'affiche sur laquelle l'utilisateur peut cliquer afin de rejoindre le site de l'hôtel.

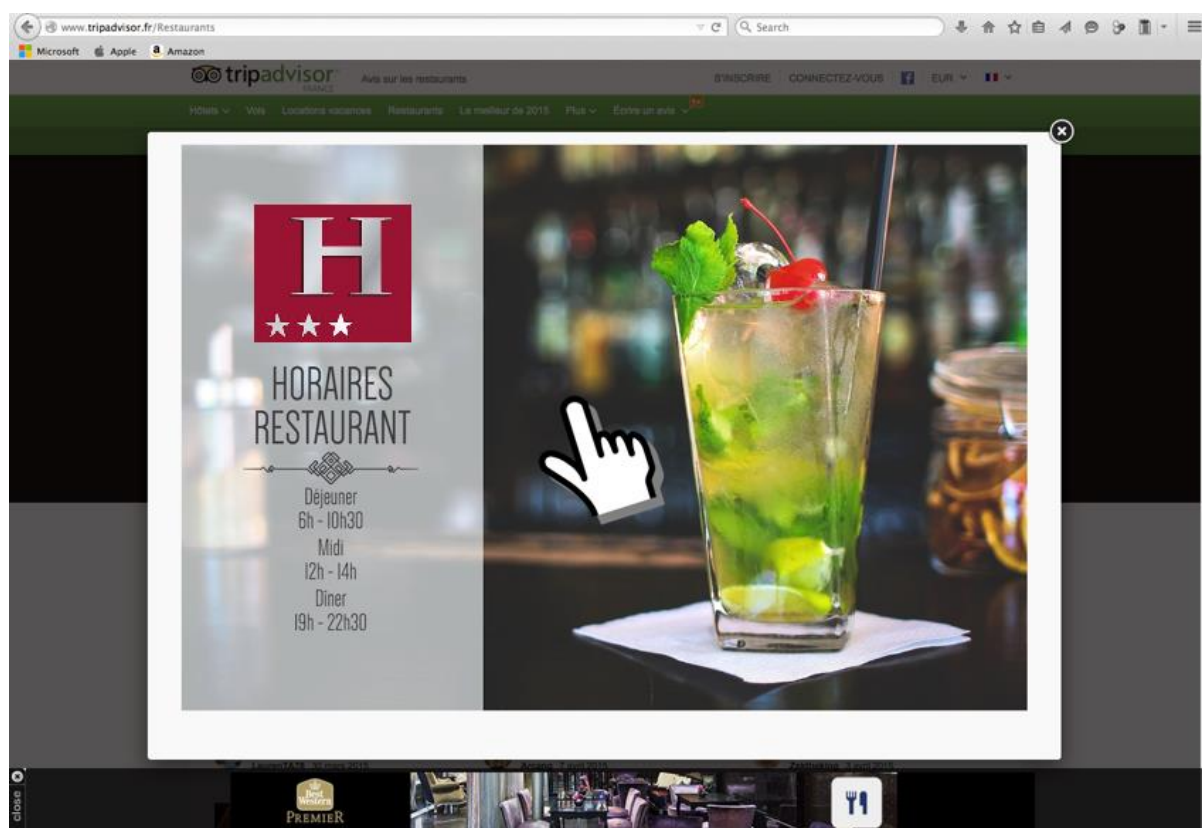


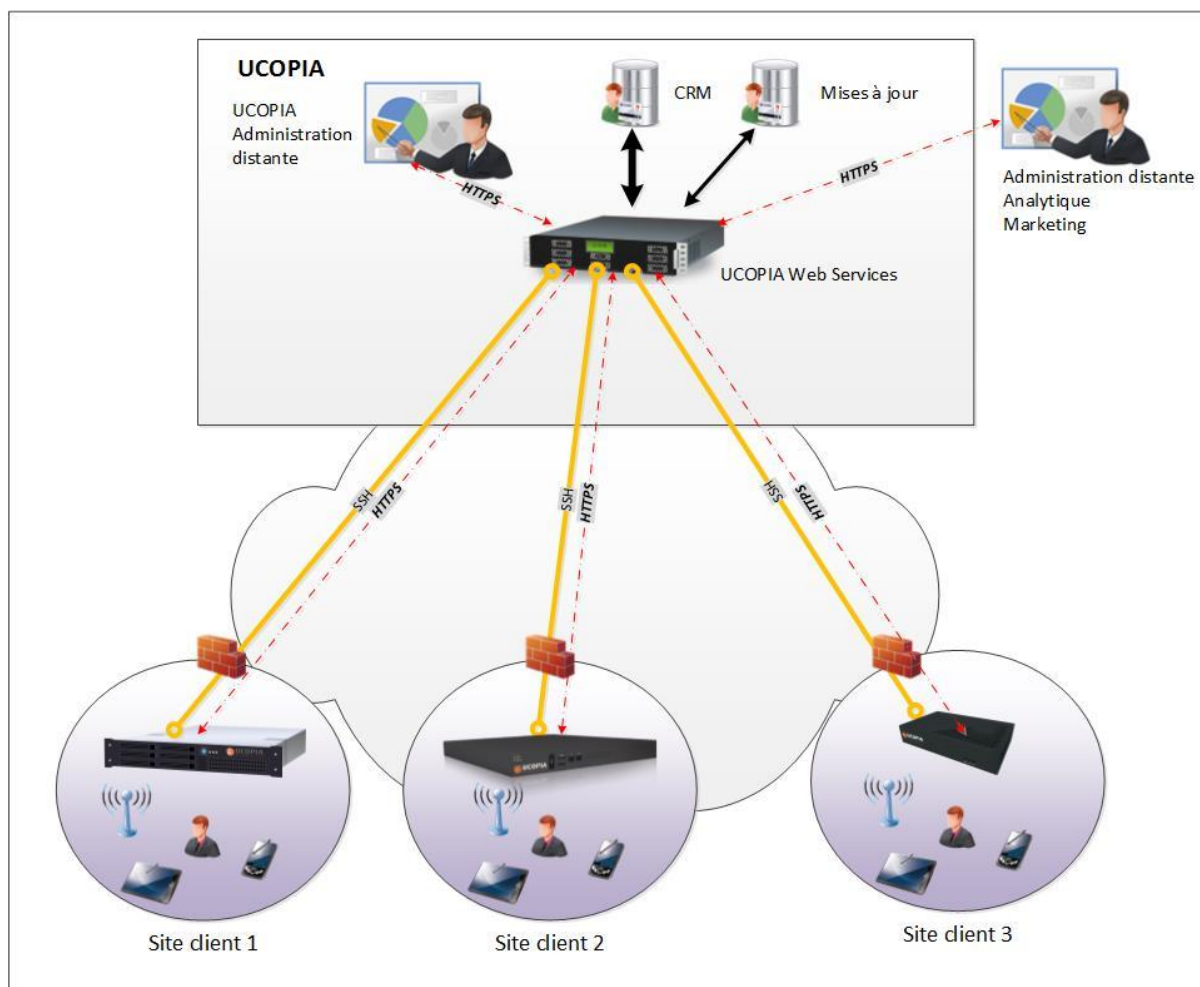
Figure 59: Exemple de campagne marketing (suite)

## 8.5 Architecture

Les contrôleurs UCOPIA communiquent avec UWS à travers le protocole HTTPS (remontée de statistiques, etc.). Des tunnels SSH sont utilisés pour l'administration distante.

L'architecture de la plate-forme UWS est la suivante.





**Figure 60: Architecture de la plate-forme UCOPIA Web Services**

## 9 Gammes UCOPIA

La solution UCOPIA se décline en deux gammes produit : la gamme UCOPIA Express et la gamme UCOPIA Advance.

- **La gamme UCOPIA Express** se présente sous la forme d'un contrôleur prêt à l'emploi parfaitement adaptée aux besoins des hôtels, cliniques, établissements d'enseignement secondaires et PME en général. UCOPIA Express propose l'essentiel des fonctions UCOPIA en termes de sécurité et de mobilité dans une approche privilégiant la simplicité de la mise en œuvre et de l'administration. UCOPIA Express fonctionne de façon autonome sans intégration forte avec le LAN.
- **La gamme UCOPIA Advance** est un contrôleur qui propose l'ensemble des fonctionnalités UCOPIA et qui est destinée aux moyens et grands projets des entreprises, des campus et des administrations. UCOPIA Advance permet de répondre aux besoins des environnements multi sites et propose toutes les fonctions d'intégration avec le LAN de l'entreprise. UCOPIA Advance peut être redondée et fonctionne également en répartition de charge.

Le tableau ci-dessous décrit les fonctionnalités de chacune des gammes UCOPIA.

