Architecture flexible de réseau sans fil WiFi sécurisé

Gwendal LE GRAND, Artur HECKER, et Franck SPRINGINSFELD

GET/Télécom Paris - LTCI-UMR 5141 CNRS, Département INFRES, 37-39 rue Dareau, 75014 PARIS, France.
{gwendal.legrand | artur.hecker | fspringi}@enst.fr

Résumé
Les réseaux locaux sans fil (WLAN) envahissent notre quotidien car la valeur ajoutée qu'ils offrent aux utilisateurs, à un coût raisonnable, est incontestable. Comme ces réseaux possèdent des frontières à géométrie variable et surtout difficilement contrôlables, il est indispensable de les protéger. Cependant, les mécanismes de sécurisation du WiFI tels que WEP sont très facilement cassables en téléchargeant des logiciels sur Internet, et la simplicité de déploiement et le coût réduit des WLAN font que beaucoup d'individus installent ce type de réseaux, mais oublient de les administrer et les sécuriser. Cet article passe en revue les différentes solutions proposées pour sécuriser les WLAN et nous constatons que ces solutions ne proposent pas simultanément facilité d'utilisation et sécurité renforcée. Nous montrons pourquoi il est indispensable d'offrir une vaste couverture avec un réseau sans fil sécurisé et nous proposons une méthodologie et une architecture de réseau pour répondre à cette problématique. La solution sécurisée proposée s'appuie sur une différentiation des clients ; elle fournit une sécurité renforcée par l'usage de certificats et de méthodes d'authentification élaborées (EAP-TTLS ou PEAP) pour les utilisateurs fréquents, ainsi qu'un usage ouvert mais restreint pour les visiteurs.

Keywords: IEEE 802.11, WiFi, Radius, EAP, 802.1X, NAT, VPN.

Ce travail est réalisé dans le cadre du projet RNRT Infradio.

1 Introduction

Le terme WiFi (*Wireless Fidelity)* regroupe des équipements conformes aux standards IEEE 802.11 [IEE99] (a, b et g), pour un accès sans fil aux réseaux locaux. Ces réseaux ont envahi notre quotidien :

- à la maison (pour partager une connexion ADSL ou câble),
- en entreprise (pour un accès au réseau local en sans fil)
- dans les lieux publics (hôtels, gares, aéroports, cafés, centres de conférences, galeries marchandes… via des Hot Spots). Ce succès est sans doute dû à des tarifs en chute libre (cartes à quelques dizaines d'euros) et des performances croissantes grâce aux nouveaux standards IEEE 802.11a et g à 54 Mbit/s.

Cependant, l'apparition des technologies sans fil modifie la manière d'appréhender la sécurité, car la morphologie des réseaux évolue vers des formes floues, puisque le medium utilisé est par nature hertzien et diffusant, donc sans frontière précise. Le WiFi peut alors devenir une porte d'entrée sur le réseau d'entreprise qui permet de déjouer les mécanismes d'authentification classiques. La Fig.1 illustre ce phénomène puisqu'un terminal filaire ne peut se connecter à un réseau d'entreprise que via une passerelle ssh (sur laquelle il faut s'authentifier), alors qu'un terminal sans fil peut utiliser un AP (Access Point) ouvert pour se connecter directement dans le réseau d'entreprise (comme s'il lui appartenait). Ceci est amplifié par l'utilisation massive de protocoles d'autoconfiguration (comme DHCP) qui fournissent automatiquement toute la configuration au terminal sans fil.

Il est extrêmement facile de déployer un point d'accès sans fil ou de partager sa connexion internet sur un lien ad-hoc sans fil. Dans ce dernier cas, il suffit de mettre en place du routage NAT (Network

Address Translation), en installant du logiciel sur les systèmes unix et en cochant simplement une case sur un système Windows ou MacOS. Ces fonctionnalités sont extrêmement pratiques pour des utilisateurs souhaitant facilement se connecter en utilisant des interfaces sans fil, mais elles prolongent le réseau d'entreprise de manière non sûre. De plus, les AP étant des ponts (entre Ethernet et IEEE 802.11), il est possible de les chaîner afin d'étendre à l'infini les frontières des réseaux d'entreprise, tout en rendant la détection de ce type d'architecture relativement compliqué. Finalement, comme ces technologies ont envahi le grand public, nombreuses sont les personnes qui déploient des AP sans se préoccuper de leur administration ; ils restent donc trop souvent complètement ouverts et même quand ils ne le sont pas, les mécanismes de sécurisation (filtrage MAC, clé WEP, SSID non diffusé …) sont généralement faciles à déjouer. En effet, il suffit de télécharger des logiciels « bien connus » sur l'Internet pour casser une clé WEP par exemple.

