Recommandations de sécurité destinées aux administrateurs systèmes et réseaux du CNRS pour l'installation de réseaux locaux sans fil (“ WiFi ”)

Jean-Luc Archimbaud, Catherine Grenet, Marie-Claude Quidoz

Recommandations de sécurité destinées aux administrateurs systèmes et réseaux du CNRS pour l'installation de réseaux locaux sans fil (« WiFi »)

Jean-Luc Archimbaud, Catherine Grenet, Marie-Claude Quidoz
CNRS / UREC – Novembre 2004

1. Introduction

1.1 Contexte

La connexion sans fil au réseau d'un laboratoire CNRS, en particulier pour les ordinateurs portables, offre une souplesse indéniable aux utilisateurs. Le personnel et les visiteurs de passage expriment de plus en plus ce besoin et l'administrateur systèmes et réseaux doit essayer d'y répondre.

La mise en œuvre d'une infrastructure de réseau sans fil peut répondre à des besoins différents, mais non exclusifs les uns des autres : connexion au réseau de lieux impossibles ou trop coûteux à câbler, par exemple un monument historique ; connexion provisoire dans le cadre de travaux ; connexion plus facile des utilisateurs dans des lieux tels que salles de réunion ou bibliothèques, ou dans le cadre de colloques ou de congrès – c'est l'utilisation la plus courante dans un laboratoire du CNRS. Il ne faut cependant pas perdre de vue que dans l'état actuel de la technique, les limites des réseaux sans fil en termes de fiabilité et de débit en font un réseau d'appoint, destiné à compléter le réseau filaire et non à le remplacer.

La technique des réseaux sans fil repose sur un mode de transport des données par ondes hertziennes et est particulièrement adaptée pour des ordinateurs nomades. Ces deux caractéristiques engendrent des vulnérabilités importantes en terme de sécurité. Néanmoins, si une réflexion est conduite avant l'installation d'un réseau sans fil, il est possible de minimiser ces risques en utilisant les solutions techniques d'ores et déjà disponibles.

Par ailleurs, le petit nombre de fréquences disponibles rend difficile l'exploitation de réseaux distincts dans un même espace. Or, de nombreux déploiements sont en cours ou en projet sur les campus universitaires : si vous êtes sur un tel site, prenez contact avec le CRI local avant d'envisager tout déploiement de borne.

1.2 But du document

L'administrateur doit donc construire une architecture (où mettre les bornes dans son réseau ?), utiliser certaines fonctions de sécurité sur les bornes, et définir des procédures pour la connexion des stations. Le but de ce document est de donner des recommandations pour ce travail, dans le contexte d'un laboratoire du CNRS, et sans décrire en détail les techniques sous-jacentes.

Ce document n'aborde que les aspects sécurité spécifiques aux réseaux sans fil. L'étude nécessaire pour avoir un bon service de transport réseau (une bonne couverture radio, un signal non perturbé, un débit suffisant par utilisateur...) n'est pas l'objet de ce document. Pour une étude de ce type, on pourra se reporter à [1].

Ces recommandations sont destinées à des administrateurs qui ne sont pas des spécialistes du domaine du WiFi (les experts trouveront eux-mêmes leurs propres solutions), dans un laboratoire c'est-à-dire un lieu où les ressources humaines et financières sont faibles, ce qui conduit à faire des compromis en termes de sécurité. Nous ne décrivons pas la solution idéale mais celles que nous considérons réalisables et acceptables dans un environnement de recherche. Les recommandations sont évidemment à adapter à l'environnement et aux besoins, chaque site ayant ses spécificités.

1.3 Rappel des deux risques principaux liés aux connexions sans fil

Les réseaux sans fil présentent deux vulnérabilités principales que n'ont pas ou moins les connexions filaires.

Les écoutes. Les données sont transportées par ondes hertziennes, en mode diffusion, et par défaut en clair. De plus il est quasiment impossible de restreindre la propagation des ondes hertziennes à un périmètre donné. Les communications peuvent dont être facilement écoutées. Le même risque existe avec des concentrateurs Ethernet mais c'est moins simple et plus visible car il faut que le curieux accède à une prise murale dans un bureau, ce qui n'est pas nécessaire avec un réseau sans fil puisqu'il suffit souvent d'être dans le couloir ou parfois dans la rue.

