Le nomadisme : problématiques et solutions

Eric Jullien, Patrick Petit, David Roumanet

Nomadisme : Problématiques et Solutions

Eric Jullien
DSIGU (Direction des Sytèmes d'Information Grenoble Universités)
Eric.Jullien@grenet.fr

Patrick Petit
DSIGU (Direction des Sytèmes d'Information Grenoble Universités)
Patrick.Petit@grenet.fr

David Roumanet
DSIGU (Direction des Sytèmes d'Information Grenoble Universités)
David.Roumanet@grenet.fr

Résumé

Depuis 2003, les universités de l'académie de Grenoble ont initié une réflexion pour fournir un accès nomade à leurs utilisateurs. Cet article présente l'évolution des technologies en s'appuyant sur les tests réalisés et les solutions retenues par le groupe technique inter-universitaire chargé de cette problématique. Le but est de répondre à l'ensemble des demandes des diverses populations du campus : enseignants, chercheurs, étudiants, invités divers. Dans tous les déploiements, ont été privilégiés l'authentification, la gestion des traces, la sécurité des échanges des données, et l'intégration de nombreux systèmes d'exploitation. Suivant les usages, différentes solutions techniques et politiques d'accès ont été étudiées : « Portail sans client » ou « portail client léger » pour des colloques avec accès web uniquement, « portail client lourd » pour accéder à ses ressources internes et enfin WPA & WPA2 (802.11i) pour des accès à tous les services de l'Internet depuis le sans fil. L'authentification s'appuie sur des serveurs RADIUS qui peuvent s'interroger mutuellement et qui puisent leurs informations à différents niveaux (serveurs LDAP, bases locales, etc.). Si de nombreux aspects du nomadisme sont peu à peu traités correctement, la seule ombre au tableau reste encore la gestion de la salubrité des postes.

Mots clefs

ASFI, Wi-Fi, Portail Captif, VPN IPsec, VPN SSL, WPA, WPA2, RADIUS, Proxy, ARREDU, Eduroam.

1 Introduction

Les Universités grenobloises ont pris conscience assez tôt de l'intérêt de fournir un service d'accès nomade à leurs utilisateurs. Pour se faire, un groupe de travail technique regroupant les principaux établissements de l'académie a été crée afin de répondre au mieux à cette problématique. L'objectif de cet article est de présenter l'évolution des technologies dans ce domaine en s'appuyant sur des tests et les solutions retenues par ce groupe. L'article s'intéresse aux technologies sans fil mais pas seulement, la notion de nomadisme couvrant d'autres domaines que l'accès plus communément appelé « Wi-fi ».

Après avoir décrit l'architecture du réseau d'origine (depuis 2004 un nomadisme au sein des universités grenobloises est possible), nous indiquons les méthodes employées pour rendre ce premier service de nomadisme et relatons les problèmes rencontrés. L'article s'attache ensuite à décortiquer les forces et les faiblesses de différentes solutions proposées actuellement sur le marché. Enfin, il détermine les moyens à mettre en œuvre et décrit la solution préconisée (un pilote est déjà disponible) pour permettre de faire évoluer la solution en place actuellement vers de nouvelles fonctionnalités.

2 Le nomadisme à l'origine du projet

2.1 L'objectif initial

L'idée de départ était de trouver rapidement une solution capable de rendre transparent l'accès à ses ressources aux différentes populations qui cohabitent dans un domaine universitaire indépendamment de leur lieu de connexion.

Parallèlement à ce premier problème, le sans fil était en passe d'envahir de manière plus ou moins encadré les infrastructures réseaux gérées par les personnels techniques.

A partir de ces deux problèmes, le groupe de travail s'est donné comme objectif de trouver une solution unique et libre de tout constructeur. L'académie de Grenoble étant composée de plusieurs établissements indépendants, la solution devait garantir une sécurité suffisante, proposer un service mutualisé tout en permettant le libre choix des produits par chaque entité.

2.2 La solution technique

2.2.1 La méthode d'accès

Les organismes grenoblois ont donc déployé une solution commune de gestion des accès.

Les principaux éléments constitutifs de la solution sont :

• Des réseaux dédiés en libre accès dans tous les organismes pour tout utilisateur (quelque soit son appartenance) avec connexion obligatoire vers les boîtiers VPN-IPsec. L'accès à ces réseaux est généralement assuré

par des points d'accès sans fil mais il existe également des salles en libre service avec des accès filaires ;

• Des boîtiers VPN-IPsec dans chaque organisme pour assurer la confidentialité des communications (chiffrement) et la centralisation des identification et authentification des utilisateurs.

Chaque utilisateur nomade peut ainsi initier une connexion vers « son » boîtier VPN d'établissement et récupérer ensuite les droits qui lui sont attribués. Il peut le faire à partir de toutes bornes sans fil d'un des quelconques établissements de l'académie, mais il peut également se connecter à partir d'un quelconque réseau IP situé n'importe où sur Internet.

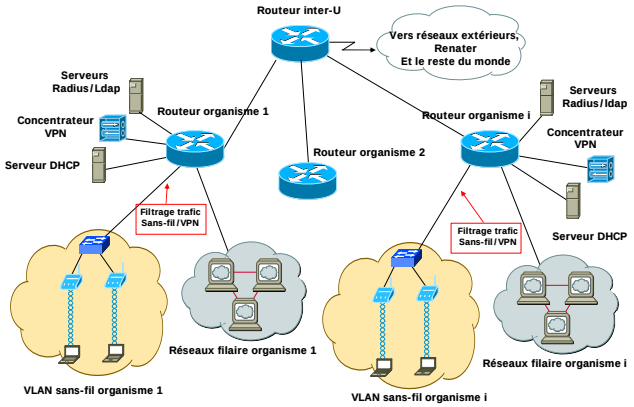

Figure 1 – *Principe d'architecture Nomadisme*

2.2.2 Cas particulier des accès sans fil

Du coté des bornes, elles sont généralement de type 802.11g et diffusent un SSID unique. Les bornes sont en accès libre et un système de filtrage strict ne permet d'accéder qu'aux boîtiers VPN.