Fonctionnalités	Express	Advance
<b>Sécurité</b>		
<b>Authentification</b>		
➤ Portail Web captif	•	•
➤ 802.1x/PEAP	•	•
➤ 802.1x/TTLS	•	•
➤ 802.1x/TLS		•
➤ Réseaux sociaux	•	•
➤ @MAC ou @IP fixe	•	•
➤ Authentification automatique par @MAC	•	•
➤ Shibboleth	•	•
➤ Authentification périodique et transparente (mode portail)	•	•
Redirection vers portail d'entreprise	•	•
Filtrage d'URLs	•	•
Droits d'accès en fonction du profil de l'utilisateur	•	•
VLANs/sous-réseaux en entrée du contrôleur	•	•
Redirection sur VLAN de sortie en fonction du profil utilisateur	•	•

Compatibilité 802.11i	•	•
Ruckus DPSK	•	•
ARP spoofing protection	•	•
URLs accessible avant authentification	•	•
Acceptation de charte avant authentification	•	•
Acceptation de charte pour information privée	•	•
Politiques de mot de passe et récupération de mot de passe perdu	•	•
Quarantaine après N tentatives de mot de passe erroné	•	•
Traçabilité	•	•
➤ Journaux des sessions utilisateurs	•	•
➤ Journaux du trafic utilisateurs (URL, applications)	•	•
➤ Compression automatique des journaux	•	•
➤ Rotation circulaire des journaux	•	•
➤ Sauvegarde automatique des journaux via FTP(S)	•	•
Journal d'audit en Syslog	•	•
<b>Mobilité</b>		
Zéro configuration	•	•
➤ Mode DHCP/IP fixe	•	•
➤ Accès transparent mail	•	•
➤ Accès transparent Internet	•	•
➤ Accès transparent Imprimante	•	•
➤ Compatibilité Airprint	•	•
VPN pass through	•	•
QoS (par service, par utilisateur)	•	•
Quota de volume de données	•	•
Contrôle d'accès basé sur le temps	•	•
➤ Plage horaire de connexion	•	•
➤ Crédit temps	•	•
Contrôle d'accès basé sur le lieu	•	•
➤ Localisation par zone en entrée et en sortie	•	•

Profils adaptables		•
BYOD		•
Multi portails (un portail par zone)	•	•
Application mobile (iPhone, Android, BlackBerry)	•	•
Compatibilité iPass	•	•
<b>Administration</b>		
Licence par zone ou profil	•	•
Administration des politiques de sécurité et de mobilité (services, profils utilisateurs, etc.)	•	•
Provisionnement de comptes par auto-enregistrement de l'utilisateur, envoi SMS ou email, formulaire Web, impression de ticket	•	•
Parrainage avec envoi d'email		•
Exportation manuelle des comptes utilisateur en CSV	•	•
Exportation automatique des comptes utilisateur en CSV		•
Administration déléguée (accueil des visiteurs)	•	•
➤ Personnalisation	•	•
➤ Multi zones	•	•
➤ Délivrance de coupon de connexion (impression, email, SMS)	•	•
➤ Création de comptes utilisateur en masse depuis un fichier CSV	•	•
Supervision des utilisateurs connectés	•	•
Statistiques	•	•
➤ Graphes prédéfinis	•	•
➤ Export CSV manuel	•	•
➤ Export CSV automatique		•
Reporting (PDF) avec envoi automatique par email et FTP(S)	•	•
Portail captif personnalisable via éditeur graphique	•	•
Coupon de connexion personnalisable	•	•
Personnalisation avancée de portail captif par import/export HTML	•	•
Sauvegarde automatique de configuration via FTP(S)	•	•
SNMP – MIB II	•	•

Syslog	•	•
CLI	•	•
Administration multi zones	•	•
Synchronisation à chaud d'annuaires UCOPIA		•
Port physique d'administration		• (US5000, US10000) et UV
<b>Paielement</b>		
Paielement en ligne via Paypal/Ogone	•	•
PMS connecteur	•	•
PPS connecteur	•	•
AAA (accounting)		•
<b>Intégration</b>		
Intégration avec un annuaire LDAP d'entreprise (OpenLDAP, ActiveDirectory)	•	•
Intégration avec plusieurs annuaires		•
Cascade d'annuaires		•
Intégration avec RADIUS (proxy)	RADIUS local intégré	•
Intégration avec proxy Web	•	•
Compatibilité ICAP	•	•
Intégration PKI		•
API Intégration produit tiers	•	•
<b>Architecture</b>		
Serveur DHCP (IN), client DHCP (OUT)	•	•
DNS serveur/relai	•	•
NAT	•	•
Routage	•	•
NAT ou routage suivant profil utilisateur	•	•
Réplication d'annuaires en multi sites		•
Haute disponibilité		•
➤ Redondance		•
➤ Répartition de charge		•
Connexion de postes utilisateurs en filaire	•	•

Architecture centralisée, distribuée ou mixte	•	•
Appliance virtuelle	•	•

## 10 Performances

Dans chacune des gammes UCOPIA, il existe plusieurs modèles proposant différentes capacités de montée en charge en termes de connexions simultanées.

Le tableau ci-dessous présente les capacités de chaque modèle.