Les connexions illicites. Sans configuration particulière des bornes, n'importe qui peut s'y connecter et donc accéder au réseau, éventuellement aux réseaux internes selon l'endroit où sont connectées les bornes. Cela veut dire : pouvoir accéder aux serveurs internes, utiliser gratuitement l'accès Internet du laboratoire, mais aussi introduire des virus et des vers dans le réseau interne. La connexion des portables sur le réseau filaire amène les mêmes vulnérabilités mais comme précédemment l'intrus est plus facilement détectable.

2. Mécanismes de sécurité sur les réseaux sans fil

Au fil du temps un certain nombre de mécanismes de sécurité sont apparus sur les réseaux sans fil.

- Non-annonce de l'identifiant de réseau (*Service Set Identifier* ou SSID) : cet identifiant est une chaîne de caractères dont la valeur par défaut est prédéfinie par le constructeur et qui peut être modifiée. Par défaut il est diffusé en permanence par les points d'accès. Il est généralement possible de désactiver la diffusion de l'identifiant ce qui empêche un utilisateur qui ne le connait pas de se connecter à la borne.
  Ce mécanisme ne fournit qu'une sécurité relative car l'identifiant de réseau apparaît en clair dans les trames dès qu'une station est connectée au point d'accès, et peut donc être facilement écouté.

- Contrôle d'accès par adresse MAC : la borne contient la liste des adresses physiques des stations autorisées à s'y connecter.
  Ce mécanisme présente deux inconvénients : d'une part il nécessite de rentrer les adresses dans les points d'accès, ce qui peut être difficile à gérer si les équipements sont nombreux ; d'autre part, il n'est pas fiable dans la mesure où il est relativement aisé de modifier une adresse physique.

- Authentification et chiffrement WEP : un code « secret » permet d'accéder à la borne. Cette clé est saisie manuellement dans le point d'accès et dans les stations. Elle permet également de chiffrer les données échangées.
  Ce mécanisme de sécurité est celui initialement prévu dans la norme IEEE 802.11 [2]. Il présente deux inconvénients. D'une part, gérer manuellement des clés n'est réaliste que pour un petit nombre d'équipements. D'autre part, les défauts intrinsèques du WEP font que la clé peut être trouvée par écoute du réseau avec des logiciels du domaine public.

Ces trois mécanismes, malgré leurs défauts, ont l'avantage de fonctionner avec tous les équipements, cartes ou points d'accès. L'utilisation de WEP en particulier annonce clairement que le réseau sans fil est un réseau privé, et la découverte de la clé demande tout de même une certaine expertise.

Plus récemment, d'autres mécanismes sont apparus pour pallier les défauts du WEP.

- Authentification 802.1X et WEP dynamique : le protocole 802.1X [3] permet l'authentification d'un client (une machine voulant se connecter au réseau) par un serveur d'authentification avant que lui soit accordé l'accès au réseau. L'équipement d'accès au réseau (commutateur Ethernet ou point d'accès sans fil) relaie les trames d'authentification entre le client et le serveur et ne permet l'accès au réseau que lorsque l'authentification a réussi. De plus, le serveur génère une clé de chiffrement par utilisateur et par session. Cette clé est utilisée pour le chiffrement des communications entre le point d'accès et le client.
  802.1X permet d'utiliser plusieurs protocoles d'authentification. Ces protocoles sont encapsulés dans le protocole EAP (*Extensible Authentication Protocol*) [4]. Les protocoles d'authentification utilisables sur les réseaux sans fil sont :
    - TLS [5] qui permet l'authentification mutuelle du serveur et du client par certificat X.509
    - TTLS [6] : authentification du serveur par certificat et utilisation du tunnel chiffré créé par TLS pour transmettre un autre protocole d'authentification tel que PAP ou MD5
    - PEAP [7] : similaire à TTLS, le protocole d'authentification encapsulé étant MS-CHAP

- WPA [8] est une spécification promue par un groupement de constructeurs et constitue un sous-ensemble de la norme IEEE 802.11i (voir ci-dessous). Le chiffrement WEP est remplacé par le chiffrement TKIP, qui est une amélioration de WEP et ne permet pas, en principe, la découverte de la clé par écoute du réseau. Deux modes de fonctionnement sont définis : le premier, dit « Entreprise », reprend les mécanismes d'authentification et de gestion des clés par 802.1X ; le second, dit « à clé pré-partagée » (WPA-PSK), fonctionne de la même manière que WEP, c'est-à-dire qu'il faut entrer les clés manuellement dans la borne et dans les cartes.