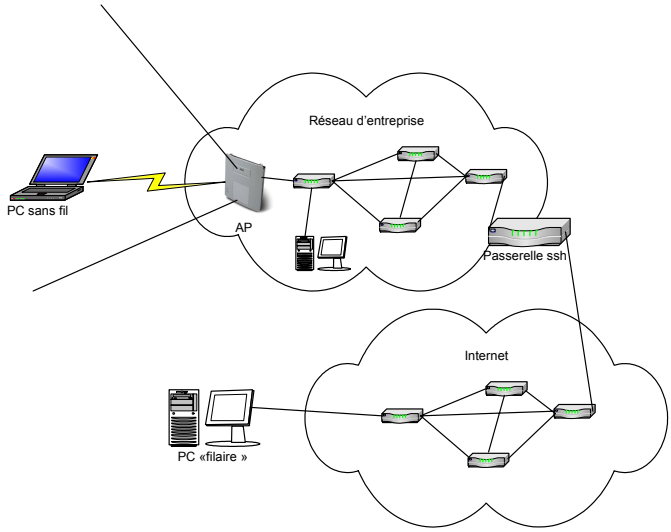

Fig. 1 – Failles morphologiques du WiFi

Dans cet article, nous présentons et justifions les choix qui ont été effectués pour le déploiement d'un réseau sans fil sécurisé sur les deux sites de l'ENST Paris (site Barrault et site Dareau). Pour combiner sécurité et facilité d'usage, ce réseau doit pouvoir offrir à la fois une sécurité renforcée pour les utilisateurs permanents (qui configurent leur machine une fois pour toutes) et un accès simplifié mais limité et contrôlé pour des invités. Nous proposons également une série de mesures qui contribuent à renforcer la sécurisation des réseaux sans fil, en parallèle du déploiement de l'architecture.

La suite de ce document se présente de la manière suivante : nous décrivons un état de l'art de la sécurité dans les réseaux sans fil dans la partie 2 ; puis, la partie 3 s'intéresse à l'architecture choisie et à une évaluation qualitative par rapport à la solution la plus fréquemment utilisée. Finalement, nous concluons et donnons des pistes de travail futures.

2 Etat de l'art

Il existe aujourd'hui de nombreuses manières plus ou moins efficaces de sécuriser les réseaux WiFi. WEP (Wireless Equivalent Privacy) [IEE99] est un protocole de sécurisation de la couche MAC qui fournit l'authentification, la confidentialité et l'intégrité. Cependant, il possède des faiblesses bien connues [Wal00] qui sont essentiellement dues aux limitations du vecteur d'initialisation IV et à la génération du RC4(IV, K_S) [Flu01]. Ils est donc vulnérable à de nombreuses attaques comme par exemple : attaque de l'authentification WEP, vulnérabilités de la clé secrète K_S, attaque de rejeu, attaque par la linéarité du Checksum CRC, réutilisation du vecteur d'initialisation IV, collision des

vecteurs d'initialisation IV, utilisation de vecteurs d'initialisation IV « faibles », attaque par IV connu.

TKIP (Temporal Key Integrity Protocol) [WiFiA] permet de résoudre certaines failles de sécurité du WEP tout en conservant le même équipement. Les apports algorithmiques de TKIP sont :

- Un message code d'intégrité (Message Integrity Code), ou MIC, appelé Michael, permettant de se défendre contre les attaques de falsification de paquets.
- Une nouvelle manière de séquencer les vecteurs d'initialisation (IV Sequencing), pour contrer les attaques de re-jeu de paquets.
- Une fonction de construction de clé par paquet (per-packet key mixing function), afin de décorréler les vecteurs d'initialisation des clés utilisées.
- Un mécanisme de création de clé (rekeying mechanism) permettant de fournir des nouvelles clés de chiffrement et d'intégrité, évitant ainsi également les attaques par réutilisation de clés.

Originellement développé pour les réseaux filaires par 3Com, HP et Microsoft, le standard IEEE 802.1X [LMS01] définit une architecture de contrôle d'accès basée sur le protocole IETF EAP (Extensible Authentification Protocol) [Blu98]. Une architecture 802.1X fait intervenir un client (*supplicant)*, un point d'accès (*authenticator)* et un serveur d'authentification. Les requêtes et réponses EAP nécessaires à l'authentification du client transitent sur un port non contrôlé. Une fois l'authentification achevée, le serveur d'authentification contacte *l'authenticator* qui décide d'ouvrir une connexion par un port contrôlé. Il fournira par la même occasion à *l'authenticator* des informations permettant de dériver les clefs de session pour WEP ou TKIP.