<b>Express</b>	<b>Express 5</b>	<b>Express 10</b>	<b>Express 20</b>	<b>Express 50</b>	<b>Express 100</b>	<b>Express 150</b>	<b>Express 250</b>	<b>Express 500</b>	<b>Express 1000</b>	<b>Express 2000</b>
Nombre maximum d'utilisateurs simultanés	5	10	20	50	100	150	250	500	1000	2000

<b>Advance</b>	<b>Advance 150</b>	<b>Advance 250</b>	<b>Advance 500</b>	<b>Advance 1000</b>	<b>Advance 2000</b>	<b>Advance 5000</b>	<b>Advance 10000</b>
Nombre maximum d'utilisateurs simultanés	150	250	500	1000	2000	5000	10000

Au-delà de 10000 utilisateurs simultanés, une solution sur mesure est proposée (ex : cluster en répartition de charge pour la gamme Advance).



## 11 Appliances matérielles

Les contrôleurs UCOPIA sont proposés en cinq types de matériel. Tous les contrôleurs comportent a minima deux ports Ethernet 10/100/1000 et un disque dur pour la sauvegarde des journaux utilisateurs.

Le contrôleur « **US250** » pour la gamme Express supportant jusqu'à 250 utilisateurs simultanés.



Figure 61: Contrôleur format "US250"

Le contrôleur « **US2000** » pour les gammes Express et Advance supportant jusqu'à 2000 utilisateurs simultanés.



Figure 62: Contrôleur format "US2000"

Le contrôleur « **US5000RDP** » pour les solutions nécessitant plus de débit et de haute disponibilité. Le contrôleur est au format 2U. Il comporte 6 ports Ethernet dédiés au flux utilisateur (3 en entrée, 3 en sortie), un port dédié à l'administration, deux disques en RAID et une alimentation redondante. Gamme Advance uniquement jusqu'à 5000 utilisateurs simultanés.



Figure 63: Contrôleur format « US5000RDP »


Le contrôleur « **US10000RDP** » à l'instar du serveur US5000RDP est présenté en format 2U, il comporte 8 ports Ethernet dédiés au flux utilisateur, un port d'administration, quatre disques en RAID et une


alimentation redondante. Gamme Advance uniquement supportant jusqu'à 10000 utilisateurs simultanés.






**Figure 64 : Contrôleur format « US10000RDP »**

Le tableau ci-dessous résume le matériel pour chaque modèle UCOPIA.

Express	Express 5	Express 10	Express 20	Express 50	Express 100	Express 150	Express 250
Matériel	US250						
							

Express	Express 500	Express 1000	Express 2000
Matériel	US2000		
			

Advance	Advance 150	Advance 250	Advance 500	Advance 1000	Advance 2000	Advance 5000	Advance 10000
Matériel	US2000					US5000RDP	US10000RDP
							

Les caractéristiques techniques des contrôleurs sont les suivantes :

	Format	Format	Format	Format
--	--------	--------	--------	--------

	« US250 »	« US2000 »	« US5000RDP »	« US10000RDP »
Disque dur	320 Go	1 Tera	2 Tera (raid 1)	4 x 900 Go (raid 5)
Ports réseau	2 (10/100/1000)	2 (10/100/1000)	6 (10/100/1000) 3x IN, 3xOUT 1 (10/100/1000) Administration	8 (10/100/1000) 4x IN, 4xOUT 1 (10/100/1000) Administration
Cons. électrique	24W (alim externe)	90 W	250 W (2 alim. Hot Plug)	750 W (2 alim. Hot Plug)
Dimension (HxLxP)	52x270x160 mm Kit rack 19'' en option	44x430x500mm Rack 1U 19''	88x430x700mm Rack 2U 19''	88x430x700mm Rack 2U 19''








Les modèles sont évolutifs, soit par simple clé logicielle, soit par changement de matériel, les tableaux ci-dessous présentent les possibilités d'évolution.






















= clé logicielle



= changement de matériel

Modèles	Exp. 10	Exp. 20	Exp. 50	Exp. 100	Exp. 150	Exp. 250	Exp. 500	Exp 1000	Exp
Materiel	US250						US2000		
Exp.5									
Exp.10									
Exp.20									
Exp.50									
Exp. 100									
Exp. 150									
Exp. 250									
Exp. 500									
Exp 1000									

Modèles	Adv. 250	Adv. 500	Adv 1000	Adv 2000	Adv 5000	Adv 10000
Matériel	US2000				US5000	US10000
Adv. 150						
Adv. 250						
Adv. 500						
Adv 1000						
Adv 2000						
Adv 5000						

## 12 Appliances virtuelles

---

L'appliance UCOPIA est proposée en mode virtualisé sous VMware, gamme Express et Advance. L'ensemble des fonctionnalités des gammes est supporté (redondance et équilibrage de charge inclus).

Quatre serveurs virtuels sont disponibles : UV250, UV2000, UV5000 et UV10000.