- enfin, la norme IEEE 802.11i ([9], [10]) a été ratifiée en juin 2004. Elle reprend le mécanisme d'authentification 802.1X et introduit le chiffrement CCMP, fondé sur l'algorithme AES. Elle introduit en outre des mécanismes de protection du trafic de contrôle, qui permettront d'éviter un certain nombre d'attaques en déni de service auxquels tous les réseaux sans fil sont actuellement vulnérables.

Ces mécanismes offrent un très bon de niveau de sécurité mais au prix d'une complexité de mise en œuvre accrue. Ils nécessitent (sauf pour WPA-PSK) l'installation d'un serveur d'authentification, qui est un serveur RADIUS dans la pratique. Il faut que les points d'accès et les adaptateurs réseau supportent les protocoles utilisés. Pour cela, un logiciel client doit être installé sur les stations : il

n'est inclus que dans les systèmes d'exploitation récents. De plus, comme la norme 802.11i ne spécifie pas le protocole d'authentification à utiliser, et qu'il existe par exemple deux versions incompatibles de PEAP, trouver la bonne combinaison de tous ces éléments peut donner lieu à quelques tâtonnements.

Il existe dans les points d'accès d'autres fonctionnalités intéressantes en termes de sécurité :
- possibilité d'interdire l'administration du point d'accès depuis le réseau sans fil
- possibilité d'interdire les communications entre stations connectées au même point d'accès
- gestion des VLAN 802.1Q

3. Recommandations générales

3.1 Connaissances

Il est impératif que les administrateurs systèmes et réseaux aient un minimum de connaissances sur le sujet et aient déjà lu des recommandations sur la sécurité des réseaux sans fil. On accepte d'autant mieux les recommandations suivantes qu'on les comprend. Une littérature importante existe sur le sujet, les recommandations de la DCSSI [11] font à notre avis une bonne synthèse.

3.2 Définition des services à offrir

Avant de définir l'architecture il faut définir quels sont les services qu'on veut offrir sur le réseau sans fil, où et à qui. Dans un laboratoire du CNRS disposant d'une infrastructure de câblage décente, la connexion sans fil n'est peut-être pas nécessaire à tout le monde, partout, pour toutes les applications. Cette analyse des besoins permettra de choisir une ou des solutions : les choix ne seront pas les mêmes selon qu'on veut offrir un accès Internet aux visiteurs de passage ou bien offrir au personnel permanent les mêmes services que sur le réseau filaire.

Dans le premier cas, il n'est bien sûr pas question que le laboratoire devienne un fournisseur d'accès Internet, ce qu'il n'a d'ailleurs pas de droit de faire [12]. Par contre il est tout à fait raisonnable de permettre aux personnes en visite, en réunion ou en formation dans le laboratoire, ou encore assistant à un congrès, de consulter leur boîte à lettres avec leur portable muni d'une carte sans fil.

Dans le second cas, il s'agit d'offrir aux utilisateurs autorisés (et à eux seuls) les services, ou une partie des services auxquels ils ont accès sur le réseau filaire.

3.3 Administration du matériel

Toutes les bornes doivent être sous le contrôle total d'un administrateur systèmes et réseaux. Il est absolument interdit aux utilisateurs d'installer leur propre borne, pour deux raisons : d'une part ces bornes « sauvages » risquent d'interférer avec le réseau sans fil du laboratoire et de compromettre son bon fonctionnement, d'autre part leur installation non maîtrisée peut remettre en cause toute la politique de sécurité du laboratoire en permettant à des utilisateurs non autorisés de se connecter au réseau interne.

Dans la mesure du possible, il faut placer les bornes dans un endroit où elles soient peu visibles et accessibles : en effet la plupart des bornes sont équipées d'un bouton qui permet de les remettre dans la configuration d'usine, c'est-à-dire sans sécurité aucune. Si la borne le permet, il faut

interdire l'administration par le réseau sans fil. Il est également recommandé, si le matériel le permet, de prévoir un sous-réseau dédié à l'administration des bornes elles-mêmes.