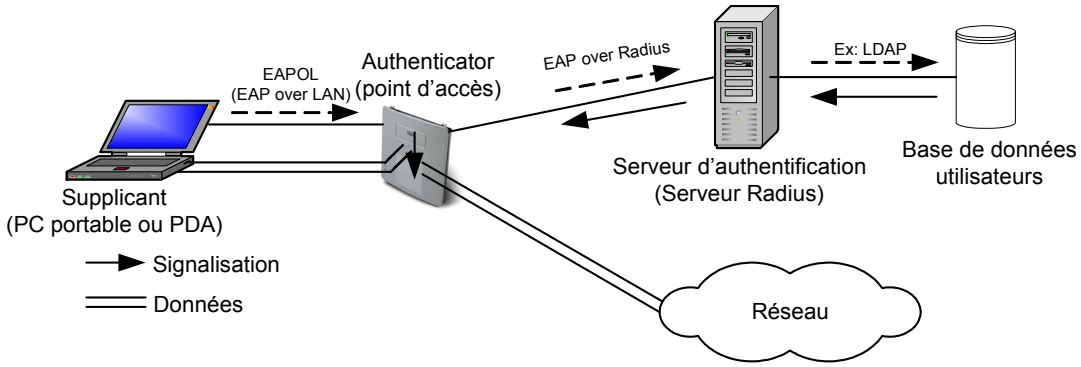

Fig. 2 – Architecture 802.1x

EAP supporte différentes méthodes d'authentification. EAP-MD5 [Blu98] est simple et relativement vulnérable (pas d'authentification mutuelle, possibilité d'attaques par dictionnaire et pas de clés dynamiques). LEAP (Lighweight EAP) est une solution propriétaire Cisco qui permet une distribution dynamique des clés. Mais LEAP reste vulnérable aux attaques par dictionnaire et permet également l'obtention par un attaquant du login du client. EAP-TLS (Transport Level Security) [Abo99] utilise le protocole handshake de TLS [Die99]. Basé sur l'utilisation de certificats, il permet une authentification mutuelle forte du client et du serveur, une négociation commune de la méthode cryptographique et un échange sécurisé de clés de session, qui permettent de dériver les clés WEP dynamiques. Cependant, cette méthode ne protège pas l'identifiant du client et impose l'utilisation d'une PKI (Public Key Infrastructure). EAP-TTLS (Tunnelled EAP-TLS), proposé par Funk Software, nécessite que le serveur (seulement) dispose d'un certificat, à partir duquel une session TLS pourra être ouverte. Les clients s'authentifient par un protocole d'authentification (PAP, CHAP, EAP, MS-CHAP ou MS-CHAPv2) transporté de manière sécurisée dans le tunnel préalablement établi. EAP-TTLS [Fun03] offre une authentification mutuelle, la distribution dynamique de clefs, il ne fait pas paraître en clair l'identifiant du client et surtout, il permet de s'affranchir de l'utilisation d'une PKI. PEAP (Protected EAP) [Pal03], proposé par Microsoft, Cisco et RSA, est très similaire à

EAP-TTLS. En ce qui concerne son utilisation, les différences principales avec EAP-TTLS résident dans les protocoles supportés à l'intérieur du tunnel et les exigences en terme d'implémentation. En effet, EAP-TTLS supporte l'encapsulation de tous les protocoles d'authentification alors que PEAP se limite à EAP et MS-CHAPv2. De plus, du côté client, seul PEAP est supporté en natif par WindowsXP. Il existe de nombreux clients gratuits supportant ces protocoles : Alfa & Ariss SecureW2 (Windows XP et 2000), Xsupplicant (MacOSX, Linux, FreeBSD), le client Cisco Aironet 350 (Windows 95, 98, NT 4.0, 2000, ME, XP, WinCE, MacOS, MS-DOS et Linux).

Pour pallier les faiblesses du WEP, WiFi Alliance [WiFiA] a développé le standard WPA obligatoirement supporté par les produits actuellement en vente et upgradable sur certains anciens équipements. Afin d'améliorer l'authentification et les méthodes de chiffrement de WEP, WPA utilise TKIP et implémente 802.1x et EAP.

Pour procurer un accès aux utilisateurs autorisés sans que les autres puissent en bénéficier, une solution est d'installer une passerelle d'authentification (*captive portal*) entre le réseau sans fil et le réseau externe. Les fonctionnalités d'une telle passerelle sont :

- filtrage des paquets avec gestion dynamique des règles de pare-feu selon le niveau d'authentification de l'utilisateur (redirection vers page d'authentification, éventuellement filtrage MAC, restriction d'usage de protocoles),
- serveur HTTP et DNS,
- mécanisme d'authentification et d'accounting,
- adressage IP dynamique et privé si nécessaire (par serveur DHCP et NAT),

Un utilisateur se voit ainsi attribuer une adresse IP par DHCP, lance un navigateur, se retrouve redirigé vers une page où il doit s'authentifier (ex : login/password), et accède au service demandé si l'authentification est validée. Les avantages d'une passerelle d'authentification sont sa simplicité de gestion et d'utilisation au niveau du client. En effet, l'utilisateur n'a besoin que d'un navigateur pour se connecter. Cependant, cette architecture est centralisée et manque de fiabilité. Par exemple, le trafic n'est pas chiffré par défaut, mais peut l'être si on utilise un VPN (Virtual Private Network).