Aucune fonctionnalité évoluée n'est requise pour les points d'accès dans ce mode de fonctionnement même si, nous le verrons plus loin dans cet article, l'achat de bornes incluant des fonctionnalités évoluées (ou la capacité à les rajouter) est un point important pour l'avenir.

Coté poste client, l'attribution d'une adresse IP privée est réalisée via DHCP. Une fois cette étape réalisée, le poste est capable d'accéder au site http://nomadisme.grenet.fr afin d'y récupérer un client permettant de se connecter aux boîtiers VPN (cf Chapitre 2.3 pour la description du site).

2.2.3 La solution d'authentification

Si les boîtiers VPN sont chargés de « canaliser et contrôler l'accès aux ressources », l'identification et l'authentification sont cependant réalisées par des éléments supplémentaires.

Chaque établissement est libre d'implémenter une solution qui lui convient mais toutes reposent sur un tronc commun constitué des briques suivantes :

• Un serveur RADIUS [1] ;

• Des répliques partielles LDAP tirées de l'annuaire central des établissements.

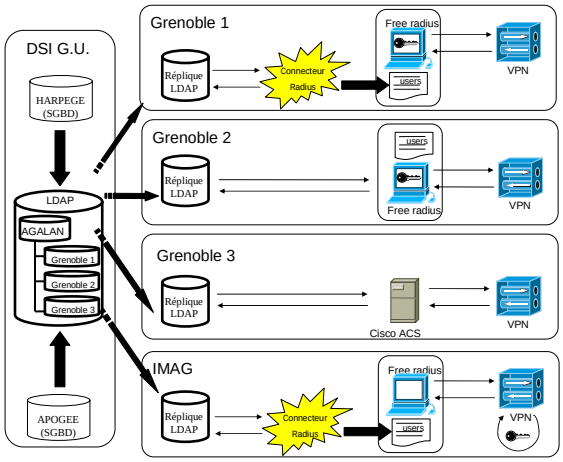

Figure 2 – *L'authentification du nomadisme*

La DSI Grenoble Universités (ex-CICG) en tant qu'organisme interuniversitaire héberge l'annuaire commun des établissements de l'académie de Grenoble. Cet annuaire de technologie LDAP a pour objectif de mettre en œuvre une authentification unique à l'ensemble des établissements [2]. Pour des raisons techniques (que nous ne détaillerons pas ici), chaque établissement dispose d'une réplique partielle de cet annuaire en son sein.

L'identification/authentification des utilisateurs nomades va s'appuyer tout naturellement sur cet annuaire commun. A l'heure actuelle, le schéma de l'annuaire ne permet pas de fournir toutes les données spécifiques liées à une application réseau telle que celle déployée pour le nomadisme (plages d'adresses IP, etc.). En conséquence, les boîtiers VPN s'appuient sur des serveurs RADIUS qui établissent la configuration nécessaire à la connexion du client. Ainsi ce sont les serveurs radius qui interrogent les répliques d'annuaire LDAP d'établissement avant d'autoriser ou non un utilisateur à bénéficier du service nomade.

Pour délivrer l'accès ou le refus à une ressource informatique, le serveur RADIUS peut fonctionner dans différents modes :

• Le serveur RADIUS interroge sa base locale d'utilisateurs. Cette base locale est construite par extraction d'informations de l'annuaire de l'établissement. L'extraction est réalisée par un connecteur spécifique développé par le groupe RADIUS du projet AGALAN. Ce connecteur est aussi en mesure de traiter des données provenant de fichiers à plat ou même d'une base de

données. Cette solution permet de retourner des attributs vers le client RADIUS (concentrateur VPN) notamment dans le but d'attribuer une adresse IP fixe à un utilisateur. C'est la solution adoptée par Grenoble 1 ;

• Le serveur RADIUS interroge l'annuaire LDAP de l'établissement de l'utilisateur via son interface LDAP. Cette solution réalise une authentification simple sans retour d'attribut vers le client. La configuration du serveur est minimale et rapidement opérationnelle. C'est la solution adoptée par Grenoble2 ;

• Grenoble 3 a décidé, dans un premier temps, de déployer la solution RADIUS commerciale ACS du constructeur Cisco. Le principe de fonctionnement est très proche de la solution de Grenoble 2 ;

• Dans le cas de l'IMAG, l'authentification est faite par certificats électroniques directement sur le concentrateur VPN. Le serveur RADIUS agit en tant que serveur d'autorisation. Il dispose donc d'une base locale des utilisateurs autorisés. Cette base locale est construite par extraction d'informations de l'annuaire réalisée par une instance spécialisée du connecteur développé par le groupe RADIUS.

Remarque :

Le schéma de la figure 2 ne représente qu'une vue partielle de tous les organismes adhérant au projet, mais il représente les cas les plus significatifs rencontrés dans le déploiement de la solution nomade.

2.3 Le site http:// nomadisme.grenet.fr

Puisque la première solution de nomadisme proposée s'appuie sur des boîtiers de concentration VPN-IPsec, il est obligatoire d'installer un logiciel client sur les postes de travail voulant s'y connecter.

Pour ce faire, il a été décidé conjointement de créer un site unique regroupant toutes les briques logicielles importantes et les informations nécessaires au bon fonctionnement du nomadisme (pour des raisons de sécurité, l'accès à ce site est soumis à authentification en s'appuyant sur l'annuaire des établissements).

Une fois authentifiés, les utilisateurs trouvent sur ce site une réponse aux questions suivantes :

- Téléchargement d'un client VPN ;
- Cartographie des accès sans fil disponibles sur l'ensemble des campus (et par extension l'ensemble des réseaux filaires disponible également pour un accès à la solution nomade) ;
- FAQ sur le fonctionnement de la solution mais aussi sur des points touchant de près ou de loin au nomadisme (comment rendre son poste fiable, diverses URL de produits libres tels qu'antivirus, suites bureautique…) ;
- Il est également possible de bénéficier d'une mise à jour automatique du client à partir du site.

