Cible de sécurité CSPN
UCOPIA 3.0

Ref : UCP-CSPN-3.0-09

SUIVI DE DOCUMENT

Version	Auteur	Date	Modifications
1.0	P. Borras	04/02/2009	Version initiale
1.1	P. Borras	10/02/2009	Intégration des remarques DCSSI
2.0	P. Borras	15/09/2009	Intégration des remarques suite évaluation Thales • Ajout d'une section 3.5.1 préconisant des outils tiers. • Section 3.6 : Précisions sur la description des rôles • Section 5 : Biens protégés par le produit. Prise en compte des remarques • Section 6 : Menaces. Prise en comptes des remarques • Ajout d'une section 7.5 présentant le fonctionnement du produit et plus particulièrement les méthodes d'authentification • Ajout d'une section 8 détaillant l'architecture UCOPIA et l'interaction entre les différents modules

TABLE DES MATIERES

1 Introduction 5
2 Identification du produit 5
3 Argumentaire du produit 5
3.1 Description générale du produit 5
3.2 Description de la manière d'utiliser le produit 6
3.3 Description de l'environnement prévu pour l'utilisation du produit 6
3.4 Description des hypothèses sur l'environnement 7
3.5 Description des dépendances. 8
3.5.1 Préconisations pour les outils tiers 9
3.6 Description des utilisateurs typiques concernés. 10
3.7 Définition du périmètre de l'évaluation. 11
4 Environnement technique de fonctionnement du produit 12
5 Biens sensibles devant être protégés par le produit 13
5.1 Biens protégés par le produit UCOPIA 13
5.2 Biens appartenant au produit UCOPIA 13
6 Description des menaces 14
6.1 Menaces relatives au contrôle d'accès d'un utilisateur 14
6.2 Menaces relatives à l'administration 15
6.3 Menaces relatives aux journaux 15
6.4 Menaces relatives à la télémaintenance 15
7 Description des fonctions de sécurité du produit 15
7.1 Authentification 16
7.1.1 Authentification par certificats et protocole 802.1x 16
7.1.2 Authentification par login/mot de passe et protocole 802.1x 16
7.1.3 Authentification depuis le portail Web captif UCOPIA 16
7.1.4 Génération des mots de passe utilisateur 16
7.2 Contrôle d'accès par filtrage de flux 16
7.3 Cloisonnement VLAN 17
7.4 Traçabilité 18
7.5 Principe de fonctionnement 19
7.5.1 Authentification par protocole 802.1x/EAP 19
7.5.2 Authentification par portail Web 22
8 Architecture du produit 23
8.1 Le contrôleur UCOPIA 24
8.2 L'administration UCOPIA 26
8.3 Télémaintenance de l'appliance UCOPIA 28
7.5.3 Téléchargement de licence et de mises à jour 29
7.5.4 Télémaintenance 29
9 Description des mécanismes cryptographiques 29
10 Glossaire 30
10.1 Terminologie UCOPIA utilisée dans le cadre de la cible de sécurité 30
10.2 Réseau 30
10.3 Wi-Fi 30
10.4 Authentification 31
10.5 Chiffrement 32
10.6 Annuaire 33
11 Références (RFC et standards) 33

TABLE DES FIGURES

Figure 1: Architecture globale de la solution UCOPIA 7
Figure 2: Exemple d'architecture UCOPIA 9
Figure 3 : Architecture physique de la plate-forme d'évaluation 12
Figure 4: Cloisonnement par VLAN 17
Figure 5: Flux pour le contrôle d'accès 19
Figure 6: Authentification 802.1x dans la norme 802.11i 20
Figure 7: Flux d'authenfication EAP 21
Figure 8: Flux d'authentification par portail captif 22
Figure 9: Architecture globale UCOPIA 24
Figure 10: Architecture du contrôleur UCOPIA 25
Figure 11: Architecture des outils d'administration UCOPIA 27
Figure 12 : Architecture de la plate-forme de gestion de parc d'appliances UCOPIA 29

1 Introduction

Ce document décrit la cible de sécurité relative au produit UCOPIA 3.0 en vue de l'obtention d'une certification de sécurité de premier niveau des technologies de l'information (CSPN).

2 Identification du produit

Société éditrice	UCOPIA Communications
Lien vers la société	www.ucopia.com
Nom commercial du produit	UCOPIA
Numéro de la version évaluée	3.0
Catégorie de produit	Contrôleur d'accès réseau

3 Argumentaire du produit

3.1 Description générale du produit

La solution UCOPIA 3.0 est une solution sécurisée dédiée à la gestion de la mobilité dans les réseaux sans fil Wi-Fi et filaires. UCOPIA 3.0 se présente sous la forme d'une **appliance matérielle**.

Deux familles de fonctions sont proposées par UCOPIA 3.0, les fonctions de sécurité et les fonctions de mobilité.

- **Sécurité :** UCOPIA propose une authentification forte construite sur une architecture 802.1x et un serveur RADIUS. Une fois authentifié, l'appliance transmet les clés de chiffrement négociées au point d'accès Wi-Fi pour que 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 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 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.
  UCOPIA peut s'interfacer avec un (ou plusieurs) annuaire(s) LDAP, s'intègre avec les architectures VLANs et peut cohabiter avec d'autres solutions de sécurité en place (RADIUS, Domaine Windows, PKI, etc.)

- **Mobilité :** UCOPIA permet de définir les politiques de mobilité de l'entreprise ou de l'organisation puis de les mettre en œuvre sur les différents sites concernés. 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. La transparence est un ensemble de mécanismes permettant à l'utilisateur de ne plus être contraint à reconfigurer ses différentes applications réseaux (tel que la

messagerie ou son navigateur Web) dès qu'il se déplace d'un réseau à un autre. Avec UCOPIA, l'accès aux services est transparent : pas besoin de reconfigurer son poste de travail, ni d'attendre l'aide de l'assistance technique locale.

UCOPIA 3.0 fournit deux outils d'administration de haut niveau proposant des interfaces Web conviviales. L'un est dédié à l'administrateur du réseau et autorise l'ensemble des fonctions d'administration, l'autre a des prérogatives plus restreintes et est dédié à des administrateurs délégués.

3.2 Description de la manière d'utiliser le produit

Le produit UCOPIA une fois installé, configuré et mis en route dans son environnement réseau (voir Section suivante pour la description de l'environnement), est utilisé par les utilisateurs finaux pour accéder aux ressources du réseau protégées par UCOPIA. Ces utilisateurs s'authentifient dans un premier temps puis se voient attribuer un profil utilisateur qui décrit les droits d'accès aux ressources du réseau en fonction de leur lieu de connexion et de leur heure de connexion. Les différentes méthodes d'authentification sont décrites en Section 7.1.

3.3 Description de l'environnement prévu pour l'utilisation du produit

L'appliance UCOPIA vient se positionner dans un réseau d'entreprise dit **réseau de confiance**[1] en point de coupure (logique ou physique) entre une infrastructure Wi-Fi et/ou filaire (infrastructure d'accueil) potentiellement « hostile » où sont accueillis des visiteurs ou utilisateurs nomades et le réseau local d'entreprise (LAN). UCOPIA a des fonctions d'authentification et de contrôleur de trafic réseau. Pour ce faire, l'appliance UCOPIA dispose de deux cartes Ethernet, l'une en entrée sur l'infrastructure d'accueil, l'autre en sortie sur le LAN. L'architecture est présentée ci-dessous.

[1] Voir définition en Section 10.1

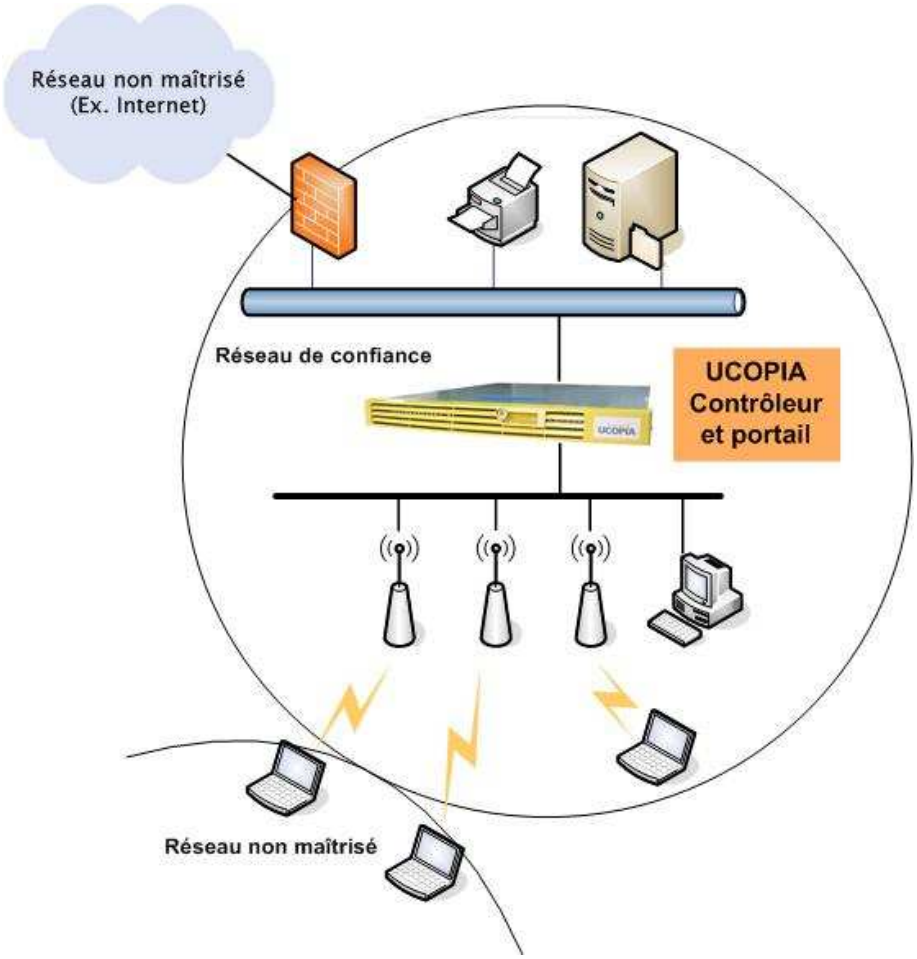

Figure 1: Architecture globale de la solution UCOPIA

3.4 Description des hypothèses sur l'environnement

PRODUIT : Le produit UCOPIA est supposé être conforme à sa documentation et fournir les fonctions pour lesquelles il est prévu.