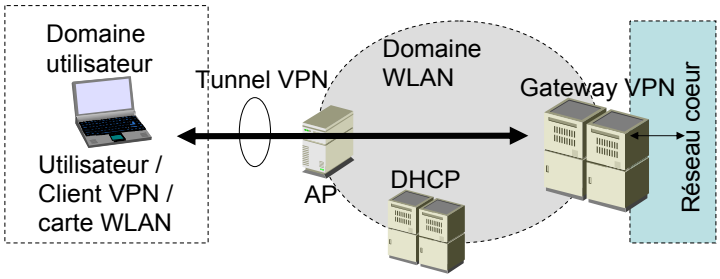

Fig. 3 – Architecture VPN

La technologie VPN utilise des protocoles cryptographiques connus tels que IPSec pour proposer une solution suffisamment sûre pour protéger l'accès à distance des utilisateurs à leur réseau d'origine. L'intégration des solutions VPN dans les systèmes d'exploitation courants, dans les composants des réseaux et dans les architectures de sécurisation, rend cette technologie largement utilisée et très populaire. L'utilisateur se connecte d'abord au réseau sans fil . Le serveur *DHCP* local attribue alors une adresse IP à l'interface de la carte. Cette adresse IP est nécessaire puisqu'elle sera utilisée comme adresse externe du tunnel du client VPN de l'utilisateur à la passerelle VPN (*VPN Gateway*). Néanmoins, son utilisation est limitée au réseau local et, par conséquent, elle peut être une adresse IP privée. La passerelle VPN possède deux interfaces réseaux dont l'une est connectée au domaine du réseau sans fil (*WLAN domain*) et l'autre au *réseau cœur*. Le client VPN et la passerelle VPN s'authentifient mutuellement en utilisant leur protocole VPN. Cette authentification négocie typiquement les paramètres de sécurité de la session à établir. Si l'authentification réussit, le client VPN ouvre une interface réseau virtuelle du coté utilisateur. Celle-ci représente l'accès au tunnel : toutes les données envoyées à cette interface sont chiffrées et encapsulées par le client VPN. Le

serveur VPN inspecte les paquets reçus des clients, décapsule les données, déchiffre le contenu selon les paramètres négociés et renvoie les données (i.e. typiquement le paquet IP d'origine) sur son interface du réseau cœur. Dorénavant, les paquets envoyés par les applications de l'utilisateur ont conceptuellement le format présenté ci-dessous :

Fig. 4 – - En-têtes des paquets traités par un client VPN

Aucune des solutions proposées ci-dessus ne permet, à elle seule, de répondre aux exigences de nombreux administrateurs de réseaux qui souhaitent bénéficier d'au moins deux infrastructures logiques : un réseau d'invité « ouvert » et contrôlé, ainsi qu'un réseau de permanents sécurisé. Dans la suite, nous présentons l'architecture retenue pour notre réseau, qui répond à ce cahier des charges.

3 Déploiement du réseau

3.1 Objectifs

Nous souhaitons supporter plusieurs types de populations dans la même architecture physique. Il est nécessaire de disposer d'un côté d'un réseau sans fil sûr pour les permanents et de l'autre d'un réseau disponible facilement pour des invités. Malheureusement, nous avons vu précédemment que ces deux contraintes sont souvent contradictoires. La méthodologie consiste donc à déployer plusieurs architectures logiques qui vont isoler les trafics des différentes catégories d'utilisateurs.
De plus, il faut disposer d'outils pour le dimensionnement du réseau, son administration, sa prévention et sa sécurisation, que nous détaillons dans la suite.

3.2 Méthodologie de déploiement

3.2.1. Expression des besoins

La première étape dans le déploiement d'une architecture de réseau sans fil consiste à recenser les besoins afin d'établir un cahier des charges. Il faut effectuer des mesures de propagation dans l'environnement pour déterminer le dimensionnement du réseau en nombre de points d'accès. La surface représentée sur la partie droite de la Fig. 5 représente le niveau de signal reçu en plusieurs points d'un étage d'un bâtiment dont le plan est sur la gauche de la figure. Les courbes de niveau du signal sont également représentées. Nous constatons que la puissance du signal reçu diminue de manière non régulière, en fonction de la nature des obstacles entre le point d'accès et du client effectuant les mesures (Fig. 5).

Il est également nécessaire de définir les besoins en terme de sécurité. Les besoins exprimés aujourd'hui par les administrateurs de réseaux concernent d'abord la possibilité de distinguer plusieurs populations avec la même infrastructure physique. Nous devons donc distinguer :

- les permanents avec un accès protégé,
- les visiteurs avec un accès ouvert et limité,
- d'autres types de populations, utilisant des techniques d'authentification variées, que nous devons pouvoir intégrer simplement dans l'environnement.