Les solutions techniques déployées étant laissées au libre choix des établissements, chacun d'eux dispose d'une arborescence propre sur ce site pour la gestion de ses clients.

Ce site créé initialement pour héberger les clients VPN des établissements permet de répondre à d'autres problèmes techniques dans le cadre du nomadisme (serveur DNS, …).

2.4 Avantages et inconvénients de la solution actuelle

La solution retenue pour la gestion des accès nomades est commune en terme d'architecture. Elle fonctionne pour tout utilisateur quelque soit le campus ou le lieu sur lequel il se trouve (maison, étranger, …).

Elle permet à chaque organisme de décliner sur le plan technique la solution qui s'adapte le mieux à ses contraintes : aucune obligation en terme de matériel, protocoles ou mode d'authentification. D'autre part, la solution VPN permet à chaque établissement d'établir une politique d'accès spécifique par type d'utilisateurs. Ce point très important permet, par exemple, de diversifier l'accès aux ressources en fonction de l'appartenance à un profil d'utilisateur ou à un autre.

Exemple de l'Université Joseph Fourier :

- Les étudiants disposent d'un accès aux ressources identique à celui qu'ils peuvent trouver dans les salles libre service ;
- Les personnels retrouvent un accès aux ressources réseaux identique à celui de leur bureau.

Pour la sécurité des échanges, les flux étant chiffrés il n'y a pas de problème pour garantir leur confidentialité. La charte RENATER est également respectée, un système de gestion de traces étant réalisé.

Du coté des inconvénients :

- Le chiffrement grève les performances qui sont déjà moyennes ;
- Le concentrateur VPN est le « maillon faible » (que ce soit en terme de bande passante ou de sûreté de fonctionnement même si des solutions redondantes sont envisageables) ;
- Enfin le point noir principal est l'obligation d'utiliser un client sur le poste de travail.

2.5 Retours d'expérience

Après plus d'un an d'exploitation de la solution, on peut citer les points suivants :

- Tous les usagers ne sont pas dans les annuaires ;

- L'utilisation obligatoire d'un client à télécharger et à installer est un exercice parfois difficile ;
- La gestion des visiteurs n'est pas aisée (congrès, invitation, visite) ;

  Le cas des congrès avec accès « Wi-Fi » n'est pas traité de cette manière.
- Il existe une inégalité de « confort » entre les bâtiments ;

  Certaines structures refusent d'installer le Wi-fi pour ne pas subir la présence dans leurs locaux d'utilisateurs équipés de portables sans fil ;
- On assiste à l'apparition de vols de portables « à l'arraché », de trafic de mots de passe (vol, commerce, pressions…).

Devant la demande croissante d'aide en provenance d'utilisateurs pour du matériel personnel parfois douteux (virus, spyware,…), des solutions sont envisagées à divers niveaux pour fournir une aide sous forme de cellule d'assistance.

Les CRI n'étant responsable que du matériel de l'université, comment prendre la responsabilité d'une intervention sur un poste personnel ? Une expérimentation est en cours à l'Espace de Vie Etudiante (E.V.E.) pour fournir une aide aux utilisateurs de la solution de nomadisme. Cette aide est dispensée par des étudiants préalablement formés par les personnels universitaires.

Du coté du taux d'utilisation, à la fin de l'année universitaire 2004-2005 on comptait plus de 500 connexions/semaine/établissement (selon les endroits, 50 connexions simultanées en permanence).

Globalement tout le monde est satisfait de la solution (étudiants, personnels, CRI,) utilisée de manière croissante.

3 Compléments envisagés pour la solution actuelle

Les premiers retours d'expérience montrent que 90 % des utilisateurs recherchent avant tout un simple accès au web. Cela nous a amené à étudier des solutions répondant à ce type de demande. Le cahier des charges est simple : trouver un moyen de fournir l'accès au web le plus simplement possible mais garantissant un minimum de sécurité aux administrateurs du réseau.

Parallèlement à cette demande, les technologies sans fil évoluent régulièrement (surtout pour la partie assurant la sécurité des communications). Nous nous sommes donc penchés sur les technologies de type 802.11 et plus particulièrement sur les avancées récentes telles que le standard 802.11i [3]. Le sans fil représentant une part importante du nomadisme, il nous a semblé important de continuer à suivre les derniers développements de ces technologies.

Ce chapitre balaye donc différentes solutions que nous avons testées dans l'optique de répondre à ces deux questions, le champ d'investigation est volontairement large (nous n'avons pas voulu nous priver d'une solution miracle capable de répondre à toutes nos questions !). Pour chaque solution testée, nous soulignons les avantages et inconvénients dans notre contexte grenoblois. Le chapitre 4 reprendra ensuite les solutions retenues dans le cadre d'un déploiement opérationnel en complément de l'existant. Dernier point à souligner, les offres disponibles étant abondantes, nous avons découpé les différents tests en sous-groupes suivant une taxonomie « maison » … ouverte bien entendu à toute discussion.

3.1 Les « portails d'accès » sans client

Les solutions que nous qualifions de « portail d'accès » (souvent appelés portails captifs) sans client offrent l'avantage d'être indépendantes des logiciels et du système d'exploitation des postes clients. On dispose rapidement d'un accès HTTP sur tous types de systèmes d'exploitation. Il n'y a aucune intervention ou ajout de logiciel sur le poste.

3.1.1 « Portail d'accès travaillant au niveau de l'infrastructure »

Nous rangeons sous ce terme les « portails captifs » qui s'appuient sur l'ouverture de règles de filtrage (IPtables). Ces règles filtrent l'adresse MAC ou un couple adresse MAC adresse IP de l'utilisateur : un couple que l'on peut facilement usurper ! S'il n'y a pas de demande de fin de connexion, la règle de filtrage reste appliquée et l'accès reste ouvert.

Ces portails ne forcent pas le chiffrement des données. Or, certains sites web proposent encore de s'authentifier en HTTP (certains webmail). Le mot de passe peut alors être capturé en accès sans fil et compromettre ainsi l'ensemble des systèmes d'informations.