LOCAUX : L'appliance UCOPIA, ainsi que tous supports contenant les biens sensibles UCOPIA (papier, CDs, sauvegardes,...) sont supposés se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

INSTALLATION :

- Les boîtiers appliances UCOPIA sont installés dans un réseau de confiance et ne sont utilisés que pour les fonctions de sécurité décrites dans la CSPN.
- Les boîtiers appliances UCOPIA sont supposés être installés conformément à la politique d'interconnexion des réseaux en vigueur et sont supposés être les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information. (*Cette architecture en « coupure » peut être réalisée physiquement ou logiquement. La coupure logique se fera en utilisant des VLANs).*
- Les échanges entre l'appliance UCOPIA et d'autres machines via un réseau ouvert sont

supposés contrôlés par un pare-feu contrôlant et limitant les échanges.

ADMINISTRATEUR :

- Les administrateurs sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

- L'administrateur est supposé être habilité à se connecter via l'outil d'administration UCOPIA à l'appliance UCOPIA pour les opérations d'administration (configuration, mise en place des politiques de sécurité, exploitation, mises à jour). Il est chargé de la définition des profils des administrateurs délégués. Toutes les interventions sur les appliances UCOPIA se font sous sa responsabilité.

- Différents administrateurs avec les mêmes droits ne mènent pas des actions d'administration contradictoires (modifications incohérentes de politiques de sécurité).

- L'administrateur dispose des moyens de contrôler la configuration UCOPIA, de la sauvegarder et de la restaurer dans un état sûr.

- L'administrateur est en charge de surveiller les évènements d'audit et les alarmes.

BONNE PRATIQUE : Les mots de passe des utilisateurs et des administrateurs devraient être choisis de façon à retarder toutes les attaques visant à les casser, via une politique de création de ceux-ci (par exemple, mélange alphanumérique, longueur minimum, ajout de caractères spéciaux, pas de mots de dictionnaires usuels, etc.).

3.5 Description des dépendances.

Nous décrivons ici les dépendances que peut avoir UCOPIA avec des matériels et/ou des produits tiers.

UCOPIA s'interface essentiellement avec deux types de produit réseau (appartenant au réseau de confiance) :

- **Commutateur**
  L'appliance UCOPIA est connectée à un commutateur à travers une architecture physique ou logique (VLAN).
- **Pare feu**
  Les échanges entre l'appliance UCOPIA et d'autres machines via un réseau ouvert sont supposés être contrôlés par un pare-feu contrôlant et limitant les échanges.

Par ailleurs, durant la phase d'authentification des utilisateurs, UCOPIA peut être configuré pour dialoguer avec un **annuaire LDAP**. L'annuaire doit être standard LDAP V3, le protocole utilisé entre UCOPIA et l'annuaire est LDAPS.

Le schéma ci-dessous décrit un exemple d'architecture dans lequel UCOPIA interfère avec un commutateur et un pare feu.

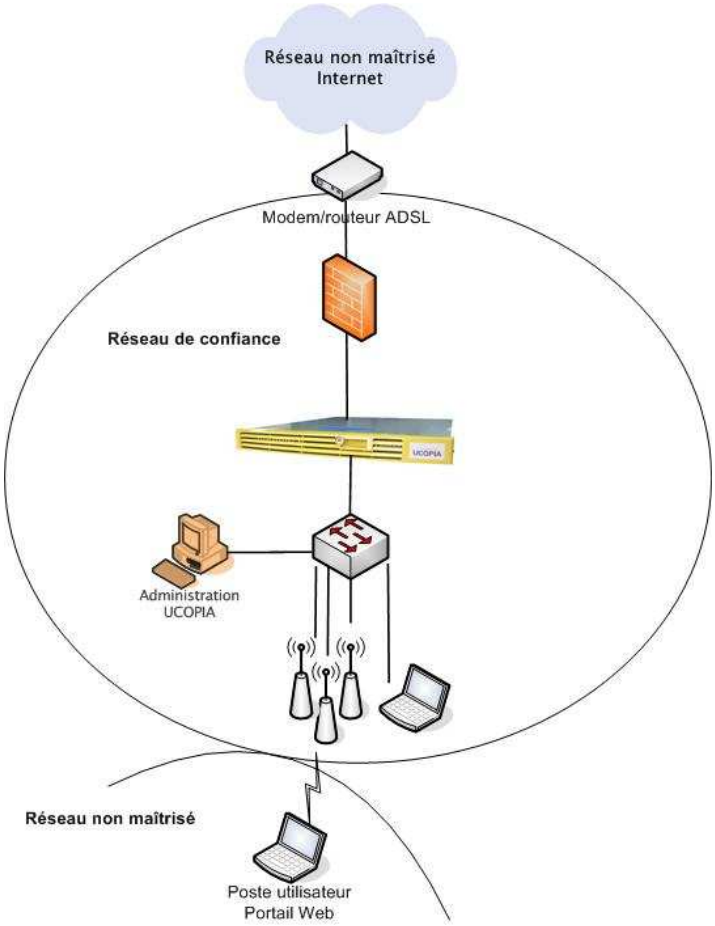

Figure 2: Exemple d'architecture UCOPIA

3.5.1 Préconisations pour les outils tiers

Les choix des outils tiers avec lesquels l'appliance UCOPIA communique et/ou s'interface doit se faire en conformité avec les exigences de sécurité imposées par la CSPN.

A titre d'exemples, voici quelques produits certifiés pouvant satisfaire à l'architecture.

- Pare-feu :
  - **Suite logicielle IPS Firewall Netasq version 5**
  - Rapport de certification 2005/06
  - Référentiel: Critères Communs version 2.2
  - Niveau:EAL2+
  - Augmentations: ADV_HLD.2, ADV_LLD.1*, ADV_IMP.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1*, AVA_MSU.1 et AVA_VLA.2

  - **Arkoon Fast Firewall V3.0/11**
  - Rapport de certification 2004/33
  - Référentiel: Critères Communs version 2.1
  - Niveau: EAL2+

  - Augmentations: ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1, AVA_VLA.2
- Commutateurs :
  - **Cisco Catalyst Switches** (2900, 3500, 3700, 4500, 4948, 6500)
  - Validation Report Number: CCEVS-VR-VID6012-2008
  - Date Issued: 27 May 2008
  - Assurance Level: EAL 3 Augmented ALC_FLR.1Protection
- Annuaire :
  - **Microsoft Windows Serveur 2003** (incluant Active Directory)
  - Certificate Date: 01 April 2007
  - Validation Report Number: CCEVS-VR-07-0023
  - Conformance Claim: EAL4 Augmented with ALC_FLR.3, AVA_VLA.4

3.6 Description des utilisateurs typiques concernés.

Cette section présente les différentes catégories d'utilisateur du produit UCOPIA et leur rôle respectif.

- **Administrateur**
  Administrateur disposant de droits complets sur la configuration des boîtiers appliances UCOPIA, seul habilité à s'y connecter, et ne devant accomplir les tâches d'administration qu'en dehors des phases d'exploitation (i.e. installation ou maintenance).
  L'administrateur est en charge des opérations :
  - d'administration (configuration, définition de profils utilisateurs, ajout de comptes utilisateurs, définition des profils des administrateurs délégués, etc.)
  - d'exploitation et de maintenance (installation du produit, installation des mises à jour, définition des politiques de sauvegarde des journaux, remplacement de l'appliance UCOPIA en cas de panne, etc.)
  - de supervision (surveillance des événements d'audit, surveillance des alarmes).

- **Administrateur délégué**
  Personnel habilité à effectuer certaines opérations d'administration et responsable de leur exécution correcte.
  Les opérations autorisées pour un administrateur délégué sont les suivantes :
  - Création/destruction/modification de comptes utilisateurs (individuellement ou en masse). Lors de la création de compte l'administrateur délégué ne peut pas modifier les droits d'accès définis par l'administrateur.
  - Création de tickets de connexion (à transmettre à l'utilisateur final) résumant les identifiants de connexion de l'utilisateur final ainsi que ses conditions de connexion.

- **Mainteneur**
  Personne assurant la maintenance du produit (intervention physique sur le produit, remplacement, ouverture du tunnel de maintenance). Ce rôle est assuré par l'administrateur.

- **Télémainteneur**
  Personnel habilité à effectuer des opérations de maintenance à distance sur un contrôleur

UCOPIA. Le télémainteneur est la personne en charge du bon fonctionnement de la solution, que ce soit l'intégrateur réseau, ou le support technique UCOPIA.

- **Auditeur**
  Personne en charge de la surveillance des événements d'audit sur le produit. Ce rôle est assuré par l'administrateur.