Le caractère stable des permanents justifie l'emploi de certificats pour l'authentification de ces utilisateurs ; une authentification par EAP-TLS ou PEAP est donc envisageable. Comme nous l'avons mentionné plus haut, il n'y a pas véritablement de problèmes concernant l'installation de client. Il existe des freewares sur tout système d'exploitation, certains clients sont même en natif (PEAP sur Windows XP). Les invités doivent avoir un niveau de contraintes minimales, la qualité de l'authentification en sera logiquement affectée. Il est donc nécessaire de séparer les trafics i.e. le trafic *Invités* à faible authentification et le trafic *Permanents*. A cet effet, nous utilisons 3 VLAN

différents (1 pour les invités et 2 pour l'authentification IEEE 802.1X des permanents). Les invités passent sur le VLAN correspondant au SSID diffusé ostensiblement par l'AP. Lorsqu'ils veulent se connecter via le réseau WiFi, le trafic est intercepté par la passerelle d'authentification et les utilisateurs sont reroutés vers une page d'accueil qui leur demande un login/password ou peut leur offrir un accès limité avec filtrage de protocoles.
Une granularité plus fine (en distinguant davantage de catégories) est également envisageable.

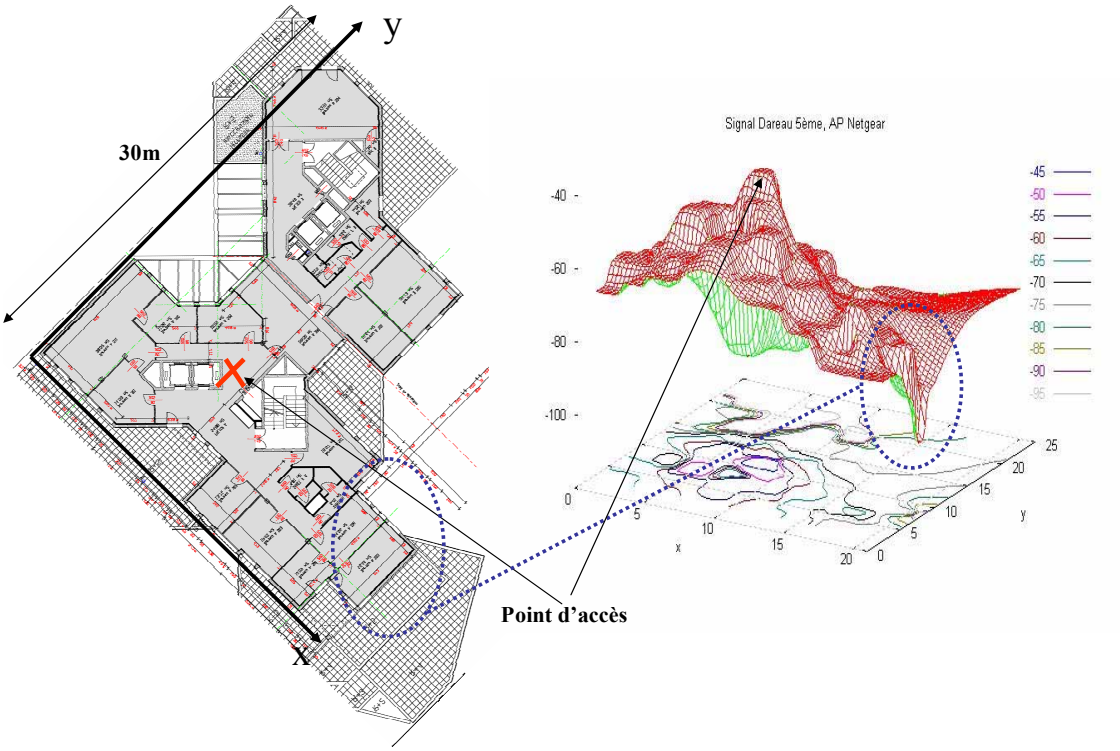

Fig. 5 – Mesures de l'environnement radio

De plus, des outils d'administration du réseau doivent être développés afin par exemple de pouvoir :

- détecter des clients du réseau qui se connectent (intentionnellement ou non) sur des réseaux hors du réseau d'entreprise ; ce phénomène prend de l'ampleur puisque les réseaux sans fil se multiplient et on peut donc se connecter sur l'AP d'un autre réseau,
- Mettre à jour la configuration des AP facilement,
- Détecter si un AP a été déconnecté du réseau,
- Etc.

3.2.2. Recensement des AP et détection AP pirates

Avant de déployer un réseau sans fil sécurisé, il convient de recenser l'ensemble des AP existants dans le réseau, afin de les mettre à jour et de les intégrer dans l'architecture sécurisée quand c'est possible. Si les AP sont trop anciens pour supporter les fonctionnalités de sécurité décrites ci-après, il est indispensable de les sortir du réseau pour ne pas se trouver dans le cas présenté précédemment Fig.1.

Les AP modernes permettent de détecter la présence d'autres AP. Cette fonctionnalité doit être exploitée afin de surveiller l'apparition éventuelle d'AP ou de SSID inconnus. Nous développons donc des outils SNMP afin de déclencher des alertes en cas d'anomalie constatée.

3.2.3.Charte informatique et couverture globale

Comme il est très facile de partager sa connexion internet, n'importe quel utilisateur peut devenir routeur NAT et peut, sans s'en rendre compte, ouvrir des portes pour entrer dans le réseau. Il existe plusieurs manières de lutter contre ce phénomène. Il est possible d'administrer toutes les machines pour empêcher d'utiliser cette fonctionnalité et empêcher de créer des liens ad hoc (au sens IEEE 802.11 et pas au sens du réseau ad hoc). Cependant, ceci est très difficile dans un environnement universitaire. De plus, des utilisateurs peuvent également placer des AP non administrés et non sécurisés dans leurs bureaux, ce qui a sensiblement les mêmes conséquences.