## 13 Maintenance

---

Les contrôleurs UCOPIA sont commercialisés avec a minima une maintenance de 3 ans, extensible à 5 ans.

Le contrat de maintenance couvre les points suivants :

- Changement anticipé du contrôleur en cas de défaillance matérielle (pour les appliances physiques). Envoi d'un matériel équivalent à J+1 (en France métropolitaine).
- Mise à disposition des mises à jour logicielles correctives et évolutives.
- Accès pour le partenaire au service de support technique UCOPIA (niveau 2 et plus).



## 14 Conclusion

---

UCOPIA développe et commercialise une solution à destination des utilisateurs mobiles, elle leur permet de se connecter simplement, en toute sécurité et avec tout type d'équipement (PC, smartphone, tablettes) aux réseaux Wi-Fi ou filaire.

UCOPIA présente les avantages et les bénéfices suivants.

- **Une sécurité professionnelle et un respect des obligations légales**

UCOPIA met en œuvre des fonctions de sécurité robustes conformes aux standards de l'industrie. Des mécanismes d'authentification allant d'un portail captif HTTPS à une authentification forte basée sur les protocoles 802.1x/EAP et RADIUS. Un contrôle d'accès basé sur le profil de l'utilisateur, son lieu de connexion, son heure de connexion, son type d'équipement. Un filtrage d'URLs par profil utilisateur. Une parfaite traçabilité du trafic utilisateur et la conservation des journaux de connexion pour répondre aux exigences légales.

UCOPIA est certifié par l'ANSSI pour ses fonctions de sécurité.

- **Un parcours client simple et convivial**

UCOPIA propose une grande variété de parcours client permettant de répondre à différents usages. Du simple clic pour se connecter à des méthodes nécessitant authentification et confidentialité. La reconnaissance de l'équipement utilisateur permet si besoin d'assurer une connexion transparente.

Le portail captif donne la possibilité aux utilisateurs de s'auto-enregistrer avec réception des identifiants par divers biais (SMS, email, coupon papier, ...).

Les mécanismes de zéro-configuration UCOPIA facilitent l'accès, ils permettent à l'utilisateur de se connecter aisément quel que soit son équipement ou sa configuration.

Une application mobile pour smartphone contribue au confort de l'utilisateur.

- **Une gestion des utilisateurs nomades**

UCOPIA permet aux employés nomades, aux clients, partenaires, fournisseurs de se connecter simplement et en toute sécurité en tout lieu (bureau mobile, salle de réunions ou de formation, etc.), d'accéder à leur messagerie, à l'Internet, d'échanger ou d'imprimer des documents. Aucun pré requis ou configuration n'est imposé à l'utilisateur et il n'aura pas à faire appel à l'assistance technique pour imprimer un document ou envoyer un message. UCOPIA contribue à l'image de marque des entreprises en permettant aux visiteurs d'accéder à leur réseau.

- **Une approche génératrice de revenus**

Le service d'Analytique permet de mieux appréhender les usages et les utilisateurs. Il est alors possible de proposer des services à valeur ajoutée ou de la publicité ciblée sur le portail captif ou dans les pages visitées grâce à l'injection Web. Ceci contribue à promouvoir, à fidéliser et à monétiser les accès.

L'accès aux services peut également être facturé en achetant des forfaits en ligne depuis le portail (carte de crédit, PayPal, Ogone) ou à travers les connecteurs avec des outils de facturation.

- **Une solution hautement disponible**

Grâce à son architecture en cluster, UCOPIA peut garantir une haute disponibilité du service. Un cluster fonctionne en mode redondance et/ou en mode répartition de charge.

### ■ **Un coût de possession (TCO) optimisé**

Le déploiement d'une solution d'accueil de nomades nécessite une intégration avec l'infrastructure de communication et de sécurité existante. Sans UCOPIA, cela peut nécessiter beaucoup de travail et de délai. UCOPIA s'intègre simplement au réseau en place (VLAN, annuaire, etc.) sans remettre en cause les politiques de sécurité déjà présentes. Par ailleurs grâce à sa simplicité d'administration et à ses mécanismes de zéro configuration, UCOPIA limite le besoin en ressources techniques. Tous ces avantages contribuent à réduire fortement le coût de possession d'une telle solution.

### ■ **Une solution pérenne et évolutive**

L'offre UCOPIA est composée d'une large gamme de produits permettant de répondre aussi bien aux besoins des petites structures qui souhaitent accueillir quelques utilisateurs qu'aux architectures centralisées multi sites assurant plusieurs milliers de connexions simultanées.

La solution UCOPIA s'administre à travers des outils de haut niveau puissants et conviviaux. Des rapports de statistiques (nombre de sessions simultanées, durée des sessions, types de matériels utilisés, etc.) permettent de mieux appréhender l'usage qui est fait de la solution en place.