Autre contrainte technique (qui s'avère problématique dans notre architecture actuelle), le portail, qui repose sur le filtrage d'adresse MAC, impose de le placer dans le même vlan que les bornes.

La solution M0n0wall

M0n0wall [4] est un projet basé sur un ensemble d'outils disponibles sous FreeBSD.

La solution « portail captif » de M0n0wall permet :

- Un démarrage sur CDRom (pas de modification possible mais sauvegarde de la configuration sur un support externe) ;
- Une administration par une interface web très lisible ;
- Un filtrage complet (sur socket avec numéros de ports) permettant l'utilisation de nombreux services ou applications autres que le web ;

- Une authentification par session HTTPS (à partir de la version 1.2 beta 7) ;
- Un enregistrement de traces succinctes (IPtables).

Il existe tout de même des inconvénients encore incontournables :

- De nombreux bugs ont été rencontrés (versions bêta 1.2b7 et 1.2b8) entraînant des plantages ;

  La version stable (1.1) ne propose pas toutes les fonctionnalités requises dans notre cahier des charges (pas d'authentification HTTPS), elle a donc été écartée d'emblée.
- la fermeture de session HTTPS (popup après authentification) ne ferme pas les filtres. De plus il faut accepter les popups pour pouvoir fermer la session : il y a possibilité d'usurpation d'une machine autorisée ;
- le filtrage est basé sur l'adresse physique (adresse MAC), ce qui ne permet pas un déploiement mutualisé (M0n0wall ne peut être placé après un ou plusieurs routeurs) ;
- dans la configuration utilisée à la DSI Grenoble Université, l'accès à l'interface d'administration se fait par l'interface connectée sur le réseau privée (coté réseau sans fil, ce qui le rend plus sensible a une attaque) ;
- Les traces ne fournissent pas les tables de translation : il est impossible de retrouver une machine attaquante derrière M0n0wall (la seule possibilité est de retrouver toutes les personnes connectées au moment de l'incident).

La solution Pfsense

La solution Pfsense [5] est techniquement identique à la solution M0n0wall hormis l'installation qui se fait sur un disque dur classique. Ce critère lui permet d'offrir un système de cache, et donc des performances supérieures à M0n0wall. C'est, dans notre contexte, le seul critère différentiateur pouvant nous amener à la préférer par rapport à une solution de type M0n0wall.

Il existe bien d'autres solutions du même type, mais nous ne les avons pas testées par manque de temps. On peut citer par exemple des solutions telles que Aruba, NoCathAuth, ChiliSpot, Cisco SSG redirect.

3.1.2 « Portail d'accès de niveau applicatif »

Nous rangeons sous cette appellation les portails qui réalisent un traitement au niveau de la couche application. Un « portail d'accès de niveau applicatif » offre l'avantage dans notre contexte de pouvoir être déployé n'importe où dans le réseau.

La solution Talweg

Talweg [6] est un projet développé par le CRIUM (CRI de l'Université de Metz). La version testée est 0.3 ce qui témoigne de la jeunesse du produit. Toutefois, ses qualités sont indéniables et son mode de fonctionnement est très sécurisé : Talweg encapsule tout le trafic émis par le client dans une session SSL.

L'utilisation de Talweg est intuitive : en tapant n'importe quelle URL (ou en cliquant sur n'importe quel lien) dans un navigateur, Talweg intercepte la requête. Si l'utilisateur n'est pas encore authentifié, un formulaire s'affiche (après acceptation du certificat du serveur si ce dernier n'est pas validé par une autorité de confiance dans la liste du navigateur) demandant un login et un mot de passe.

Ensuite, tous les liens sont automatiquement réécrits.

Dès la fermeture du navigateur, la session SSL est rompue, il est ainsi impossible pour une personne malveillante de récupérer la session d'un utilisateur précédemment connecté sur le poste.

Talweg présente de nombreux points intéressants :

- Une authentification sécurisée ;
- Du multifenêtrage ;
- Une communication chiffrée entre le serveur et le client (tunnel SSL) ;
- Un fonctionnement mutualisé dans notre environnement mais qui nécessite la mise en œuvre de routage politique (nous verrons comment dans le chapitre 4) ;
- Des traces très détaillées (de type proxy web : date, utilisateur, URL complète) ;
- La possibilité d'utiliser ses « liens favoris » (en lecture) ou des liens par copier/coller.

En revanche, il y a des points à améliorer pour en faire la solution idéale :

- Talweg ne fonctionne pas avec certains javascript, ActiveX et ne fonctionne pas du tout avec les pages ASP ;
- Il n'y a pas de gestion de la durée de connexion des utilisateurs ;
- Il est impossible d'enregistrer des liens issus de la réécriture des URLs.

La solution Squid en mode transparent

SQUID [7] est une application "serveur proxy cache", c'est à dire un système de relais de requêtes HTTP et HTTPS.

Afin d'éviter aux utilisateurs une quelconque configuration, nous avons pensé utiliser le serveur SQUID en mode transparent : ce mode permet de relayer toutes les trames web. Problème : il n'est pas possible d'utiliser de mécanisme d'authentification des utilisateurs dans ce mode. Cela n'est malheureusement pas envisageable pour des machines nomades (la fonctionnalité d'authentification est semble-t-il à l'étude pour la prochaine version).

3.1.3 Les Proxies Web

Pour fonctionner correctement, ces proxies web nécessitent de mettre en place un mécanisme de configuration automatique relayé soit par DNS, soit par DHCP. Le poste client est ensuite « conscient » qu'il doit passer par le proxy pour toute requête web.

Le mécanisme de configuration automatique doit être pris en charge soit au niveau du système, soit au niveau des applications du coté du client :

- La configuration automatique de proxy en DHCP fonctionne uniquement pour des postes clients Microsoft Windows ;
- La gestion de configuration automatique de proxy par DNS ne fonctionne pas pour tous les butineurs sous Mac OS X (fonctionnement validé avec Mozilla mais pas avec safari et internet explorer).