- **Responsable Sécurité**
  Personne en charge des alarmes et des actions qui en découlent. Ce rôle est assuré par l'administrateur.

- **Utilisateur final**
  Personne utilisant le produit UCOPIA à partir de réseaux maîtrisés ou non maîtrisés pour accéder à des ressources d'un réseau de confiance protégé par UCOPIA. Un utilisateur final correspond à toute personne en possession d'identifiants valides qui se connecte au réseau via UCOPIA.

3.7 Définition du périmètre de l'évaluation.

Toutes les fonctionnalités de sécurité (authentification, filtrage, cloisonnement VLAN, traçabilité), fonctions d'administration et téléchargement des nouvelles versions de produits appartiennent au périmètre de la cible d'évaluation.

L'architecture de la plate-forme d'évaluation est présentée par le schéma ci-dessous.

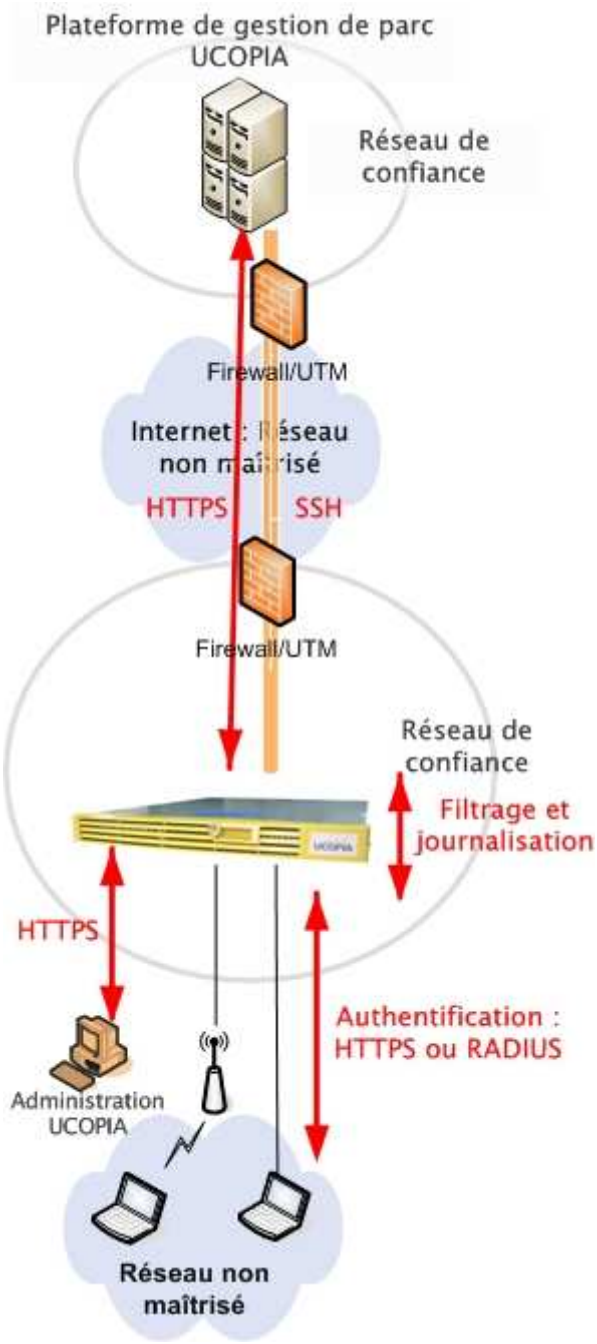

Figure 3 : Architecture physique de la plate-forme d'évaluation

4 Environnement technique de fonctionnement du produit

Le produit UCOPIA est composé d'un logiciel embarqué dans une appliance matérielle. Cette appliance doit être en coupure réseau grâce à ces deux cartes Ethernet (IN et OUT).

5 Biens sensibles devant être protégés par le produit

5.1 Biens protégés par le produit UCOPIA

Les biens sensibles protégés par le produit UCOPIA sont les suivants :

- **BP1** : Les services proposés par des serveurs du réseau de confiance. L'accès aux serveurs est contrôlé par les politiques de contrôle des flux.

- **BP2** : Les ressources se trouvant sur les équipements du réseau de confiance. L'accès aux équipements est contrôlé par les politiques de contrôle des flux.

- **BP3** : Les informations de topologie du réseau contre des tentatives de sondage basées sur une utilisation des protocoles Internet contraires aux bonnes pratiques (confidentialité).

5.2 Biens appartenant au produit UCOPIA

- **BA1** : Les paramètres de configuration du produit UCOPIA.
  Ces paramètres vont définir les informations réseau :
  - configuration du nom du contrôleur,
  - configuration des VLANs d'entrée et de sortie,
  - configuration du serveur de temps,
  - configuration des routes statiques,
  - DNS,

  ainsi que les informations permettant d'interagir avec des produits tiers du réseau de confiance (exemple : adresse IP et numéro de port d'un serveur LDAP).
  Les paramètres sont stockés dans des fichiers de configuration sur le contrôleur UCOPIA.
  Les paramètres ne doivent pouvoir ni être lus, ni modifiés, ni détruits (intégrité, confidentialité, disponibilité).

- **BA2** : Les données d'authentification des administrateurs et des utilisateurs. Ces données sont stockées dans l'annuaire LDAP interne au produit UCOPIA (intégrité, confidentialité, disponibilité).

- **BA3** : Les politiques de contrôle des flux implémentées par le produit UCOPIA. Ces politiques correspondent aux droits d'accès aux services du réseau. Les politiques d'accès s'appliquent à chaque utilisateur et sont stockées dans l'annuaire LDAP interne au produit UCOPIA (intégrité, confidentialité, disponibilité).

- **BA4** : Les enregistrements d'événements de sécurité du produit UCOPIA. Ces événements sont enregistrés dans un fichier syslog (intégrité, confidentialité).

- **BA5** : Les certificats qui sont utilisés pour l'authentification par portail (SSH), l'authentification RADIUS et également pour la mise en œuvre du tunnel de télémaintenance (SSH). (intégrité, confidentialité, disponibilité).

- **BA6** : Les clés de chiffrement utilisées pour chiffrer les fichiers de mises à jour et pour le tunnel de maintenance (intégrité, confidentialité, disponibilité)

- **BA7** : Les mises à jour qui sont téléchargées sur le boîtier UCOPIA (intégrité, confidentialité, disponibilité).

- **BA8** : Les journaux UCOPIA assurant la traçabilité des connexions des utilisateurs. Ces journaux sont enregistrés dans une base de données SQL (intégrité, confidentialité, disponibilité).

6 Description des menaces

6.1 Menaces relatives au contrôle d'accès d'un utilisateur

- **M1 :** Une entité non-autorisée sur le réseau non maîtrisé contourne la politique de contrôle des flux d'informations en contrefaisant l'adresse IP source et l'adresse MAC des paquets qu'il émet afin d'usurper l'identité d'une entité d'un réseau autorisé. L'ensemble des biens protégés par le produit est impacté. La menace vient d'une personne malveillante. Une méthode d'attaque pourrait être du type « ARP spoofing ».

- **M2-a :** Une entité non-autorisée sur le réseau non maîtrisé parvient à accéder aux services et ressources réservés à un utilisateur soumis à une authentification obligatoire en usurpant son identité en rejouant une séquence d'authentification légitime basée sur des données réutilisables qu'elle a interceptée. Tous les biens protégés par le produit sont menacés. La menace vient d'une personne malveillante. Une méthode d'attaque consisterait à subtiliser le cookie de session d'un utilisateur connecté.

- **M2-b :** Une entité non-autorisée sur le réseau non maîtrisé parvient à accéder aux services et ressources réservés à un utilisateur soumis à une authentification obligatoire en usurpant son identité en devinant les données d'authentification de l'utilisateur suite à des tentatives aléatoires répétées. Tous les biens protégés par le produit sont menacés. La menace vient d'une personne malveillante. Une méthode d'attaque pourrait être de type « Force Brute » sur le portail d'authentification.

- **M2-c :** Une entité non-autorisée sur le réseau non maîtrisé parvient à accéder aux services et ressources réservés à un utilisateur soumis à une authentification obligatoire en usurpant son identité en devinant les données d'authentification de l'utilisateur par le biais d'analyses de séquences d'authentification interceptées. Tous les biens protégés par le produit sont menacés. La menace vient d'une personne malveillante. Une méthode d'attaque pourrait être de « casser » le cryptage SSL entre le portail d'authentification et l'appliance UCOPIA.

- **M2-d :** Une entité non-autorisée sur le réseau non maîtrisé parvient à accéder aux services et ressources réservés à un utilisateur soumis à une authentification obligatoire en usurpant son identité en accédant illégitimement aux données stockées dans l'appliance permettant l'authentification des utilisateurs. Tous les biens protégés par le produit sont menacés. La menace vient d'une personne malveillante. Cette menace nécessite l'accès en tant qu'administrateur et donc renvoie aux menaces en ce qui concerne les méthodes

d'attaque.

6.2 Menaces relatives à l'administration

- **M3 :** Un attaquant ou une entité non-autorisée parvient à effectuer des opérations d'administration ou administration déléguée illicites. Les biens menacés sont tous les biens protégés par le produit et les biens appartenant au produit BA1 à BA5. La menace vient d'une personne malveillante. Une méthode d'attaque pourrait être la récupération du mot de passe de l'outil d'administration (ou administration déléguée), par attaque de type « Brut Force » sur la page Web d'authentification des outils concernés.