Une plate-forme centralisée permet une administration et une supervision distantes d'un parc de contrôleurs UCOPIA.

La solution UCOPIA est indépendant des équipements réseau et peut fonctionner en environnement hétérogène, elle garantit ainsi la pérennité des choix de matériel. UCOPIA fonctionne en environnement filaire et Wi-Fi, son niveau d'abstraction par rapport au réseau physique lui permet d'évoluer avec les standards.

## 15 Annexe 1 : Documentation

---

Un ensemble de documentations est proposé avec le produit UCOPIA.

### 15.1 Manuels

---

- **Manuel d'installation**

Ce manuel s'adresse aux administrateurs système et/ou réseaux désirant installer la solution UCOPIA. Il décrit l'installation et la configuration de l'ensemble des composants de la solution. Il existe un manuel pour Express et un pour Advance.

- **Manuel d'administration**

Ce manuel s'adresse aux administrateurs système et/ou réseaux ayant en charge l'administration d'UCOPIA.

Sont présentés dans ce manuel l'outil d'administration et l'ensemble des procédures d'administration. Il existe un manuel pour Express et un pour Advance.

- **Manuel d'administration déléguée**

Ce manuel décrit le portail de délégation, il est commun aux deux gammes de produit UCOPIA : Express et Advance.

- **Manuel d'utilisation de l'éditeur de portail UCOPIA**

Ce manuel décrit l'éditeur graphique de portail UCOPIA. Ce manuel est commun aux deux gammes de produit UCOPIA: Express et Advance.

- **Manuel d'utilisation d'UCOPIA**

Ce manuel s'adresse aux utilisateurs d'un réseau contrôlé par UCOPIA. Il décrit l'utilisation des différents modes de portail.

Ce manuel est commun aux deux gammes produit UCOPIA: Express et Advance.

- **Manuel d'utilisation de la base de données des journaux utilisateurs**

Les journaux de sessions et de trafic sont créés localement sur le contrôleur UCOPIA et sont accessibles depuis l'outil d'administration UCOPIA. Les journaux sont stockés dans une base de données SQL.

Afin de faciliter l'intégration avec des applications tierces, UCOPIA propose de se connecter à la base SQL des journaux. Ce document décrit le fonctionnement de cette base de données, les entités de la base et de leurs attributs.

- **Manuel d'utilisation de la CLI UCOPIA**

Ce document décrit la CLI (Command Line Interface) UCOPIA. Ce langage donne accès à certaines commandes réseau, système ou administration avancée. La CLI permet également de diagnostiquer d'éventuels dysfonctionnements.

### 15.2 APIs

---

- **API UCOPIA Administration déléguée**

L'objectif de l'API d'administration déléguée est de permettre de coupler le contrôleur UCOPIA avec un outil tiers tel qu'un outil de provisionnement de compte et/ou de facturation de services.

L'API d'administration déléguée permet de créer/détruire/modifier un compte utilisateur ainsi que de récupérer un temps de connexion cumulée pour un utilisateur.

- **API UCOPIA Portail**

L'API Portail est utilisée dans le cas d'une personnalisation de portail avancée. L'API définit l'ensemble des interactions entre le portail et le contrôleur UCOPIA. A travers cette API, tous les modes d'authentification sont possibles (portail standard avec login et mot de passe, portail avec inscription par SMS, portail avec inscription par email, etc..).

- **API UCOPIA Application mobile**

L'API Application mobile est utilisée pour apporter les fonctions de l'application mobile UCOPIA (authentification, sponsoring) à une application tierce, par exemple une application métier.

## 15.3 Couplage avec produits tiers

---

- **Envoi de SMS via le contrôleur UCOPIA**

UCOPIA propose un mode de provisionnement de compte pour lequel l'utilisateur s'auto enregistre sur le portail UCOPIA en utilisant son téléphone mobile. Il reçoit ses identifiants de connexion par SMS.

Ce document décrit les différentes plates-formes de SMS avec lesquelles UCOPIA s'interface.

- **Couplage UCOPIA avec un PMS**

Le contrôleur UCOPIA s'interface avec des produits de type PMS (*Property Management System*).

Ce document décrit la façon dont les produits interopèrent.

- **Utilisation de Paypal avec UCOPIA**

Ce document décrit le mode de fonctionnement du portail UCOPIA permettant aux utilisateurs d'acheter forfait en ligne via Paypal. Il détaille également comment ouvrir un compte Paypal et comment configurer UCOPIA en conséquence.

- **UCOPIA et compatibilité iPass**

Ce document décrit la façon dont UCOPIA doit être configuré pour accueillir des utilisateurs iPass. Il précise également les contraintes et configurations au niveau des équipements réseau.