Par conséquent, nous préconisons :

- une couverture de réseau sans fil globale et flexible pour tous, afin que la création de liens ad hoc ou le déploiement d'AP ne soit plus un besoin pour les utilisateurs du réseau. En effet, un utilisateur qui dispose en tout point d'un réseau sans fil simple d'usage ne sera pas tenter de recourir à ces pratiques.
- En parallèle, il est indispensable de définir une charte informatique qui définit clairement les règles d'usage.

3.3 Présentation de l'architecture

Plusieurs architectures logiques (représentées Fig. 6 et 7) sont supportées sur la même architecture physique. Il faut simplement associer un nom de réseau (SSID) à un VLAN (Virtual LAN). Un VLAN est utilisé par une population d'usagers et chaque SSID/VLAN peut bénéficier d'une technique d'authentification spécifique. Les points d'accès récents (comme les Cisco Aironet 1200 que nous utilisons) supportent les SSID multiples et le mapping SSID/VLAN.

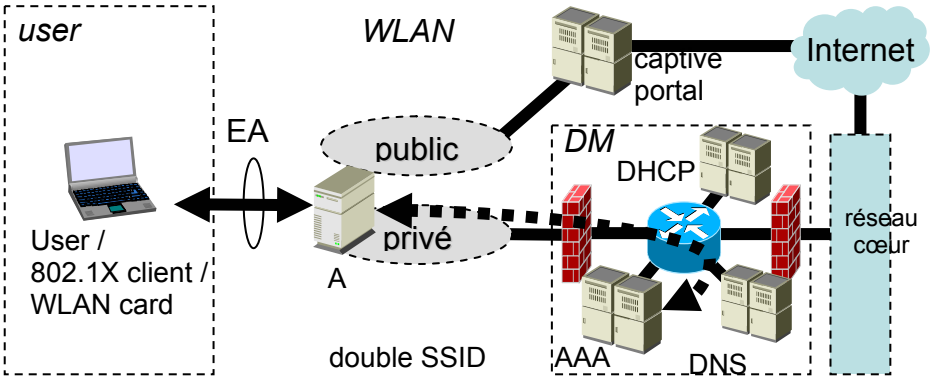

Fig. 6 – Architecture logique pour la protection des WLAN

Les points d'accès que nous utilisons supportent IEEE 802.11a, b et g. Les utilisateurs peuvent donc se connecter à 11 ou 54 Mbit/s en fonction du matériel dont ils disposent, et cela de manière transparente par rapport à la technique de sécurité, puisque que l'on peut affecter le même SSID à plusieurs interfaces et les mapper sur le même VLAN. L'architecture déployée (sur le site Dareau) est décrite Fig.7. Elle est extensible à l'autre site en prolongeant simplement les VLAN des utilisateurs du réseau sans fil vers les prises Ethernet d'où l'on souhaite connecter des AP sur l'autre site.

Supposons que dans notre architecture, nous disposions de la plage d'adresses 138.142.54.0/23. Nous subdivisons cette plage en plusieurs sous-réseaux : le réseau 138.142.55.0/24 pour distribuer des adresses par DHCP aux permanents, le 138.142.54.0/25 pour les points d'accès du réseau, le 138.142.54.128/26 pour le réseau d'administration (RADIUS, DNS…), le 138.142.54.192/26 pour la zone remontant vers l'Internet. On utilise aussi les adresses privées 10.0.0.0/24 pour les invités. Les

invités obtiennent des adresses privées et passent par un SSID *Invit* pour se diriger sur le NAT alors que les permanents ont une adresse globale, un SSID *Perm* et des certificats pour s'authentifier.

Comme présente Fig. 7, nous utilisons plusieurs VLAN dans le réseau (le choix des numéros des VLAN étant purement arbitraire) : 103 correspond au VLAN de management sur lequel transite notamment le trafic d'authentification, 100 remonte vers l'Internet, 104 est le VLAN de la DMZ (entre les firewalls), 101 et 102 supportent respectivement les permanents et les invités.
Le serveur RADIUS [Rig00] utilisé est Freeradius (opensource) et nous gérons les utilisateurs par une base de données MySQL. Comme la différenciation est basée sur le marquage des paquets et sur les VLAN, les switchs traversés doivent supporter également le tagging IEEE 802.1q.

Cette architecture, comme les réseaux filaires, est administrée et l'utilisateur n'est finalement qu'un client du réseau, et ne participe pas au déploiement de l'infrastructure. Des utilisateurs particuliers ne peuvent donc pas déployer des APs à leur guise. D'autre part, notre architecture comportant une partie filaire considérée comme fiable, il n'est pas nécessaire d'établir des tunnels de bout en bout puisque seule la partie sans fil a besoin d'être sécurisée. En effet, il n'est pas souhaitable d'imposer un chiffrement (de type VPN) qui ne serait pas utilisé dans un architecture filaire classique dans laquelle les utilisateurs ne chiffrent que pas leurs données de bout en bout.