- **M4 :** Une entité non-autorisée lit, modifie ou supprime le contenu d'une session d'administration ou administration déléguée établie entre l'appliance UCOPIA et une station d'administration à distance pour le compte d'un administrateur. Les biens menacés sont tous les biens protégés par le produit et les biens appartenant au produit BA1 à BA5. La menace vient d'une personne malveillante. Une méthode d'attaque pourrait être la subtilisation de sessions par vol de cookie de session sur le poste de l'administrateur.

6.3 Menaces relatives aux journaux

- **M5 :** Une entité non-autorisée empêche l'enregistrement d'événements de sécurité et des journaux utilisateurs en épuisant la capacité de stockage de l'appliance UCOPIA de ces événements, dans le but de masquer les actions illicites d'un attaquant. Les biens BA4 et BA8 sont menacés. La menace vient d'une personne malveillante. Une méthode d'attaque pourrait être de générer suffisamment de trafic HTTP pour remplir le disque avec la journalisation du trafic Web.

- **M6 :** Une entité non-autorisée lit, modifie ou supprime le contenu des journaux de sessions et de trafic des utilisateurs. Les biens menacés sont BA8. Un exemple d'attaque pourrait être par technique d'injection SQL à travers les paramètres envoyés depuis l'IHM. La menace vient d'une personne malveillante.

6.4 Menaces relatives à la télémaintenance

- **M7** : Une entité non-autorisée modifie ou supprime le contenu d'une session de télémaintenance établie entre l'appliance UCOPIA et le serveur de gestion UCOPIA. La menace vient d'une personne malveillante. Tous les biens protégés et appartenant à la cible sont menacés. Une attaque consisterait à se procurer les clés publique et privée présentes sur un contrôleur pour accéder à la machine de support.

7 Description des fonctions de sécurité du produit

Les fonctions de sécurité de l'appliance UCOPIA sont les suivantes :

7.1 Authentification

UCOPIA propose plusieurs modes d'authentification, allant d'une authentification forte basée sur le protocole 802.1x/EAP jusqu'à une authentification souple de type portail Web captif basée sur HTTPS. 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.

7.1.1 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. Ce type d'authentification permet de fournir une authentification mutuelle de l'utilisateur et du serveur d'authentification. Elle requiert cependant la gestion d'une PKI sur chaque terminal utilisateur.

7.1.2 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. En effet, un serveur RADIUS est embarqué dans le contrôleur UCOPIA permettant de jouer le rôle du serveur d'authentification de l'architecture 802.1x.

7.1.3 Authentification depuis le portail Web captif UCOPIA

L'utilisateur, à l'ouverture de son navigateur Web, se voit automatiquement redirigé vers une page Web d'authentification hébergée par le contrôleur UCOPIA. Celle-ci 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. Tant que cette fenêtre reste ouverte (et que la validité du compte n'expire pas) la connexion reste active. UCOPIA renforce la sécurité pour ce mode d'authentification en proposant une authentification qui est rejouée périodiquement et ce de façon transparente pour l'utilisateur. De plus, le même login/mot de passe ne peut pas être utilisé pour deux connexions simultanées.

7.1.4 Génération des mots de passe utilisateur

Les mots de passe utilisateur sont créés soit via l'outil d'administration soit via l'outil d'administration déléguée. Via l'outil d'administration, l'administrateur doit mettre en place une politique de création de ceux-ci (par exemple, mélange alphanumérique, longueur minimum, ajout de caractères spéciaux, pas de mots de dictionnaires usuels, etc.). Via l'outil d'administration les mots de passe des utilisateurs sont générés automatiquement (8 caractères aléatoires alpha-numériques).

7.2 Contrôle d'accès par filtrage de flux

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 est placé en position de coupure réseau et utilise un mécanisme de filtrage de trafic basé sur des règles. Celles-ci sont automatiquement déduites à partir du profil de l'utilisateur et du contexte de connexion de l'utilisateur (notamment

le temps et lieu de connexion). 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.

7.3 Cloisonnement 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. A titre d'exemple, considérons le cas d'un déploiement Wi-Fi classique. A chaque SSID configuré sur les points d'accès Wi-Fi est associé un VLAN, ces VLANs se retrouvent en entrée du boîtier UCOPIA. Le contrôleur UCOPIA gére chacun des VLANs comme un réseau différent : adressage IP, routage, etc …
Par ailleurs, en fonction de son profil, le flux d'un utilisateur pourra être réinjecté en sortie du boîtier UCOPIA dans un VLAN particulier afin d'isoler les flux. Par exemple, les visiteurs sur le VLAN Internet et les employés sur le LAN d'entreprise. La figure suivante illustre une architecture possible pour ce type de déploiement, où les différents cloisonnements de trafic sont réalisés à l'aide d'un unique équipement.

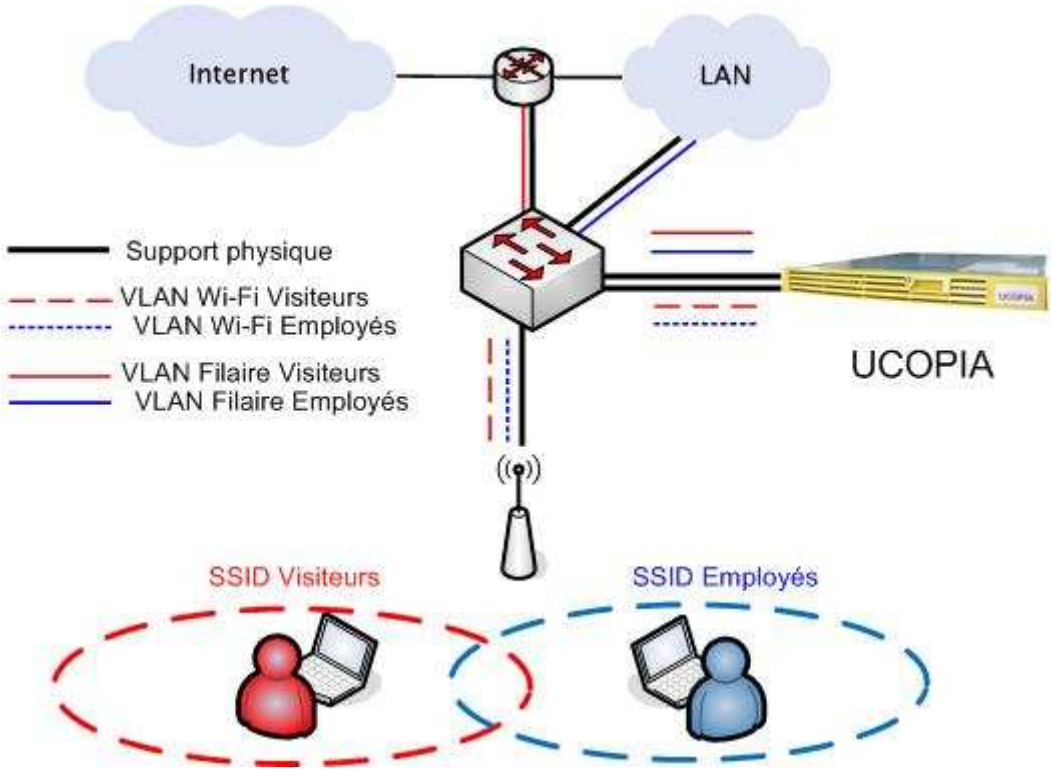

Figure 4: Cloisonnement par VLAN

L'utilisation de VLAN permet de cloisonner le trafic d'une façon logique. Les équipements implémentant la norme 802.1q de l'IEEE sont capables de détecter/ajouter/modifier des tags ou labels VLAN se situant dans une trame Ethernet. Différentes applications sont possibles comme :

- Relayer les trames Ethernet uniquement sur un sous-ensemble de ports physiques (ceux

possédant le même label). Il est ainsi possible de segmenter un même équipement matériel de commutation niveau 2 en plusieurs réseaux distincts. Un commutateur possédera alors 4 ports physiques dédiés à un VLAN 1, et 4 autres ports physiques dédiés à un VLAN 2.

- Relayer des trames avec différents labels VLAN sur le même port physique : cela correspond au mode « Trunk ». Différents sous réseaux seront alors véhiculés sur le même support physique mais pourront être différencié comme deux réseaux indépendants.

Dans le cas du déploiement précédemment cité, le premier cas correspond par exemple à un cloisonnement de trafic physique : le trafic des visiteurs peut être injecté sur un port physique différent de celui des employés.
Le mode « Trunk » est typiquement utilisé dans les environnements Wi-Fi, où chaque borne possède plusieurs SSID, correspondant à un VLAN. Le même support physique transporte les différents VLAN jusqu'au contrôleur UCOPIA.

Dans le cas d'un cloisonnement par VLAN apportant un élément de sécurité architectural, il est important de vérifier la conformité des équipements. Des certifications de ces matériels réseaux existent et permettant d'assurer un niveau de conformité de ces éléments clés. A titre d'exemple, le rapport de validation CCEVS-VR-VID6012-2008 du NIAP-CCEVS offre un niveau de certification EAL3 augmentée de ALC_FLR.1 (http://www.niap-ccevs.org/cc-scheme/st/vid6012/).
Dans le cas contraire, il est important de noter que toute architecture réseau incluant des VLAN, que ce soit une architecture incluant UCOPIA ou non, peut également être déployée sans VLAN, à condition de disposer de suffisamment d'équipements réseaux.

7.4 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). L'ensemble de ces informations pourra être utilisé à des fins de statistiques et/ou de sécurité. **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).**

Les journaux de sessions et de trafic sont crées localement sur le boîtier UCOPIA et sont accessibles depuis l'outil d'administration UCOPIA. Les journaux peuvent être exportés, manuellement ou automatiquement (via FTPS), vers une machine tierce.