Sur les grands sites, il est souhaitable que l'administrateur se dote d'outils pour surveiller les radiofréquences, en particulier pour détecter les bornes sauvages. De nombreux outils du domaine public permettent de faire cela [13].

3.4 Activation et portée

Si une borne n'est utilisée qu'à certaines périodes courtes (à la demande de visiteurs, lors de réunions ou conférences…), il est inutile de laisser actif cet équipement. Il peut être mis hors tension dès qu'il n'est plus utilisé et réactivé à la demande. Une borne inactive ou hors de portée ne permet pas de se connecter.

Il est judicieux de limiter la portée d'une borne en diminuant sa puissance d'émission, pour l'ajuster au mieux au rayon d'action désiré. Ainsi si l'on veut des connexions sans fil dans une seule salle, il est inutile et dangereux que la portée couvre tout l'étage du bâtiment, voire la rue adjacente.

3.5 Identifiant de réseau (SSID)

Il ne nous semble pas utile d'essayer de cacher l'identifiant de réseau dans la mesure où d'autres mécanismes de sécurité sont mis en œuvre : afficher un identifiant de réseau clair est plus simple pour tout le monde, utilisateurs et administrateurs, surtout dans un environnement où plusieurs réseaux cohabitent.

3.6 Informations et recommandations aux utilisateurs

Dans les salles où une connexion sans fil est possible et autorisée, il est conseillé de l'afficher clairement, d'indiquer les modalités de connexion (à qui s'adresser… sans évidemment donner les mots de passe ou autres secrets) et leurs limitations éventuelles. Si le chiffrement est inexistant ou faible (WEP), l'affiche devrait aussi informer les utilisateurs que l'écoute est possible et qu'ils doivent de préférence utiliser des connexions chiffrées (SSL, SSH par exemple).

3.7 Traces

Il est nécessaire de tracer l'utilisation des bornes (quelle machine s'y est raccordée à quelle heure) et de stocker ces traces sur un serveur interne au laboratoire, le serveur de logs par exemple. Ceci peut être utile en cas de malveillance pour mieux cerner l'origine et la durée du délit.

4. Recommandations d'architecture

On peut définir deux types de réseaux sans fil selon l'utilisation et le niveau de sécurité apporté.

4.1 Réseau « libre service »

Offrir une connexion Internet aux visiteurs de passage impose plusieurs contraintes. Pour ce type d'utilisation qui devrait rester courte, dix minutes pour relever son courrier par exemple, il n'est pas raisonnable d'imposer une procédure d'enregistrement d'une demi-heure à chaque utilisateur.

L'utilisateur doit également pouvoir accéder au réseau quel que soit le système d'exploitation et la carte sans fil dont est équipé son portable, et sans que la configuration prenne trop de temps.

Pour offrir ce type de service, on pourra utiliser l'authentification et le chiffrement WEP sur les bornes. La clé WEP sera donnée aux utilisateurs qui veulent se connecter. L'administrateur pourra la communiquer au personnel permanent, supposé responsable de ses visiteurs, au responsable d'un colloque, d'une formation… Il faudra également changer cette clé à des fréquences raisonnables (par exemple tous les deux ou trois mois) pour éviter une diffusion trop large.

Les bornes constituant ce réseau sans fil seront placées dans un VLAN dédié, correspondant à un sous-réseau qui sera considéré comme « extérieur » par rapport au réseau interne : les seuls services du réseau interne accessibles depuis ce sous-réseau seront ceux qui sont également accessibles depuis l'extérieur. Le personnel permanent pourra utiliser ce même mode de connexion pour accéder aux ressources internes auxquelles il a normalement accès depuis le réseau public (par exemple webmail, accès SSH…). Cette architecture est représentée figure 1.