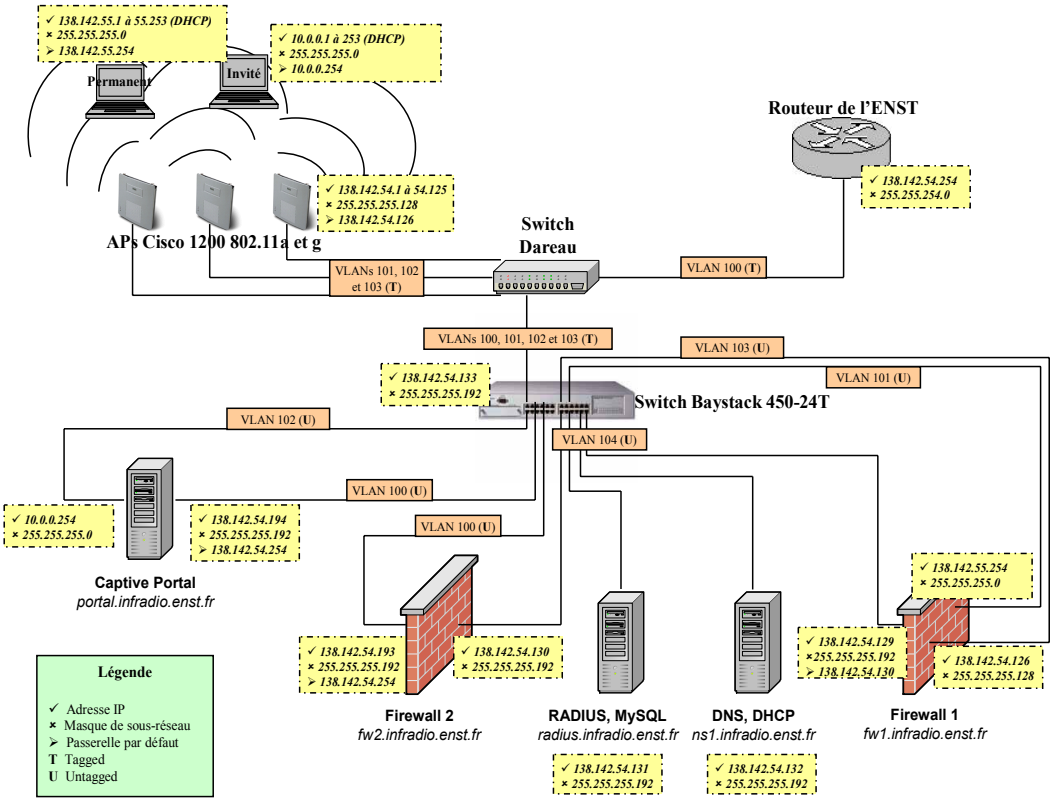

Fig. 7 – Architecture physique de réseau de campus sécurisé.

3.6. Evaluation qualitative de la solution

La majorité des réseaux sans fil avec une sécurité augmentée que l'on rencontre aujourd'hui reposent sur l'établissement d'un VPN. Nous allons évaluer qualitativement notre solution par rapport à cette technologie.

Les VPN, permettant de traverser de manière sécurisée les réseaux publics et particulièrement Internet, se situent au dessus de la 3ème couche ISO/OSI. Ainsi, ils sont directement intégrables dans les architectures de sécurisation des réseaux locaux sans fil. A l'origine, les VPN étaient conçus pour la sécurisation des connexions par les réseaux publics (RTC, Internet, etc.) aux réseaux privés (entreprise) pour sécuriser une connexion multi-sauts constituée de liens potentiellement hétérogènes. En particulier, la technologie VPN vise la sécurisation des données de l'utilisateur et suppose l'insécurité des liens utilisés. Par conséquent, les VPN ajoutent une charge considérable à chaque paquet envoyé et gaspillent les ressources du lien radio ; de plus, la passerelle VPN devient un goulot d'étranglement. De plus, pour être capable de se connecter à la passerelle VPN, l'utilisateur a besoin de pouvoir se connecter au réseau sans fil librement i.e. d'avoir accès au réseau avant la première authentification. Ensuite, l'utilisateur a besoin d'une adresse IP et donc d'un accès libre au serveur DHCP du WLAN. Par conséquent, un attaquant peut se connecter librement au WLAN déployé dont les portes sont désormais largement ouvertes, obtenir une adresse IP et envoyer des paquets aux autres terminaux connectés. Ceci lui permet de réunir des informations sur l'utilisation du réseau (trafic, statistiques, adresses IP du matériel, etc.). Il peut ainsi mettre au point plusieurs types d'attaques DoS (Denial of Service), dont la plus évidente est probablement l'attaque sur le serveur DHCP (en changeant l'adresse MAC continuellement, on demande des adresses IP jusqu'à l'épuisement du stock).