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 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 nom de société, numéro de carte d'identité.

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

D'autres journaux sont également créés dans le boitier UCOPIA mais ne sont pas en rapport avec la traçabilité des utilisateurs et du trafic généré. Il s'agit des journaux systèmes, permettant de tracer l'activité des différents modules UCOPIA lors de l'exploitation du produit. Ces journaux systèmes ne sont pas accessibles pour l'administrateur mais uniquement pour le télémaineneur.

7.5 Principe de fonctionnement

Cette Section décrit les flux entre un utilisateur, UCOPIA et l'environnement protégé par UCOPIA. L'appliance UCOPIA est en coupure logique (ou physique) entre le réseau d'accueil (Wi-Fi et/ou filaire) sur lequel se trouve l'utilisateur et le LAN de l'entreprise (réseau de confiance).

Le principe de fonctionnement est le suivant.

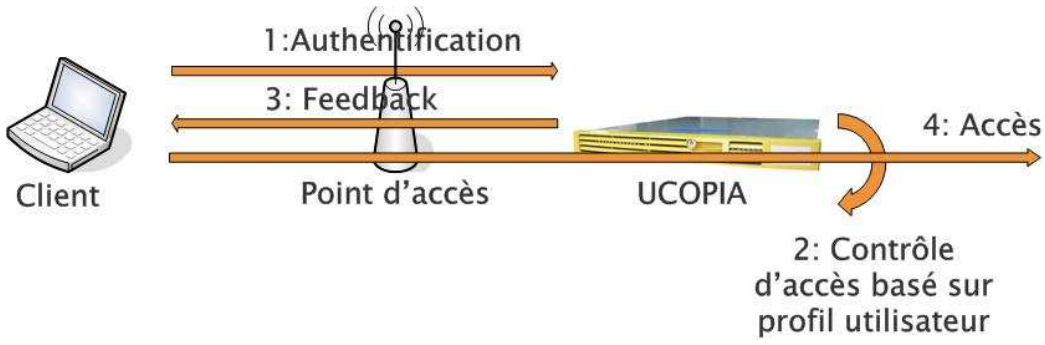

Figure 5: Flux pour le contrôle d'accès

L'utilisateur s'authentifie en utilisant une des deux familles d'authentification UCOPIA (802.1x/EAP ou portail d'authentification captif), UCOPIA vérifie que l'utilisateur est habilité à se connecter et applique ses droits. Le contrôle d'accès est basé sur la notion de profil utilisateur proposé par UCOPIA.

Les Sections suivantes détaillent les flux d'authentification pour les deux familles.

7.5.1 Authentification par protocole 802.1x/EAP

Le 802.1x, ou Port Based Access Control, permet un contrôle d'accès par port. Le trafic arrivant sur un port du NAS (Network Access Point : un commutateur ou un point d'accès sans fil) est bloqué par défaut. Pour que le NAS, ou Authenticator, accepte le passage du trafic, le client doit d'abord s'authentifier ce qui débloquera le port sur lequel il est connecté.
L'authentification est réalisé entre le client, ou supplicant, et un serveur d'authentification, le plus souvent RADIUS (RFC 2865). Le protocole RADIUS permet le transport de protocoles d'authentification tels que PAP, CHAP ou EAP. Le protocole EAP (Extensible Authentication

Protocol) permet le transport de n'importe quelle méthode d'authentification. La figure suivante illustre l'échange de message 802.1x dans le cadre de la norme IEEE 802.11i, amendement de sécurité du Wi-Fi.

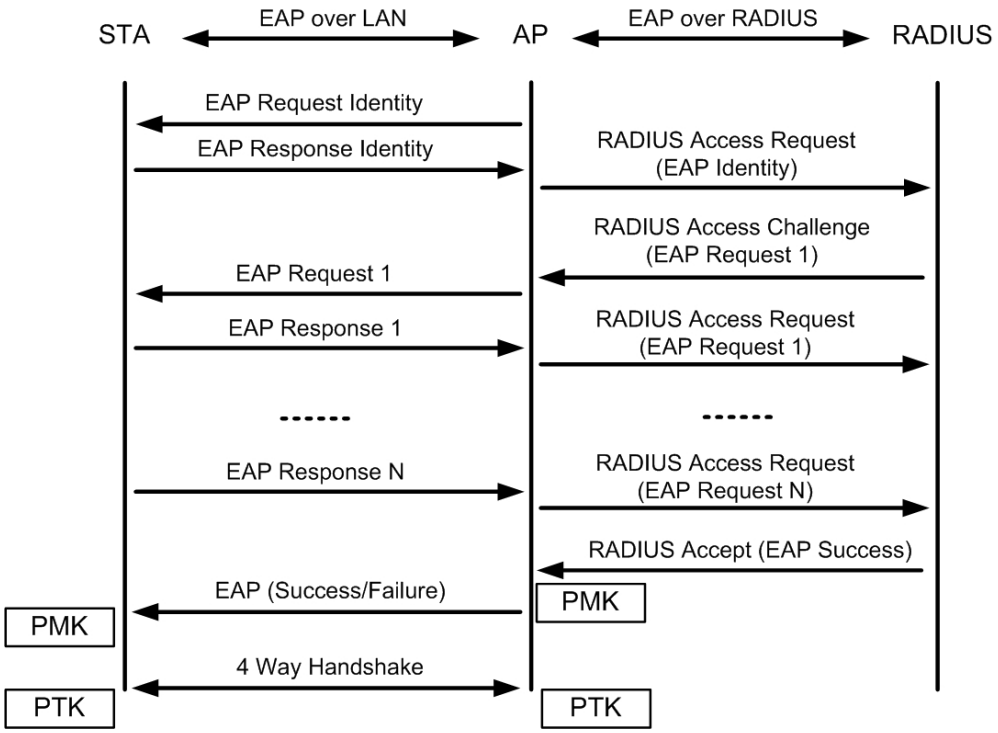

Figure 6: Authentification 802.1x dans la norme 802.11i

UCOPIA embarque un serveur RADIUS et est compatible avec les solutions EAP suivantes :

- **EAP-TLS (Transport Layer Security):** Proposée par Microsoft et accepté comme standard de l'IETF , RFC 5216, EAP-TLS est la seule méthode EAP obligatoire pour obtenir le label WPA/WPA2. Elle permet une authentification mutuelle entre le client et le serveur basée sur l'utilisation de certificats X.509. Le certificat client, qui contient l'identité de l'utilisateur, et le certificat serveur sont issus d'une autorité de certification de confiance, permettant ainsi une authentification mutuelle.

  UCOPIA permet l'utilisation d'un certificat serveur et d'un certificat d'autorité de certification existants, mais n'offre pas de fonctionnalité de gestion d'infrastructure de clés publiques ou PKI. Un certificat client par terminal doit être déployé, ce qui peut engendrer des coûts de gestion conséquents. Des solutions sans certificats clients, telles que PEAP ou TTLS, ont été crées par la suite pour contourner cette contrainte.

- **EAP-PEAP (Protected EAP) :** Solution proposée par Microsoft, RSA et Cisco Systems. Cette solution utilise généralement la version PEAPv0, définie dans le draft « draft-kamath-pppext-peapv0-00.txt », qui consiste à encapsuler une méthode d'authentification dans un tunnel TLS.

  UCOPIA utilise la méthode PEAPv0/MS-CHAPv2. MS-CHAPv2 utilise un couple login / mot de passe (utilisateur et/ou machine). Le principe consiste à :

- Authentifier le serveur par validation TLS du certificat serveur
- Créer un tunnel SSL/TLS encrypté entre le supplicant et le serveur RADIUS
- La méthode d'authentification MS-CHAPv2 est alors réalisée. Elle est basée sur une authentification mutuelle du client et du server par l'utilisation respective de fonction de hachage de challenge aléatoire, avec comme clé le password du client.

La méthode d'authentification MS-CHAPv2 est répandue dans les environnements Microsoft et l'authentification PEAP/MS-CHAPv2 est généralement utilisée avec un annuaire Active Directory. Avec le système d'exploitation Vista, l'ancienne méthode MS-CHAPv1 est abandonnée et seule MS-CHAPv2 est utilisable.

- **EAP-TTLS (Tunneled TLS) :** Solution co-développée par Funk Software et Certicom**,** EAP-TTLS est décrit dans la RFC 5281. Cette solution a un fonctionnement similaire à celui de PEAP : un tunnel chiffré SSL/TLS est créé après la validation du certificat serveur et permet l'encapsulation chiffrée de différentes méthodes d'authentification : CHAP, PAP, MS-CHAP, MS-CHAPv2 ou une méthode EAP. UCOPIA utilise une des méthodes parmi les plus courantes, souvent implémentée dans les systèmes d'exploitation ou par installation de logiciel sur le supplicant : TTLS/PAP.
  La méthode PAP (Password Authentication protocol), utilisée notamment par PPP (Point to Point Protocol), consiste en un envoi en clair du login et du mot de passe. Le tunnel TLS permet de sécuriser l'échange de données.