## 15.4 Certification de sécurité

---

[http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat\\_cspn\\_2010\\_01.html](http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat_cspn_2010_01.html)

## 16 Annexe 2 : Glossaire

---

Nous présentons dans cette annexe la définition des mots clés ou des acronymes utilisés dans ce document.

### 16.1 Réseau

---

- **DNS - *Domain Name Service*** : Service de nom de domaines (correspondance IP<->nom des machines)
- **SNMP - *Simple (ou Smart) Network Management Protocol*** : Protocole de la couche application pour l'administration réseau.
- **HTTPS - *Hyper Text Transfert Protocol over SSL*** : Protocole de transmission issu de Netscape lié à une connexion par socket sécurisée.
- **VLAN – *Virtual Local Area Network***: Permet de réaliser plusieurs réseaux logiques sur un même réseau physique. Les VLANs sont configurés au niveau des Switch et des routeurs.
- **DHCP – *Dynamic Host Configuration Protocol*** : DHCP est un protocole permettant d'allouer une adresse IP a un client voulant se connecter au réseau.
- **NAT – *Network Address Translation*** : NAT est un mécanisme permettant d'allouer des adresses IP privées à partir d'une seule adresse IP publique.
- **ICAP – *Internet Content Adaptation Protocol*** : Le protocole ICAP définit une interface normalisée entre des équipements réseau jouant le rôle de client (serveur mandataire, pare-feu, passerelles de sécurité), et des équipements de services (serveurs ICAP) dont l'objectif est l'analyse et l'adaptation en temps réel des flux Web (ex : filtrage d'URLs).

### 16.2 Wi-Fi

---

- **Wi-Fi – *Wireless Fidelity***: Wi-Fi est le nom commercial pour la technologie IEEE 802.11. Le Wi-Fi est composé de plusieurs standards.
- **802.11 b/a/g/n** : Il s'agit d'un ensemble de standards pour définir les différents débits du Wi-Fi : 802.11a propose une bande passante de 54 Mbps sur une fréquence de 5 Ghz, 802.11b et g opèrent sur la fréquence 2,4 Ghz et propose une bande passante respectivement de 11 et de 54 Mbps. 802.11n propose une bande passante supérieure à 100 Mbps.
- **802.11i** : Standard de sécurité pour le Wi-Fi ratifié en juin 2004. Il inclut 802.1x pour l'authentification et AES (Advanced Encryption Standard) pour le chiffrement. 802.11i requière des équipements compatibles à la fois côté client et côté point d'accès.
- **802.11e** : Standard pour la Qualité de Service. Il n'est pas ratifié. 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
- **802.11f** : Standard pour le roaming. Il n'est pas ratifié. 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau.

## 16.3 Authentification

---

- **802.1x** : Standard de contrôle d'accès au réseau, indépendant du support physique. Le réseau permet uniquement le passage de trafic d'authentification tant que l'authentification n'est pas accomplie avec succès. Le 802.1x spécifie également le protocole EAPOL (EAP over LAN) qui permet l'encapsulation des méthodes d'authentification EAP.
- **EAP – Extensible Authentication Protocol**: EAP est un protocole d'authentification opérant au niveau 2 OSI avant que le client n'obtienne une adresse IP, il renforce ainsi la sécurité. Basées sur EAP, il existe de nombreuses méthodes d'authentification, par mot de passe (PEAP, TTLS), par certificat (TLS), etc. EAP est utilisé dans une architecture 802.1x et fonctionne par conséquent avec un serveur d'authentification, généralement RADIUS.
- **EAP-MD5**: Le client est authentifié par le serveur en utilisant un mécanisme de défi réponse. Le serveur envoie une valeur aléatoire (le défi), le client concatène à ce défi le mot de passe et en calcule, en utilisant l'algorithme MD5, une empreinte (" hash ") qu'il renvoie au serveur. Le serveur qui connaît le mot de passe calcule sa propre empreinte, compare les deux et en fonction du résultat valide ou non l'authentification.
- **LEAP – Lightweight EAP**: est une méthode propre à Cisco qui repose sur l'utilisation de secrets partagés pour authentifier mutuellement le serveur et le client. Elle n'utilise aucun certificat et est basée sur l'échange de défi et réponse.
- **EAP-TTLS – Tunneled Transport Secure Layer** : utilise TLS comme un tunnel pour échanger des couples attribut valeur à la manière de RADIUS servant à l'authentification..
- **PEAP – Protected EAP**: est une méthode très semblable dans ses objectifs et voisine dans la réalisation à EAP-TTLS. Elle est développée par Microsoft. Elle se sert d'un tunnel TLS pour faire circuler de l'EAP. On peut alors utiliser toutes les méthodes d'authentification supportées par EAP.
- **EAP-TLS – Extensible Authentication Protocol-Transport Layer Security**: C'est la plus sûre. Le serveur et le client possèdent chacun leur certificat qui va servir à les authentifier mutuellement. Cela reste relativement contraignant du fait de la nécessité de déployer une infrastructure de gestion de clés. Rappelons que TLS, la version normalisée de SSL (Secure Socket Layer), est un transport sécurisé (chiffrement, authentification mutuelle, contrôle d'intégrité).
- **NTLM – NT Lan Manager**: est un protocole d'authentification Microsoft. Ce protocole utilise un mécanisme de challenge-réponse pour l'authentification dans lequel les clients peuvent prouver leur identité sans envoyer de mot de passe au serveur. Le protocole consiste en 3 messages : Type 1 (négociation), Type 2 (challenge) and Type 3 (authentification).
- **PKI – Public Key Infrastructure**: Une PKI est une architecture basée sur des clés publiques et privées stockées dans des certificats. Cette architecture permet aux entreprises de déployer des solutions sécurisées pour échanger des emails, des documents, etc.
- **RADIUS - Remote Access Dial-in User Services**: RADIUS est un protocole standard pour interroger de façon distante un serveur d'authentification.
- **OTP - One Time Password** : Consiste à utiliser des mots de passe qui ne peuvent être utilisés qu'une seule fois. Même si le mot de passe est dérobé, il n'est pas réutilisable. Dans la pratique, ce dispositif repose sur des techniques de cryptographie à clés secrètes ou symétriques et prend généralement la forme d'une calculatrice avec un clavier et un affichage numérique (ex. ActivCard, SecureID).