Le système de configuration automatique n'étant pas disponible pour toutes les populations nomades, il n'est pas envisageable de le déployer. A cela s'ajoute un problème de gestion du chiffrement des flux HTTP laissant apparaître les mots de passes en clair.

Microsoft ISA Server 2004

Microsoft ISA Server 2004 est un proxy cache et firewall commercial. Les fonctionnalités de proxy cache ont l'avantage de gérer, outre les navigateurs web, des applications comme msn messenger. De nombreuses options sont disponibles mais aucune n'offre le chiffrement des flux HTTP.

Il existe beaucoup d'autres solutions que nous n'avons pas testé : bluecoat, Squid, EZproxy, iPrism.

3.2 Les portails avec « client léger »

Un client est dit léger si les postes ne nécessitent pas de droits administrateurs, et de redémarrage de la machine.

Rappel : nous sommes toujours dans l'optique de trouver une solution offrant un simple accès http. Certaines offres « clients léger » font plus qu'un simple accès HTTP, mais il faut alors des droits évolués sur le poste.

Inconvénient majeur, ils dépendent souvent d'une couche logicielle installée sur le poste client ou parfois même du système. Certains fonctionnent avec des ActiveX, d'autres nécessitent une certaine version de l'interpréteur Java.

3.2.1 VPN Cisco 3030 en mode webSSL

Le VPN Cisco 3030 offre un mode SSL qui après de nombreux tests est compatible avec tous les sites web. La navigation sur le web se fait à l'aide d'un champ de saisie de l'URL dans un popup, ou sur la page web d'accueil ouverte après authentification.

Il est loin cependant d'offrir une solution idéale dans notre contexte :

- L'interface d'utilisation n'est pas intuitive, donc difficilement exploitable par un nomade invité ;
- Les performances en WebSSL ne sont pas très convaincantes ;
- Il gère un nombre restreint d'utilisateurs simultanés ;
- Les logs ne permettent pas de tracer un utilisateur ;
- Il n'y a pas de gestion de multi fenêtrage.

3.2.2 Aventail en mode SSL

Le produit Aventail EX-1500 a été écarté car il n'a pas non plus répondu à nos besoins. Le mode SSL limite, dans sa version client léger, l'accès à des sites web **déjà** référencés dans un profil.

3.2.3 Array Networks SPX 3000 en mode SSL

Le boîtier d'Array Networks SPX3000 offre un mode SSL qui après authentification ouvre une page d'accueil web sur laquelle on saisit une URL. Une fois saisie, le navigateur ouvre sur le site l'URL correspondante avec un composant de navigation Java. Ce dernier permet de revenir à la page d'accueil ou de saisir l'URL dans une zone de texte. A noter de nombreux aspects positifs :

- L'interface de navigation Java est conviviale bien que pas assez intégrée dans le navigateur ;
- Les logs détaillés permettent de tracer les utilisateurs correctement ;
- Les performances sont excellentes.

Il y a cependant encore des points non résolus :

- Le produit ne fonctionne pas avec certains sites (www.microsoft.com, www.hotmail.com, …) ;
- Il ne prend pas en compte les liens favoris du navigateur et ne permet pas d'en enregistrer ;
- Il ne gère pas de multi-fenêtres.

3.2.4 F5 - Firepass 1000 en mode SSL

Le Firepass 1000 de chez F5 offre un mode de client léger très succinct à savoir que l'URL ne peut-être saisie que dans la page d'accueil. L'interface de l'utilisateur est complexe. Le boîtier offre des possibilités avancées en SSL, cependant elles requièrent l'installation en tant qu'administrateur d'activeX ou d'applet Java.

Il existe beaucoup d'autres solutions que nous n'avons pas pu tester : Juniper Netscreen, AEP networks Netilla (cf demo sur le site http://www.netilla.com), Symantec 4400 (des renseignements pris par téléphone indiquent que le boîtier se destine uniquement à un usage de type Intranet en VPN-SSL), Menlo logic, Net Swift, iGate Safenet SSL-VPN, eGAP SSL-VPN, Arkoon, Permeo Technologies (approche très intégrée mais ne fonctionne qu'avec des ActiveX), SSL Explorer, OvisGate SSL, CheckPoint…

3.3 Les portails avec « un client lourd »

Toujours dans notre taxonomie « propriétaire », un client est dit lourd si l'installation nécessite les droits administrateurs ou un redémarrage du poste de travail.

La solution retenue il y a 2 ans et actuellement en place (voir paragraphe 2.2) fait appel à un « portail » avec un client lourd du type VPN IPsec.

Nous n'avons pas approfondi ce point car la solution en place est dans l'ensemble satisfaisante. Elle s'appuie majoritairement sur des boîtier VPN Cisco 3030. Les clients VPN sont gratuits et disponibles pour un grand nombre d'OS : toutes les plateformes Windows, Mac OS X, Linux, Solaris. Le constructeur assure une mise à jour régulière et gratuite des versions logicielles de ces divers produits (boitiers vpn, clients, …).

Il existe beaucoup d'autres solutions que nous n'avons donc pas testé : NuFW, CyberGuard, bluesocket, Ucopia…

3.4 Le WPA & WPA2 (802.11i)

Comme annoncé en début de ce chapitre, et après avoir étudié des solutions permettant un accès web simple, nous avons tenu à étudier l'évolution des solution d'accès purement sans fil, en l'occurrence le standard 802.11i.

Comme nous l'avons précisé également au paragraphe 2.2.2, le choix majoritaire de bornes sans fil intégrant des fonctions évoluées permet de migrer assez naturellement vers du 802.11i (les bornes retenues dans notre déploiement sont capable d'offrir ce type de solution éventuellement par simple upgrade logiciel). Il reste cependant des points techniques à valider pour la mise en œuvre de ce type de solution.

3.4.1 Le Fonctionnement WPA et WPA2

Le mécanisme d'authentification WPA et WPA2 est le même : il s'agit d'EAP. Seules les méthodes de chiffrement diffèrent (chiffrement TKIP basé sur RC4 pour WPA et chiffrement CCMP basé sur AES pour WPA2). Par la suite, le terme WPA pourra être utilisé de manière générique pour désigner une solution de ce type (Un SSID[1] « WPA » peut offrir un chiffrement conforme WPA et/ou WPA2 en fonction du client sans configuration supplémentaire).