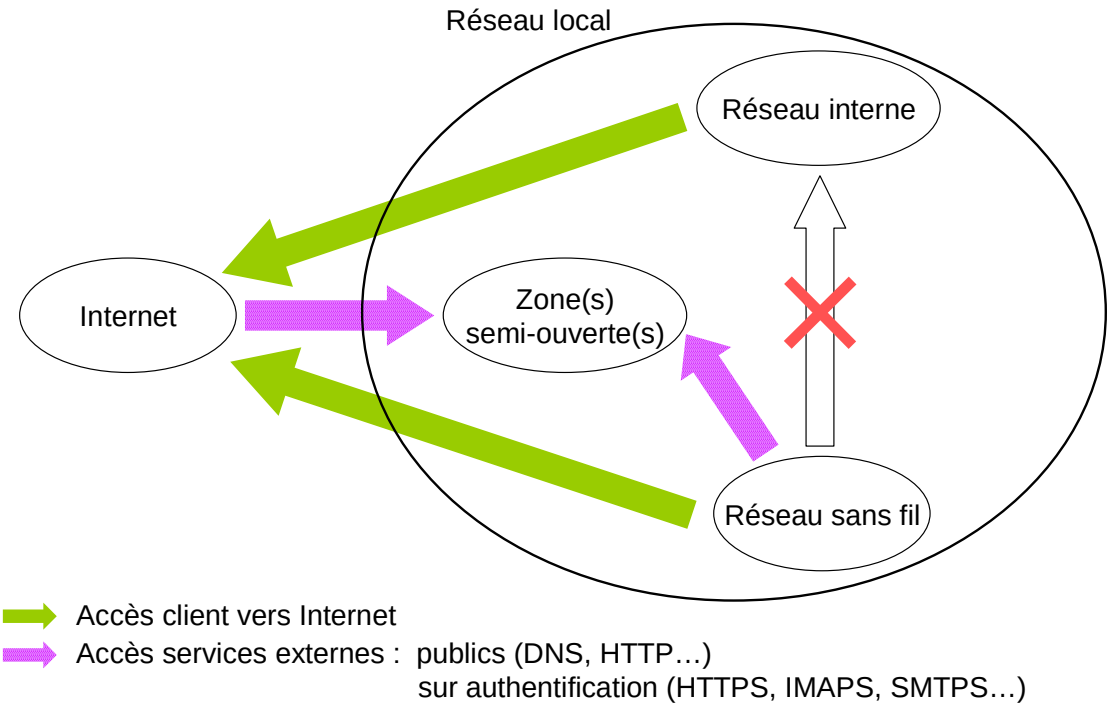

Figure 1 – Réseau libre-service : contrôle d'accès WEP

Pour éviter les abus, il peut être judicieux de limiter également les accès en sortie de ce sous-réseau, en n'autorisant que certains ports. Il faut veiller cependant à ne pas être trop restrictif : une utilisation légitime d'Internet n'est pas limitée aux protocoles HTTP et POP3, il est par exemple tout à fait normal qu'un visiteur veuille utiliser IMAPS, SMTPS ou établir un VPN vers son site d'origine.

Une amélioration de cette configuration est l'utilisation de WPA avec une clé pré-partagée, mais cela nécessite que les équipements (point d'accès, stations et logiciels associés) soient compatibles, donc récents.

4.2 Réseau « utilisateurs identifiés »

Si l'on veut offrir aux utilisateurs davantage de services que ceux qui sont accessibles depuis le réseau public (par exemple l'accès à une imprimante), il faut d'une part utiliser un mécanisme de contrôle d'accès plus fiable qu'une simple clé WEP, d'autre part être capable de cloisonner les différentes catégories d'utilisateurs et de leur attribuer des droits d'accès différents selon par exemple qu'ils font partie du personnel permanent, que ce sont des visiteurs de longue ou de courte durée... C'est à chaque laboratoire de définir sa politique en la matière, le but recherché étant d'éviter que des portables sur lesquels l'administrateur n'a aucun contrôle n'introduisent des virus dans le réseau interne.

Pour ce faire, on pourra utiliser les fonctionnalités d'authentification 802.1X et de gestion des VLAN des points d'accès récents. Cela nécessite d'abord d'installer un serveur d'authentification (serveur RADIUS) et de choisir le protocole d'authentification. Comme le CNRS dispose d'une autorité de certification, TLS est un bon choix si tous les utilisateurs concernés disposent d'un certificat. A défaut, on pourra choisir TTLS ou PEAP. PEAP a l'inconvénient d'être un protocole propriétaire mais l'avantage d'être intégré dans Windows XP. A l'inverse, TTLS a vocation à être un standard ouvert mais nécessite, sous Windows, l'installation d'un client spécifique (qui est parfois founi avec la carte sans fil). Pour la mise en œuvre de telles solutions, on pourra se reporter à [14], [15], [16], [17].