Le principe du protocole d'authentification 802.1x/EAP dans le cas d'une infrastructure Wi-Fi gérée par UCOPIA est le suivant :

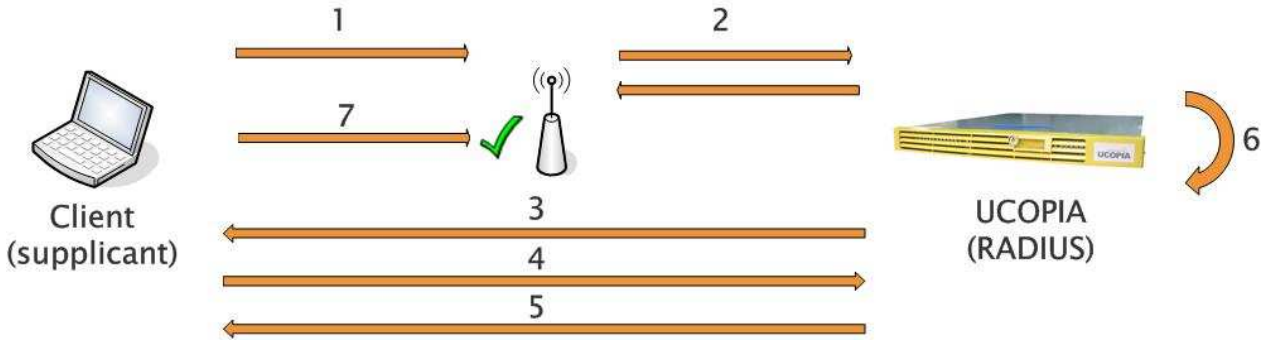

Figure 7: Flux d'authenfication EAP

1. Le client envoie une requête d'authentification EAP
2. Le point d'accès relaye la requête d'authentification EAP
3. Le serveur RADIUS envoie un défi au supplicant
4. Le supplicant répond au défi en utilisant une méthode EAP spécifique (PEAP/TTLS…)
5. Le serveur RADIUS fournit une clé de session au supplicant
6. Le serveur RADIUS envoie une requête au gestionnaire de sécurité UCOPIA qui va procéder aux vérifications concernant le profil utilisateur (validité du compte, crédit temps, zones d'entrée et de sortie…)
7. Une fois le supplicant authentifié, le point d'accès autorise celui-ci à communiquer avec le réseau

7.5.2 Authentification par portail Web

Le principe du protocole d'authentification par portail captif UCOPIA dans le cas d'une infrastructure Wi-Fi est le suivant.

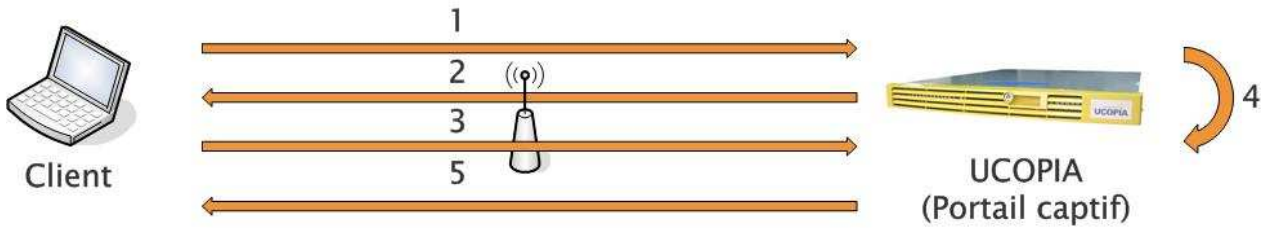

Figure 8: Flux d'authentification par portail captif

1. Le client demande l'accès à une URL (exemple : www.google.fr) depuis son navigateur Internet.
2. Le boitier UCOPIA identifie une demande de type Web, provenant d'un utilisateur inconnu, et renvoie la requête vers le portail d'authentification UCOPIA. Cette redirection est automatiquement faite en HTTPS afin de sécuriser les échanges. Lorsque la requête est valide et ne nécessite pas une redirection (URL du portail valide, au lieu d'une requête vers www.google.fr), le type de protocole est vérifié. Dans le cas d'une requête HTTP, la redirection est forcée vers le portail en HTTPS. Le portail d'authentification UCOPIA n'est donc accessible qu'avec un protocole HTTPS.
3. Le client envoie une demande d'authentification avec un couple login/mot de passe via l'interface sécurisée du portail d'authentification
4. Le module interne du portail d'authentification UCOPIA envoie une requête au gestionnaire de sécurité UCOPIA qui va procéder aux vérifications concernant le profil utilisateur (validité du compte, crédit temps, zones d'entrée et de sortie…). Le gestionnaire de sécurité vérifie non seulement l'identité de l'utilisateur (authentification simple) mais également la conformité des autres paramètres de validité propre à UCOPIA: heure de connexion, zone de connexion. En cas de succès, le gestionnaire de sécurité calcule dynamiquement les paramètres réseaux de l'utilisateur.
5. En fonction du résultat obtenu par le gestionnaire de sécurité, UCOPIA envoie un feedback à l'utilisateur pour l'informer de ses droits (services autorisés, plages horaires, crédit temps) ou bien de la raison de l'échec de l'authentification

La sécurité des échanges entre le terminal utilisateur et le portail d'authentification repose sur l'usage du protocole HTTPS. La solution UCOPIA utilise un certificat serveur issu d'une autorité de certification tierce afin de sécuriser ces échanges en permettant :

- l'authentification de la validité du certificat par le navigateur Web du terminal utilisateur
- le chiffrement des échanges avec un cipher possédant un niveau de sécurité suffisant (par configuration des ciphers autorisés sur le serveur web UCOPIA)

Le certificat serveur est issu d'une autorité de certification reconnue et incluse par défaut dans la plupart des navigateurs des systèmes d'exploitation du marché. Tant que le certificat serveur est valide, le navigateur valide automatiquement celui-ci. Dans le cas contraire, un message d'avertissement sera affiché par le navigateur du client.

Il est important de noter que ce mode ne représente pas le mode d'authentification le plus sécurisé proposé par UCOPIA : il s'agit d'une alternative permettant un niveau de sécurité suffisant pour

l'accueil de visiteurs, sans avoir à gérer un certificat client par poste.
L'utilisation de PKI (avec certificats serveur, clients et un certificat CA) reste possible afin d'augmenter le niveau de sécurité. Comme dans le cadre d'une authentification EAP/TLS, le boîtier UCOPIA permet l'usage de ses propres couples de certificats par configuration, à effectuer par l'administrateur.

8 Architecture du produit

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

Trois composants principaux constituent le boîtier 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'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).

- **La télémaintenance** permet de maintenir en état de bon fonctionnement le boîtier UCOPIA. La télémaintenance permet le téléchargement de patch, permettant de faire évoluer la version logicielle du boîtier. Elle permet également d'intervenir à distance sur un boîtier à des fins de support technique.

L'ensemble du trafic en provenance des utilisateurs est redirigé vers l'appliance UCOPIA qui est en coupure logique (ou physique) entre un réseau d'accueil (Wi-Fi et/ou filaire) et le LAN de l'entreprise (réseau de confiance). Les protocoles d'authentification entre les postes des utilisateurs et l'appliance UCOPIA sont soit 802.1x/EAP/RADIUS ou HTTPS. Les modules d'authentification d'UCOPIA 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 boîtier UCOPIA est basé sur une architecture Linux distribution Mandriva 2009.

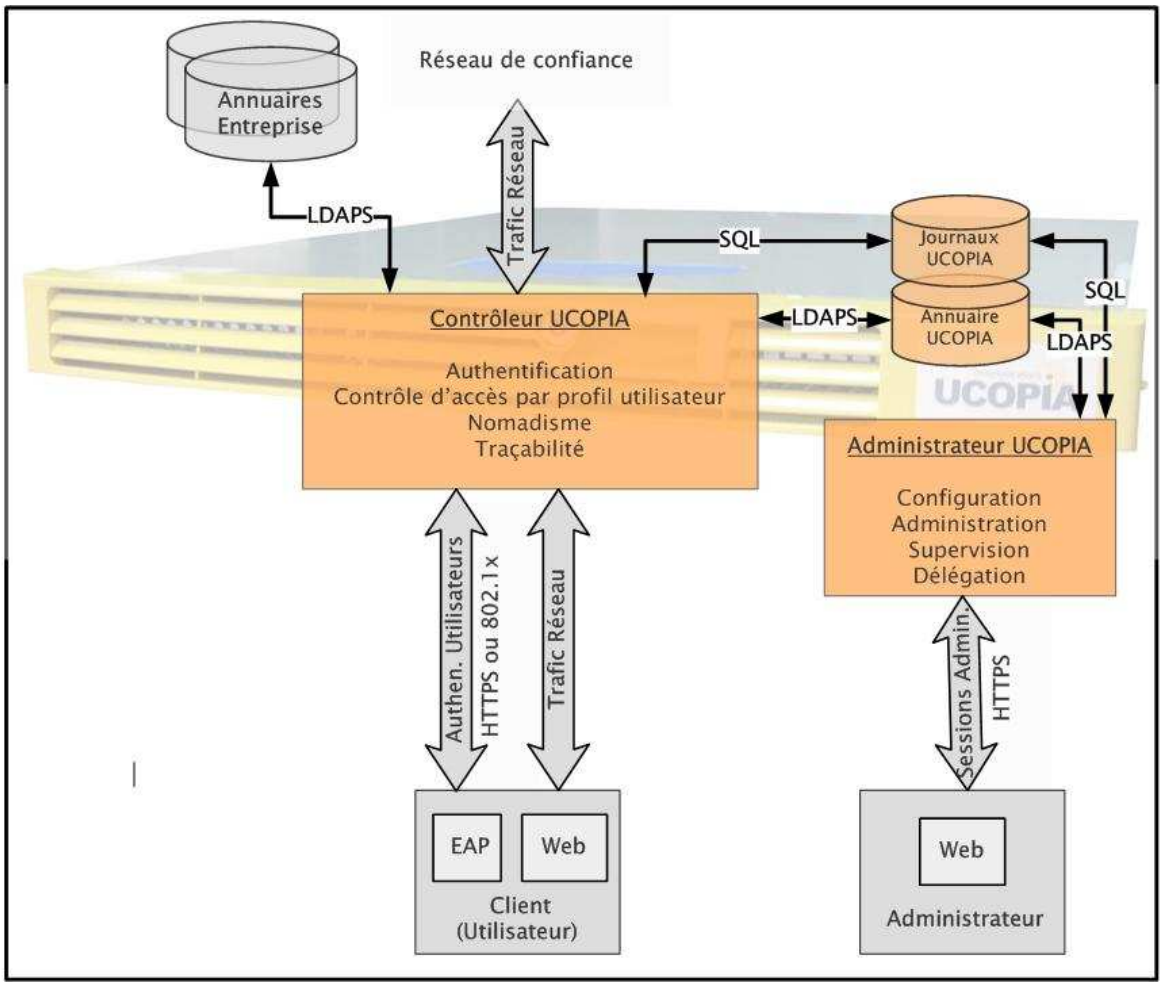

Figure 9: Architecture globale UCOPIA

8.1 Le 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 et de l'accès transparent aux services. Le module « **Gestionnaire de Sécurité et de Mobilité** » orchestre l'ensemble des modules.