Pendant la phase d'authentification, un point d'accès ne laisse passer aucun protocole autre que EAP. C'est seulement lorsque l'authentification est positive que le NAS (Network Access Server) autorise l'utilisation de protocoles différents. Les échanges EAP correspondent à la méthode d'authentification choisie. Notre choix s'est porté sur EAP-TTLS car il représente un bon compromis sécurité/déploiement. EAP-TTLS requière l'utilisation d'un certificat coté serveur et d'un client compatible coté équipement nomade.

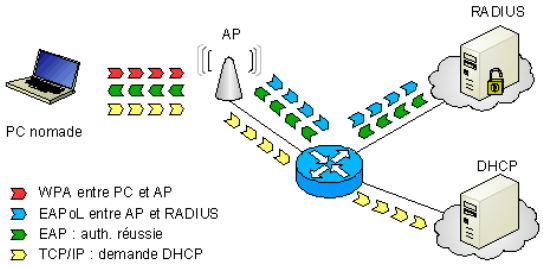

Figure 3 - *Architecture WPA*

Cette méthode participe fortement à la robustesse du réseau qui ne peut être attaqué qu'après une authentification réussie. De plus, les informations transmises entre l'équipement mobile et le point d'accès sont chiffrées avec une clef qui est changée périodiquement, ce qui rend l'écoute inutile.

En revanche, l'authentification et l'affectation d'adresse étant séparés, il est nécessaire de mettre au point un système qui établisse la correspondance entre ces deux éléments afin d'assurer une certaine traçabilité des connexions et par extension des utilisateurs.

3.4.2 La gestion des traces

A l'heure actuelle, un problème majeur d'une solution WPA est le problème de traçabilité des utilisateurs : assurer la correspondance entre l'authentification effectuée par un serveur RADIUS et l'adresse IP fournie par un serveur DHCP. En effet, le mécanisme RADIUS intègre l'affectation d'une adresse IP mais seulement pour les protocoles point à point (PPP). Dans le cas d'un accès sans fil, on doit s'appuyer sur un serveur DHCP pour fournir les adresses IP. Le serveur RADIUS dans le cadre d'un accès sans fil n'a donc pas la visibilité de l'adresse IP affectée à un utilisateur.

Pour régler ce problème de dispersion d'informations, nous avons récupéré et adapté un script développé par Rock PAPEZ membre du groupe de travail Eduroam [8].

Ce script s'appuie sur le langage Perl. Il utilise une base de données mySQL et les fonctionnalités de syslog des systèmes linux. Il résout le problème de synchronisation des données grâce aux accès concurrents et aux requêtes de recherche.

D'un coté, on obtient les informations collectées par RADIUS :

- L'identifiant de l'utilisateur ;
- La date et l'heure d'authentification ;

[1] SSID : Service Set IDentifier

- Les adresses MAC du terminal et du point d'accès.

De l'autre, le serveur DHCP fournit les données suivantes :

- L'adresse MAC et IP affectée au terminal ;
- La date / heure d'attribution de l'adresse IP.

Le script lance deux démons sur le serveur :

- Un démon dont le rôle est de récupérer les données du serveur DHCP ;
- Un démon dont la fonction est de vérifier régulièrement sur le point d'accès la table des associations (via le protocole SNMP).

Le serveur RADIUS écrit un nouvel enregistrement à chaque nouvelle authentification. Le script surveillant le fichier syslog vient compléter cet enregistrement lorsque le serveur DHCP fournit une adresse IP à l'adresse MAC reconnue.

Lorsque le supplicant (ou poste nomade) se déconnecte, le point d'accès en informe le serveur RADIUS qui enregistre l'heure de déconnexion dans la base.

Ainsi toutes les informations utiles à la gestion des traces produites par un utilisateur sont retrouvées et synchronisées.

L'intérêt supplémentaire d'enregistrer dans la base l'identifiant du point d'accès est de pouvoir retrouver sur quel point d'accès l'utilisateur s'est connecté. Il est même possible de "suivre" un déplacement d'un point d'accès à un autre (grâce au mécanisme de handover utilisé).

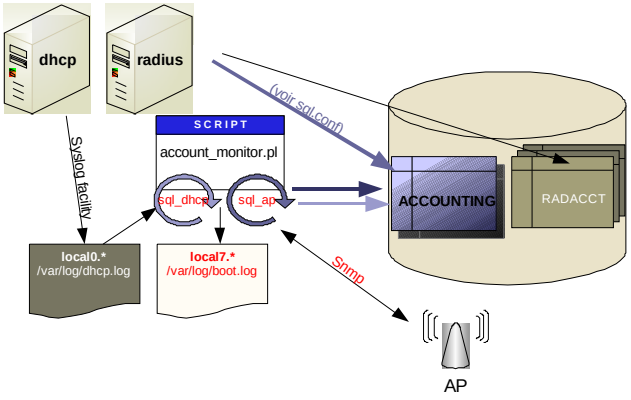

Figure 4 – *Fonctionnement du script*

Enfin il est possible d'adjoindre aux identifiants le caractère arobase (@) ce qui permet de faire appel à la notion de domaine (realm en anglais). Le script enregistre alors l'identifiant et son domaine d'appartenance, ce qui est très pratique lorsque l'on veut mettre en place une infrastructure d'authentification à plusieurs niveaux (cf chapitre suivant).

La gestion des traces est, de notre point de vue, un problème important qu'il fallait régler absolument pour envisager un déploiement opérationnel du WPA. De part l'utilisation des scripts décrits ci-dessus nous considérons que c'est un point qui est désormais réglé. Dernier point très positif, la solution de gestion des traces est libre de droits et disponible pour toute entité désirant l'utiliser (nos scripts sont disponibles à tous ceux qui veulent les utiliser).