L'authentification pourra se faire par rapport à une base d'utilisateurs propre au serveur RADIUS ou bien un fichier Unix /etc/passwd, une base NIS ou Active Directory, ou encore un annuaire LDAP.
Lorsque l'utilisateur est authentifié, le serveur RADIUS transmet au point d'accès un numéro de VLAN défini par l'administrateur dans lequel cet utilisateur est affecté. Tout le trafic émis et reçu par cet utilisateur transitera dans ce VLAN sur le réseau filaire, c'est-à-dire jusqu'à l'interface Ethernet des points d'accès. Cette étanchéité n'est bien sûr pas assurée entre les stations connectées sur une même borne : d'où l'intérêt d'utiliser la fonctionnalité qui interdit à deux stations connectées sur la même borne de dialoguer entre elles par l'intermédiaire de la borne. La figure 2 illustre une architecture de ce type.

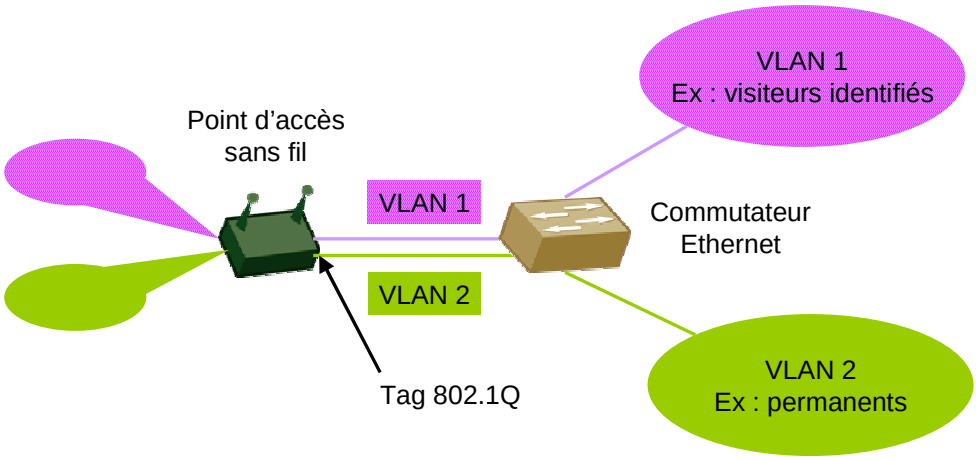

Figure 2 – Réseau utilisateurs identifiés : contrôle d'accès 802.1X

L'inconvénient majeur de cette configuration est qu'elle nécessite que les stations soient compatibles. Il faudra donc donner des recommandations aux utilisateurs qui veulent s'équiper d'une carte sans fil, en échange de quoi ils auront un accès relativement complet aux ressources du réseau local.

4.3 En pratique

Il s'agit là de configurations types. Dans la pratique, on pourra avoir besoin de ces deux configurations (WEP et 802.1X) simultanément. On peut alors soit installer des points d'accès distincts pour les deux réseaux, soit utiliser des points d'accès supportant plusieurs modes. Les clients WEP seront dans un VLAN « extérieur » et les clients 802.1X dans le VLAN qui leur aura été affecté par le serveur RADIUS.

On pourra trouver la solution 802.1X excessivement complexe. En particulier, le serveur RADIUS doit être configuré avec soin, et la configuration des clients n'est pas toujours aisée. Mais elle permet de gérer très finement le contrôle d'accès et elle peut être également utilisée sur le réseau filaire car tous les commutateurs Ethernet récents intègrent le protocole 802.1X. C'est donc un investissement dans un service d'avenir qui devrait se généraliser.

Il existe une solution alternative, qui consiste à utiliser un concentrateur de VPN. On peut alors installer soit un réseau sans fil complètement ouvert, sans aucun contrôle d'accès, qui ne permet de se connecter qu'au concentrateur de VPN [1], soit un réseau de type libre-service avec contrôle d'accès WEP comme décrit en 4.1 : seuls les utilisateurs autorisés authentifiés par le concentrateur pourront accéder au réseau local, avec les mêmes droits d'accès que lorsqu'ils se connectent depuis un réseau public. La figure 3 illustre cette architecture. Cette solution peut être très intéressante si le laboratoire est déjà équipé d'un concentrateur de VPN pour les accès distants.