- **SSO – Single Sign On** : Le SSO permet de fédérer l'authentification. Grâce au Single Sign-On, il est possible de regrouper toutes les demandes d'authentification en une procédure unique. Le confort des utilisateurs et le niveau de sécurité s'en trouvent améliorés.
- **WISPr – Wireless Internet Service Provider roaming** : WISPr est un protocole qui permet aux utilisateurs de "roamer" entre plusieurs fournisseurs d'accès Internet. Un serveur RADIUS est utilisé pour l'authentification et la vérification des identifiants.

## 16.4 Chiffrement

---

- **WEP – Wired Equivalent Protection** : WEP est un protocole fondé sur l'algorithme RC4 (clé de 64 bits), il permet de réaliser le contrôle d'accès l'authentification, la confidentialité et l'intégrité. Le WEP est connu pour ses faiblesses : clé de petite taille, clé statique et partagée par plusieurs utilisateurs.
- **TKIP – Temporary Key Interchange Protocol**: TKIP est un protocole de chiffrement destiné à améliorer le WEP. Il génère des clés dynamiques via des réauthentifications 802.1x périodiques.
- **AES, DES, 3DES**: Il s'agit d'algorithmes de chiffrement utilisant des clé de 128 bits. Ils sont utilisés dans les solutions de VPN et dans les mécanismes de chiffrement des dernières générations de points d'accès.
- **VPN – Virtual Private Network**: Le principe du VPN est basé sur la technique du tunnelling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel. Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le protocole de tunnelling encapsule les données en rajoutant une entête, permettant le routage des trames dans le tunnel. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.
- **IPSec**: Protocole permettant de sécuriser les transmissions à travers des réseaux non sécurisés comme l'Internet. IPSec agit au niveau de la couche réseau, protégeant et authentifiant les paquets IP entre les dispositifs participants, comme un routeur.
- **SSL – Secure Socket Layer** : SSL est un protocole pour gérer la sécurité de la transmission de messages sur Internet. Il se positionne entre les couches HTTP et TCP.
- **WPA – Wireless Protected Access**: WPA est un sous-ensemble du standard 802.11i regroupant 802.1x et TKIP.
- **WPA2** – Renforce la sécurité WPA en se basant sur l'algorithme de chiffrement AES.
- **WPA-PSK - Pre Shared Key** : Mode permettant de profiter de la sécurité WPA sans disposer de serveur d'authentification. La configuration du WPA-PSK commence par la détermination d'une clé statique ou d'une "passphrase" comme pour le WEP. Mais, en utilisant TKIP, WPA-PSK change automatiquement les clés à un intervalle de temps prédéfini.
- **DPSK – Dynamic Pre Share Key** : Solution Ruckus permettant de délivrer dynamiquement une clé de chiffrement unique par utilisateur.

## 16.5 Annuaire

---

- **LDAP – Light Directory Access Protocol**: LDAP est un protocole pour accéder à différents services d'un annuaire (interrogation, mise à jour, etc). Les annuaires peuvent être de différents types.



- **LDAPS – *LDAP over SSL***: Protocole sécurisé pour accéder à un annuaire.



[www.ucopia.com](http://www.ucopia.com)