3.4.3 Conclusion sur le WPA

Cette solution prometteuse offre les avantages suivants :

- Pas d'accès au réseau avant authentification ;
- Mécanisme d'authentification indépendant des serveurs RADIUS intermédiaires ;
- Après authentification, l'utilisation d'un client VPN IPsec n'est pas bloquée ;
- Solution ouverte et gratuite (utilisation d'un standard, logiciel client gratuit) ;
- Sécurisation des flux efficace (chiffrement TKIP ou CCMP) ;
- Gestion de l'affectation dans un vlan choisi ;
- Journaux (logs) contenant les données essentielles (identifiant, heures de connexions, point d'accès utilisé, adresse MAC et adresse IP) ;
- Intégration au projet ARREDU [9] en accord avec la charte RENATER et les réseaux d'éducation et de recherche.

Elle ne peut toutefois pas faire oublier les inconvénients listés ci-après :

- L'installation d'un client est nécessaire pour toute autre authentification que EAP-PEAP ou EAP-TLS sous Windows (l'installation est toujours nécessaire pour les linux/unix et MacOs) ;
- Les droits d'administrateur sont nécessaires pour l'installation du client ;
- La mise en œuvre est délicate pour les administrateurs des universités (nombreuses applications à configurer) ;
- Il est nécessaire de connaître la procédure à suivre (impossible d'accéder au réseau avant l'authentification pour récupérer le logiciel client) ;
- La solution doit utiliser des adresses de réseaux publiques (adresses IP routables).

4 La nouvelle solution

4.1 Objectifs

La DSIGU se pose en terme de pilote pour les évaluations de solutions nomades pour les universités de l'académie.

Ainsi, suite à toute cette série de tests unitaires, nous avons proposé au groupe inter-universitaire s'occupant du nomadisme une architecture nouvelle. La solution proposée pérennise la solution VPN précédemment déployée, elle propose d'autres services et prépare l'avenir.

4.2 Authentification : utilisation de Proxy-RADIUS

Le protocole RADIUS permet le chaînage de serveurs : cette fonctionnalité est un avantage considérable dans un environnement comportant de multiples intervenants. Ainsi, chaque université conserve la gestion de ses utilisateurs et de leurs droits associés, tout en bénéficiant de la mutualisation des accès et des serveurs fournis par d'autres établissements.

Nous avons donc commencé à déployer une infrastructure de serveurs RADIUS qui permet aux utilisateurs des différentes universités grenobloises de s'authentifier et d'être reconnus sur n'importe quelle université de l'académie. Le projet a également pour but d'être compatible avec le projet national du CRU ARREDU s'inscrivant à plus large échelle dans le projet européen Eduroam. En effet, si notre architecture initiale à base de VPN-IPSec pouvait se passer d'une telle solution de proxy, les standards et projets d'échanges qui émergent actuellement nous a poussé à proposer ce type de service.

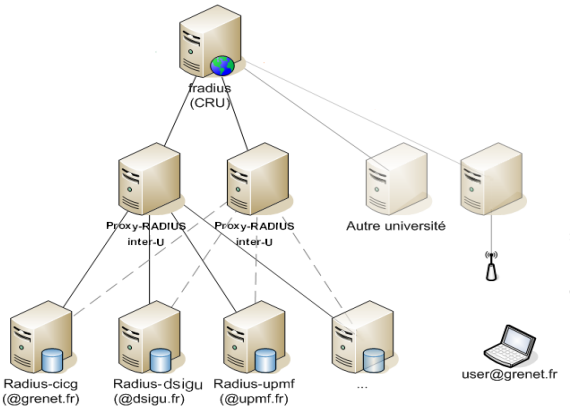

Figure 5 - *Système Transversal d'Authentification Répartie*

4.3 La solution d'accès

Pour ce qui est de l'accès filaire, rien n'est remis en cause : la solution VPN garde tout son sens quelque soit le scénario nomade de nos diverses populations (chercheur en déplacement voulant accéder à ses ressources, salles libre service pour étudiants, etc.). Les évolutions en terme de méthode d'accès sont surtout prévues pour le sans fil.

Pour ce faire, trois SSID sont proposés :

- Le SSID Accueil

Ce SSID est signalé par les bornes. Il est ouvert, sans authentification ni chiffrement, et permet d'accéder au site http://nomadisme.grenet.fr pour avoir des informations sur la solution de nomadisme ainsi que sur le réseau sans fil (une fois authentifié, téléchargement des clients VPN, carte des points d'accès,…).

Dans cette configuration, deux méthodes d'accès sont disponibles pour les utilisateurs de l'académie :

- Soit au travers d'une connexion VPN IPsec pour ceux qui ont installé le client VPN ;
- Soit à partir d'un « portail captif ».

La solution retenue au niveau du portail captif est pour le moment talweg avec une politique de routage « forcé » : tout trafic HTTP sortant de ce vlan est obligatoirement redirigé vers le portail.

Ce routage très souple présente toutefois l'inconvénient majeur d'utiliser plus de ressources CPU du routeur.

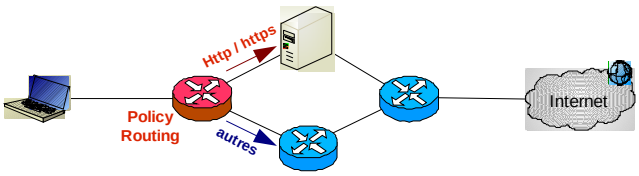

Figure 6 – *Fonctionnement du « policy routing »*

Remarque : les salles libre service équipées en filaire peuvent éventuellement fonctionner sur ce principe.

- Le SSID eduroam

Ce SSID est signalé par les bornes. Il implémente les méthodes d'accès WPA & WPA2 (802.11i). Pour accéder au réseau il faut que la borne ait validé l'authentification du client dans le cadre du projet ARREDU. La confidentialité des données est assurée par un chiffrement CCMP ou TKIP entre le client et la borne. Une fois le client connecté avec son adresse IP, ce dernier est, pour le moment, libre d'accèder à Internet (politique de sécurité en cours de définition dans le groupe national ARREDU). Le nom du SSID est eduroam (et non ARREDU) car le but est d'intégrer à terme le projet européen du même nom.