La figure ci-dessous résume l'architecture du contrôleur UCOPIA, l'ensemble des modules nécessaires à son fonctionnement est décrit.

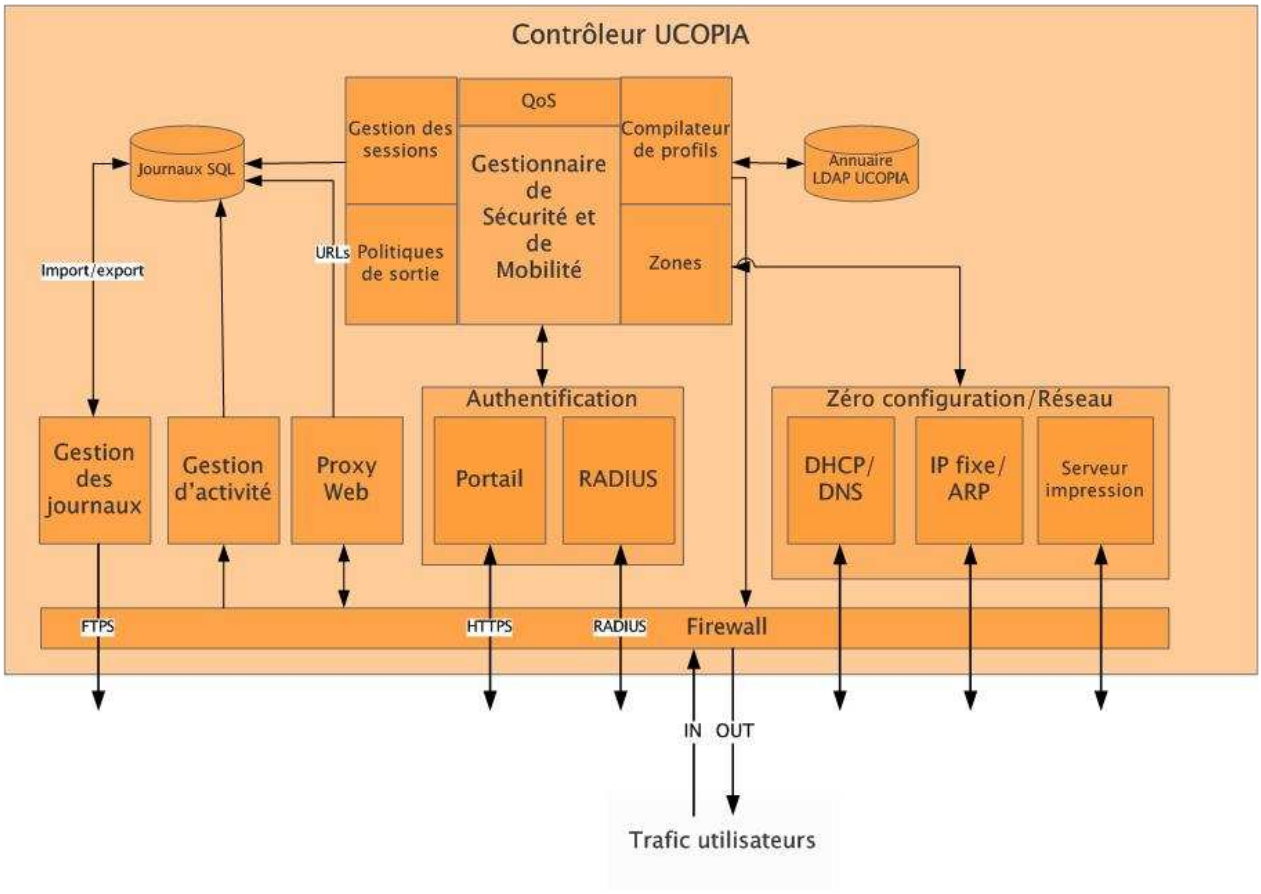

Figure 10: Architecture du contrôleur UCOPIA

Le contrôleur est basé sur une technologie de filtrage qui permet de filtrer et de classifier les paquets afin de mettre en œuvre respectivement le contrôle d'accès par profil utilisateur et la qualité de service (module « **Firewall** »). Le filtrage assure également la détection des flux correspondant à des configurations erronées. Le filtrage est de niveau 2 à 4 et se base sur les adresses IP des utilisateurs mais aussi sur les adresses MAC, les numéros de ports, les types de protocoles, etc. L'implémentation du module Firewall est réalisée au niveau Linux par le package IPTables.

- **Authentification**: le contrôleur embarque un serveur **RADIUS** (FreeRadius) 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,** basé sur le serveur Web Apache, 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 (OpenLDAP) et le compile en règles de filtrage qu'il installe dynamiquement au niveau du module « **Firewall** ». Ces règles sont retirées lorsque l'utilisateur se déconnecte. Le profil détermine également en fonction de la zone de connexion si l'utilisateur est habilité à se

connecter (module « **Zones** »). Nous rappelons que le profil peut être multiple pour un même utilisateur (fonction du lieu et du temps).

- **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'attentes afin de mettre en oeuvre la gestion de priorités.

- **Accès transparent** : Le module « **Zéro Configuration** » 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 : serveur mail ou proxy Web) soit de la mise à disposition automatique et transparente de composants nécessaires à l'exécution du service. (par exemple, driver d'imprimante). Pour réaliser la mise à disposition de drivers 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.

- **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 (MySQL) : le module '**Gestion des sessions** » enregistre les sessions des utilisateurs (login, nom, prénom, @IP, @Mac, etc.), le module « **Gestion d'activité** » enregistre le trafic des utilisateurs (entêtes de paquets IP), le module « **Proxy Web** » enregistre les URLs accédées par les utilisateurs. Le module « **Gestion des Journaux** » permet d'exporter les sauvegardes des journaux via le protocole FTPS.

8.2 L'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 et les fonctions de délégation.

Les interfaces d'administration sont essentiellement Web, l'architecture est par conséquent basée sur le serveur Web Apache. Il s'agit du même serveur qui est utilisé pour implémenter le portail d'authentification des utilisateurs.

L'outil d'administration permet de configurer les interfaces réseaux, physiques ou virtuelles, permettant l'accès à l'outil d'administration et au portail de délégation. Il est donc recommandé de restreindre l'accès à ces outils à un sous réseau d'administration, indépendant des sous réseaux

d'authentification, ou réseaux non maîtrisés.

Le schéma ci-dessous présente l'architecture de l'administration UCOPIA.

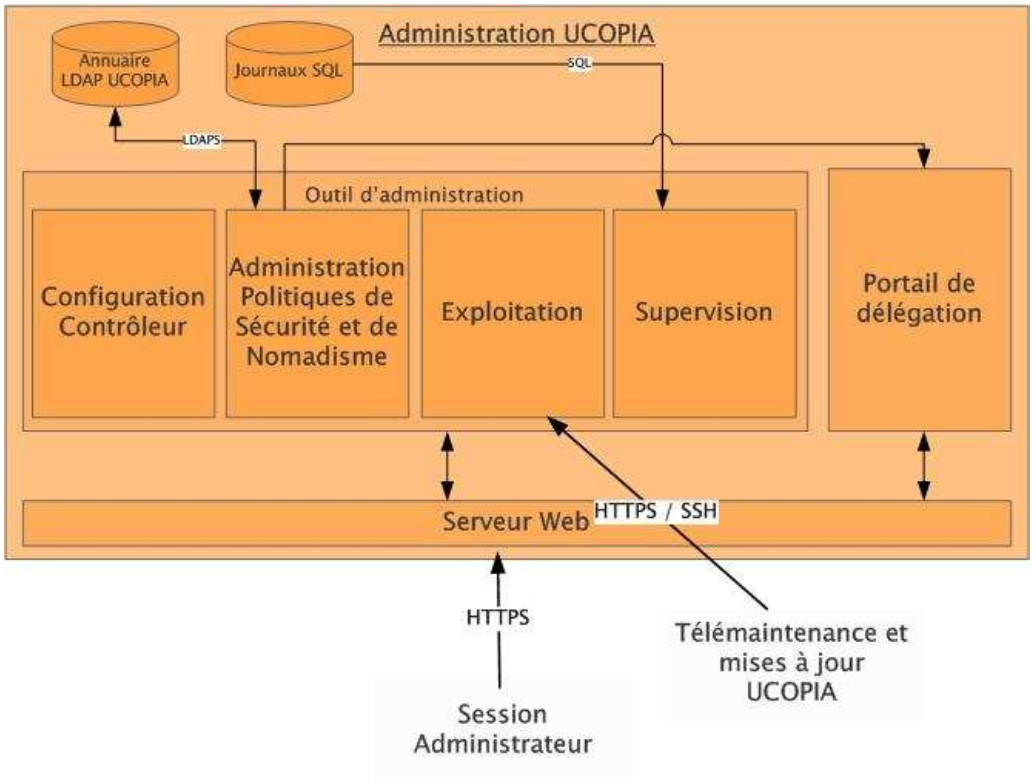

Figure 11: Architecture des outils d'administration UCOPIA

- **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 nomadisme** : 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 (MySQL). 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, mise à jour du boîtier UCOPIA avec les nouvelles Releases UCOPIA, télémaintenance, etc. Les sauvegardes sont au format archive (.tar) compressée, les Releases doivent être téléchargées depuis le site Extranet UCOPIA, la télémaintenance est assurée par un tunnel SSH qui s'établie depuis le boîtier UCOPIA vers les serveurs de maintenance UCOPIA.