Les solutions VPN existant sur le marché utilisent peu souvent une authentification mutuelle suffisamment forte. Avec la facilité de l'attaque Man in the middle (MITM) dans le cas des réseaux sans fil, ce défaut devient un véritable problème.

Finalement, les solutions basées sur un élément central de contrôle (VPN Gateway) sont centralisées et le passage à l'échelle reste problématique par définition. Pourtant, dans les WLAN, il y a un autre élément qui est indispensable, relativement robuste, peu onéreux et dont la quantité augmente automatiquement avec le débit souhaité : le point d'accès. En laissant l'accès au réseau sans fil sans aucun contrôle, on perd un point de renforcement des politiques de sécurité (en les déplaçant plus loin dans le cœur) et on risque d'avoir des attaques directes sur les terminaux sans fil, ce qui risque de causer à long terme une attaque réussie au réseau cœur.

Nous pensons que la sécurité doit être intégrée directement dans les éléments du réseau sans fil pour pouvoir répartir la charge du chiffrement/déchiffrement des paquets et renforcer le contrôle d'accès au premier point de contact avec le réseau sans fil. De plus, les points d'accès modernes (e.g. Cisco AP350, AP1200, etc.) implémentent déjà les normes nécessaires (IEEE 802.1X, WEP à clés dynamiques « rotating WEP key », intégration dans les architectures Authentication Authorization and Accounting, etc.). Le support de ces normes est également intégré directement dans la plupart des systèmes d'exploitation disponibles (Windows XP, Windows 2000, Linux, FreeBSD, MacOS X, etc.) et des cartes 802.11 sur le marché. Selon la politique de sécurité choisie, un VPN supplémentaire peut être ajouté au-dessus de cette couche de protection intégrée, si nécessaire.

4 Conclusion et perspectives

Nous avons présenté une méthodologie de déploiement ainsi qu'une architecture de WLAN sécurisé. Cette solution repose sur une séparation logique par VLAN de populations d'utilisateurs qui utilisent des mécanismes d'authentification forte pour les permanents et un accès simple (mais limité) pour des invités. Par comparaison avec la solution VPN, la plus répandue aujourd'hui, notre proposition sécurise la couche radio, est plus flexible et passe mieux à l'échelle. De plus, elle est compatible avec un chiffrement des couches hautes avec une solution VPN.
La suite de ce travail consiste à développer des outils pour faciliter l'administration du réseau, par exemple :

- Détection et localisation par triangulation d'AP qui n'appartiennent pas au réseau sécurisé,
- Détection et localisation de SSID inconnu,
- Détection d'utilisateurs qui se connectent sur un autre réseau par un lien sans fil,
- Authentification d'une population d'utilisateurs par carte à puce,

- Intégration de SSO (Single Sign On) pour que les utilisateurs n'utilisent qu'un seul login / password.
- Mobilité IP.

Références

[Abo99] B. Aboba, D. Simon, "PPP EAP/TLS Authentication Protocol", RFC 2716, IETF, October 1999.

[Blu98] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," RFC 2284, IETF, March 1998.

[Die99] T. Dierks, C. Allen, "The TLS protocol version 1.0", RFC 2246, IETF June 1999.

[Flu01] Fluhrer, S., Martin, I., and Shamir, A., "Weaknesses in the Key Scheduling Algorithm of RC4", Proc. of the 8th Annual Workshop on Selected Areas in Cryptography, August 2001.

[Fun03] P. Funk, Blake-Wilson, EAP Tunneled TLS Authentication Protocol (EAP-TTLS), IETF Internet Draft, <draft-ietf-pppext-eap-ttls-03.txt>, August 2003

[IEE99] L.M.S.C of the IEEE Computer Society, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications", IEEE standard 802.11, 1999 Editions, 1999

[IEE99b] L.M.S.C of the IEEE Computer Society, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher Speed Physical Layer Extension in the 2.4GHz Band", IEEE standard 802.11b, 1999 Editions, 1999.

[LMS01] L.M.S.C of the IEEE Computer Society, "Port-Based Network Access Control", IEEE Standard 802.1X, June 2001

[Pal03] A. Palekar, D. Simon, G. Zorn, J. Salowey, H. Zhou, S. Josefsson, Protected EAP Protocol (PEAP) Version 2, IETF Internet Draft, <draft-josefsson-pppext-eap-tls-eap-07.txt>, Octobre 2003.

[TKIP] IEEE 802.11i, "Draft Supplement to IEEE Std 802.11. Part 11: Specifications for Enhanced Security", IEEE draft, work in progress.

[Rig00] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial-In User Service (RADIUS) ", RFC 2865, IETF, June 2000.

[Wal00] Walker, J., "Unsafe at any Key Size: an Analysis of the WEP encapsulation", IEEE Document 802.11-00/362, October 2000.

[WiFiA] The Wi-Fi Alliance Association, http://www.wifialliance.org/.