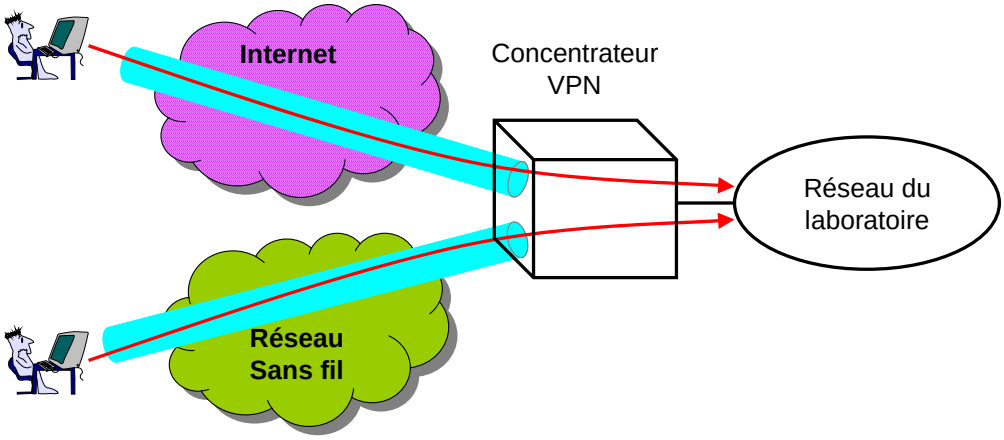

Figure 3 – Réseau utilisateurs identifiés : accès par concentrateur VPN

[1] C'est la solution qui a été mise en œuvre sur la partie inter-universitaire du campus de Grenoble. Cf. [18].

Bibliographie

[1] Azuelos, Daniel, *Architecture des réseaux sans fil*, octobre 2004, http://www.cru.fr/nomadisme-sans-fil/J1310/DAN.pdf

[2] IEEE Std 802.11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999, http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[3] IEEE Std 802.1X-2001, *Port-Based Network Access Control*, juin 2001, http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[4] RFC 3748, *Extensible Authentication Protocol (EAP)*, juin 2004, http://www.ietf.org/rfc/rfc3748.txt

[5] RFC 2716, *PPP EAP TLS Authentication Protocol*, octobre 1999, http://www.ietf.org/rfc/rfc2716.txt

[6] Internet-Draft, *EAP Tunneled TLS Authentication Protocol (EAP-TTLS)*, juillet 2004, http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-05.txt

[7] Internet-Draft, *Protected EAP Protocol (PEAP) Version 2*, octobre 2004, http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-10.txt

[8] *Wi-Fi Protected Access (WPA)*, Version 2.0, Wi-Fi Alliance (http://www.wi-fi.org), avril 2003

[9] IEEE Std 802.11i-2004, *Medium Access Control (MAC) Security Enhancements*, juin 2004

[10] *IEEE 802.11i Overview*, décembre 2002, http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf

[11] *La sécurisation des réseaux sans fil*, juin 2003, http://www.ssi.gouv.fr/fr/actualites/Rec_WIFI.pdf

[12] *Charte déontologique Renater*, décembre 1996, http://www.renater.fr/Telechargement/charte_v12.pdf

[13] Phifer, Lisa, *Open Source WLAN Analyzers*, juillet 2004, http://www.wi-fiplanet.com/tutorials/article.php/3383441

[14] Saillard, Christophe, *802.1X : Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université Louis Pasteur*, JRES 2003, Lille, novembre 2003, http://2003.jres.org/actes/paper.143.pdf

[15] Morris, François, *Authentification 802.1X, WPA ou comment sécuriser les accès des postes mobiles*, septembre 2004, http://www-ext.lmcp.jussieu.fr/~morris/802.1X/mobile.pdf

[16] Bertrand, Manuel, *Etude des solutions de connexion pour postes nomades dans le contexte d'un laboratoire de recherche*, septembre 2004, http://www.urec.cnrs.fr/publications/Rapport.connexion.nomades.pdf

[17] Birri, Rodolphe, *How to Freeradius + EAP/TTLS*, décembre 2003, http://rbirri.9online.fr/howto/Freeradius_+_TTLS.html

[18] Escaffre, Christian, Jullien, Eric, Saillard, Christophe, *Réseaux Sans-Fil Démarche projet et exemples de déploiement*, octobre 2004, http://www.cru.fr/nomadisme-sans-fil/J1310/sgt.pdf