- **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.

8.3 Télémaintenance de l'appliance UCOPIA

UCOPIA propose un service de mise à dispositions des patchs et releases pour la mise à jour des appliances ainsi qu'un service de télémaintenance.
Ce service est proposé via une plate-forme centrale de gestion du parc d'appliances UCOPIA hébergée par UCOPIA.

A travers cette plate-forme, une appliance UCOPIA peut :

1. Installer automatiquement sa licence (HTTPS)
2. Télécharger les mises à jour (HTTPS)
3. Télécharger et installer les mises à jour dîtes critiques (ex : faille de sécurité) (HTTPS)
4. Ouvrir un tunnel de maintenance (HTTPS + SSH)

L'architecture de la plate-forme de gestion de parc d'appliances UCOPIA est la suivante :

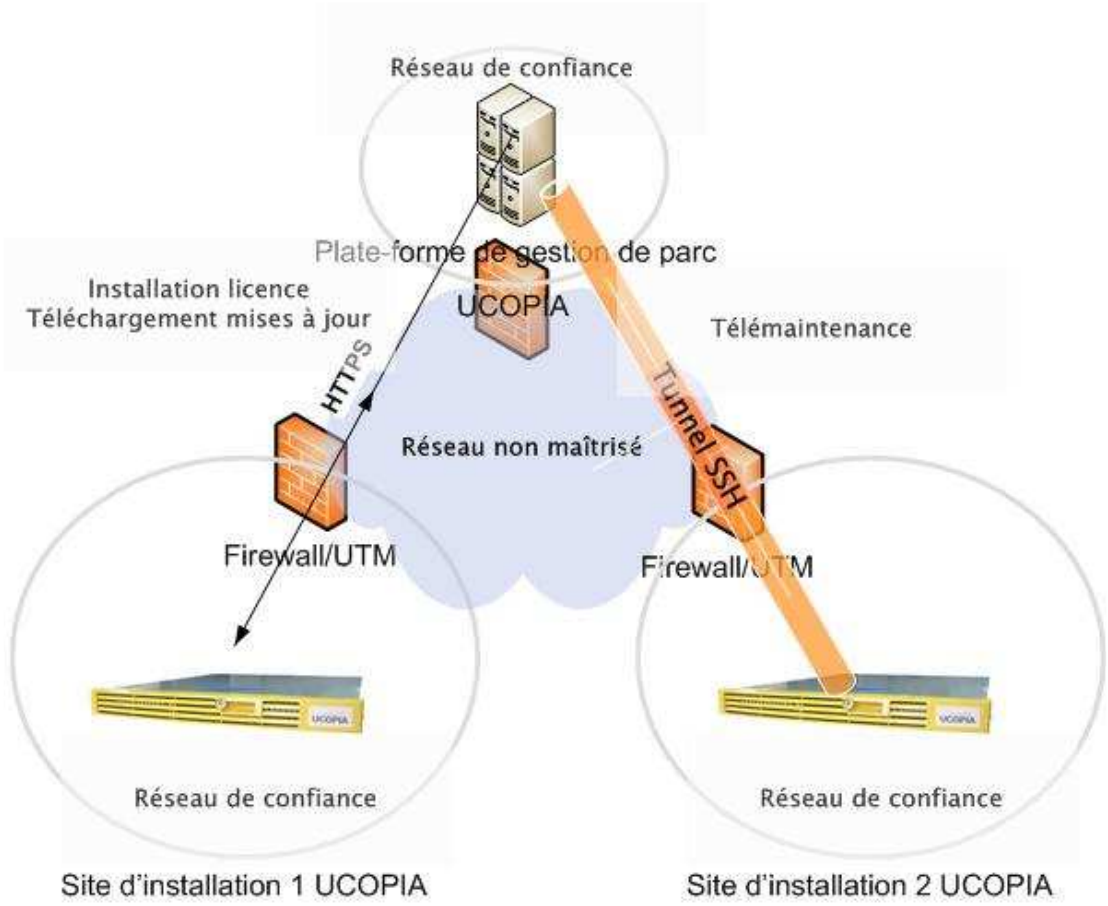

Figure 12 : Architecture de la plate-forme de gestion de parc d'appliances UCOPIA

Nous supposons que les environnements réseaux de la société UCOPIA et ceux du client chez qui UCOPIA est installé sont des réseaux de confiance.

7.5.3 Téléchargement de licence et de mises à jour

Périodiquement ou à la demande de l'administrateur, l'appliance UCOPIA ouvre une communication chiffrée HTTPS vers la plate-forme de gestion de parc hébergée par UCOPIA pour récupérer la licence de l'appliance, les mises à jour disponibles ou les mises à jour critiques.

7.5.4 Télémaintenance

La télémaintenance de l'appliance UCOPIA est assurée par un tunnel SSH déclenché depuis le boîtier UCOPIA vers les serveurs de maintenance UCOPIA.

9 Description des mécanismes cryptographiques

Voir la documentation Spécifications Crytographiques CSPN – UCOPIA 3.0 (référence UCP-CSPN-CRYPTO- 3.0-09).

10 Glossaire

10.1 Terminologie UCOPIA utilisée dans le cadre de la cible de sécurité

- **Boîtier appliance**
  Équipement UCOPIA placé en coupure entre un réseau non maîtrisé permettant l'accueil d'utilisateurs et un réseau de confiance, tel qu'un réseau d'entreprise.

- **Réseau de confiance**
  Un réseau est dit de confiance si, du fait qu'il est sous le contrôle de l'exploitant du produit UCOPIA, la politique de sécurité interne n'implique pas qu'il faille se protéger des flux qui en proviennent, mais au contraire implique qu'il faille les protéger des flux qui y parviennent.

- **Réseau non maîtrisé**
  Un réseau est dit non maîtrisé s'il n'est pas sous le contrôle de l'exploitant du produit UCOPIA, ce qui implique qu'il faille se protéger des flux établis avec les équipements de ce réseau (par exemple Internet).

10.2 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 switchs 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.

10.3 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 opérent sur la fréquence 2,4 Ghz et propose une bande passante respectivement de 11 et de 54 Mbps. 802.11n n'est pas encore disponible et proposera 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.

10.4 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 un 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 basé 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.Cette méthode est considérée comme la plus sûre, dans le sens où elle permet une autthentification mutuelle Basé sur des certificats X.509 . 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 passé 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 calculette 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.

10.5 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.

10.6 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.

11 Références (RFC et standards)

UCOPIA 3.0 est fourni sous forme de boîtier appliance. Le système d'exploitation sous-jacent est une distribution Linux : la Mandriva 2009.0. Les standards et RFC (Request For Comment)

suivants sont utilisés dans UCOPIA 3.0. Pour chacun, la version du paquetage logiciel utilisé dans UCOPIA est indiquée dans cette partie.

- **HTTP : RFC 2616**
  - apache-modules-2.2.9-12mdv2009.0
  - apache-conf-2.2.9-2mdv2009.0
  - apache-base-2.2.9-12mdv2009.0

- **SSL/TLS : OpenSSL (openssl.org)**
  - openssl-0.9.8h-3mdv2009.0
  - libopenssl0.9.8-0.9.8h-3mdv2009.0
  - mod_ssl-2.2.9-12mdv2009.0

- **LDAPv3 : RFC 2251**
  - openldap-2.4.11-3mdv2009.0
  - openldap-servers-2.4.11-3mdv2009.0

  openldap-clients-2.4.11-3mdv2009.0libldap2.4_2-2.4.11-3mdv2009.0

- **RADIUS : RFC 2865**
  - freeradius-2.1.0-2mdv2009.0
  - freeradius-ldap-2.1.0-2mdv2009.0
  - libfreeradius1-2.1.0-2mdv2009.0
  - **SQL - MySQL (ISO SQL:2003)**mysql-5.0.67-3mdv2009.0
  - mysql-common-5.0.67-3mdv2009.0
  - libmysql15-5.0.67-3mdv2009.0

- **SSH : RFC 4251**
  - openssh-5.1p1-2mdv2009.0
  - openssh-server-5.1p1-2mdv2009.0
  - openssh-clients-5.1p1-2mdv2009.0
  -

- **DHCP : RFC 2131**
  - dhcp-common-3.0.7-1mdv2009.0
  - dhcp-client-3.0.7-1mdv2009.0
  - dhcp-server-3.0.7-1mdv2009.0