Remarques :

Un utilisateur faisant partie d'une des Universités Grenobloise peut à travers ce SSID accéder à ses ressources internes au travers de la solution VPN-IPsec.

Ce SSID permet également d'offrir de l'IPv6 et des services tels que la mobilité IPv6 (des tests concluants ont été réalisé dans ce sens sur notre pilote).

- Le SSID téléphonie-wlan

Dans le cadre d'un autre type de nomadisme, les bornes sont également utilisées pour faire de la téléphonie sans fil IP. Le SSID est caché. La méthode d'accès par clé WEP ne présente pas une grande faille de sécurité puisque l'accès est restreint à une passerelle téléphonique. Regrouper la voix et la donnée sur une même infrastructure sans fil présente pour nous un réel intérêt technique et financier.

4.4 Synthèse de la solution

La solution initiale retenue pour régler la problématique du nomadisme n'est pas remise en cause à moyen terme. Nous l'avons seulement enrichie d'une part pour répondre à des populations plus diverses d'utilisateurs, et d'autre part pour suivre l'évolution des technologies essentiellement en ce qui concerne le sans fil. On peut d'ailleurs faire la synthèse de la solution proposée sous un angle retraçant les caractéristiques d'accès Wi-Fi :

- Un vlan d'accueil, orienté pour les utilisateurs de l'académie. L'accès aux ressources se fait via un concentrateur VPN (on pérennise la précédente solution de nomadisme) ou on utilise un « portail captif » purement web après authentification ;
- Un vlan compatible avec les spécifications ARREDU (standard WPA et WPA2). Cette solution prépare l'avenir d'une solution sans-fil identique au niveau national puis européen. Cette solution permet à « nos » nomades de disposer à terme d'un accès dans toute entité tierce participant au projet ARREDU puis Eduroam ;
- Un vlan téléphonique dédié répondant aux actuelles spécificités de la téléphonie sur IP.

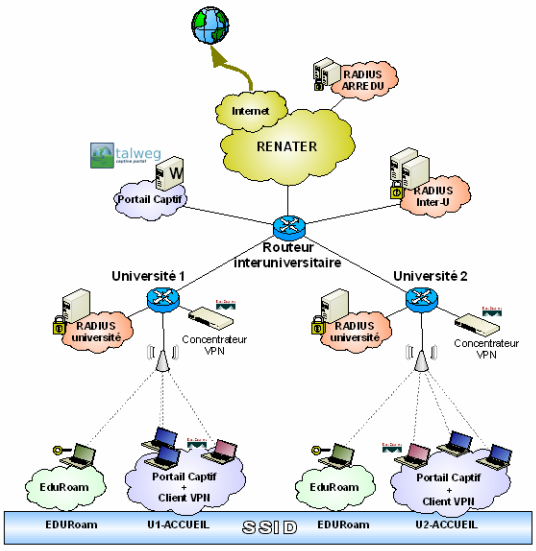

Figure 7 – *Synthèse de l'architecture pour le nomadisme*

4.5 Les problèmes à régler

Aucun produit d'accès http « sans client » testé ne répond intégralement à nos besoins. Des tests sont toujours en cours, (à l'heure de l'écriture de ces pages la solution talweg est mise à disposition).

Le nomadisme et la prolifération des virus pose également le problème de la salubrité de postes avec des systèmes hétérogènes : comment la réaliser dans un environnement ouvert ? Beaucoup de travail reste à faire sur ce sujet.

5 Conclusion

L'usage des VPNs et des portails captifs se dessine plus dans un usage à court terme vis-à-vis d'un accès sans fil. Ces solutions ont permis de palier à un problème de jeunesse de l'ASFI pour la sécurité et l'authentification.

A moyen terme, le 802.11i est un bon candidat pour les solutions sans fil. Il offre le niveau de sécurité que l'on attendait (la gestion des traces est suffisante avec la mise en place de scripts dédiés). La cœxistence entre la solution préconisée par le projet ARREDU et le VPN garde cependant tout son sens : depuis tous les sites adhérents à ARREDU « nos » utilisateurs devraient pouvoir monter un tunnel IPsec pour accéder à leurs ressources informatiques internes. Le VPN reste également d'actualité pour un accès en toute sécurité à ses ressources depuis un site distant « filaire » ou non (de chez soi, d'une cité universitaire, d'un hôtel).

Pour démocratiser le 802.11i, nous attendons cependant un client 802.11i nativement intégré aux postes de travail pour s'affranchir des problèmes de déploiement.

Enfin, à plus long terme, on peut également envisager l'utilisation d'IPv6 (sur les réseaux sans fil ou non) avec la fonctionnalité de mobilité. Cette dernière permettrait non seulement de traiter les problèmes de mobilité téléphonique ou vidéo, mais elle pourrait également régler le problème de politique d'accès réglé actuellement par les solutions de type VPN IPsec en IPv4.

Or, il semblerait que Microsoft envisage d'inclure ces deux fonctionnalités (mobileIp v6 et client 802.11i) dans la prochaine version de leur système d'exploitation client dès 2006…l'échéance est proche, il est important de s'y préparer dès à présent.

Bibliographie

[1] Jonathan Hassel, RADIUS, O'REILLY, ISBN : 0-596-00322-6 (Octobre 2002).

[2] J. Eudes, G. Forestier, E. Payan, Annuaire LDAP ou SGBD : quelles solutions pour un référentiel unique ? *les actes de Jres 2001*, page 269, Lyon, (12/2001).

[3] Aurélien Geron, Wi-Fi deployment et sécurité (le WPA et la norme 802.11i, DUNOD, ISBN : 2-10-048433-8 (2004).

[4] http://m0n0.ch/wall/

[5] http://www.pfsense.com/

[6] http://sourcesup.cru.fr/talweg/

[7] http://www.squid-cache.org

[8] http://www.eduroam.org

[9] www.cru.fr/nomadisme-sans-fil/arredu