PEDILUVES
Portail d'Entrée pour la Distinction des Invités par L'Usage d'une Vérification de l'Environnement Ssl

Jacques Landru **(GET / INT)**
TELECOM Lille 1
Cité scientifique, rue G. Marconi 59658 Villeneuve d'Ascq Cedex
jacques.landru@telecom-lille1.eu

Tovohérizo Rakotonavalona
TELECOM Lille 1
Cité scientifique, rue G. Marconi 59658 Villeneuve d'Ascq Cedex
tovo.rakotonavalona@telecom-lille1.eu

Résumé

PEDILUVES présente une alternative aux architectures utilisant le trio de protocoles (802.1x-EAP-Radius) pour l'accueil, l'authentification et le contrôle d'accès au réseau WiFi offrant notamment un accès de courtoisie aux invités. En s'appuyant sur la version communautaire (GPL) du tunnelier SSL-Explorer [1]*, il devient envisageable d'offrir un accès sécurisé et contrôlé au réseau WiFi, sans que les équipes système et réseau chargées de l'accueil et de l'assistance n'aient à intervenir sur les postes personnels des invités*

Mots clefs

réseau invité, portail d'accès, contrôle d'accès zones WiFi, portail captif, VPN SSL sans client, *SSL-Explorer*, zéro configuration.

1 Introduction

La banalisation des accès Internet dans les zones publiques (hot-spots WiFi qu'ils soient communautaires ou mis en place par les opérateurs), favorise l'exigence d'un accès réseau de courtoisie dans les zones ou espaces communs (accueil, forum, salle de réunions,...) de nos établissements. L'authentification et le contrôle d'accès à ces réseaux sans fil sont aujourd'hui largement dominés par les différentes déclinaisons des protocoles 802.1x, EAP associées à un système AAA de type Radius. Ces protocoles, bien que banalisés et disponibles sur la plupart des systèmes d'exploitation (OS), nécessitent l'activation d'un client sur les postes des utilisateurs. L'activation ou la configuration de ce client reste un obstacle pour une part non négligeable de nos utilisateurs. De plus la diversité des configurations système des postes personnels est un défi pour bien des équipes réseau chargées d'assurer l'accueil et l'assistance. De même, les droits étendus que s'octroie un utilisateur sur sa machine personnelle et l'état sanitaire de l'OS de cette dernière ne manquent pas de soulever le questionnement des administrateurs de réseaux devant accueillir ces machines dont la configuration leur échappe. PEDILUVES propose une approche par tunnels SSL dite "sans client" sur le poste afin de réduire toute intervention directe sur les ordinateurs personnels, voire d'éliminer toute configuration manuelle avec la version PEDILUVES V2.

2 Objectifs

PEDILUVES a pour objectif d'offrir l'accès au réseau WiFi sans intervention, ni installation logicielle sur les postes personnels. Il vise à couvrir un large éventail d'équipements personnels allant du PDA à la station portable ainsi que les différentes versions de leurs divers OS associés (MS-Windows, GNU/Linux, MacOS, *BSD, etc.). L'accès au réseau est authentifié et réservé à différents profils d'utilisateur (personnels, étudiants, invités déclarés). PEDILUVES délègue l'authentification et les autorisations sur les bases de comptes existantes, il ne nécessite pas de bases de comptes spécifiques. Son indépendance vis à vis des technologies réseaux lui permet d'assurer son rôle quelles que soient les technologies du réseau, 802.11a, b, g et filaires. A l'avenir, celles-ci pourront être complétées par les technologies CPL (Courant Porteur en Ligne) ou 802.11n.

Figure 1 - *affiche "Zone PEDILUVES"*.

3 Principes

Le réseau PEDILUVES, schématisé par la Figure 2, est constitué par un domaine de diffusion (VLAN) confiné de type "bac à sable". Ce réseau est complètement isolé, il ne dispose d'aucun dispositif de routage. Le VLAN connecte les différents points d'accès WiFi, ainsi qu'un commutateur en libre accès pour une connexion filaire. La pile IP des postes personnels est classiquement activée par le protocole DHCP. Ce dernier distribue une adresse non routée, dans la mesure où il n'y a pas de passerelle par défaut active dans le réseau WiFi. Le poste serveur DHCP supporte également un service DNS, référençant les différents serveurs du VLAN, dans un domaine privé dénommé « pediluves.sir ». Le choix d'un domaine DNS de premier niveau (TLD) privé « **.sir** » contribue au confinement du réseau WiFi. Un serveur web, nommé « www.pediluves.sir », fournit l'ensemble des informations d'accueil, pour guider pas à pas l'utilisateur lors de ses premières visites. L'URL de ce serveur fait partie des informations figurant sur l'affiche « zone PEDULIVES » placardée en différents points de la zone de couverture comme le montre la Figure 1.

L'accès aux ressources du réseau d'établissement (SPIDERNET) ainsi qu'au proxy web n'est possible que par l'intermédiaire d'un portail VPN SSL. Celui-ci s'appuie sur la version communautaire (GPL : GNU Public License) du tunnelier *SSL-Explorer* [1]. Il assure l'authentification des utilisateurs, ainsi que la création dynamique et la configuration automatique des tunnels SSL relayant les flux vers les ressources du réseau d'établissement en fonction des profils des utilisateurs. Ces derniers accèdent à leurs ressources disques personnelles, aux ressources web pédagogiques de l'établissement et bénéficient des mêmes services de proxy-web que ceux disponibles dans les salles de travaux pratiques. Les invités, quant à eux, doivent se faire établir un compte, associé à un profil restreint, qui ne leur est délivré qu'après signature de la charte d'usage.

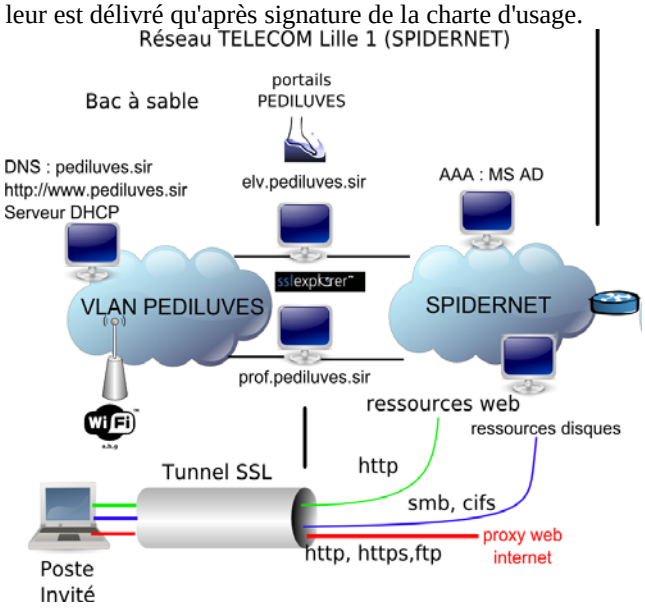

Figure 2 - *Architecture PEDILUVES V1*.

L'approche *SSL-Explorer* est dite « sans client », dans la mesure où elle ne nécessite pas d'installation et de configuration préalable de logiciel sur le poste personnel. Les fonctions du tunnelier sont assurées par un agent pré-configuré téléchargé sous forme d'une *applet* signée. Sur le poste personnel, les prérequis sont donc minimes et banalisés. Ils se résument à un navigateur conforme HTTPS associé à une machine virtuelle Java dans sa version 1.5 ou supérieure. Cette version, qui était récente lors du déploiement initial de PEDILUVES, tend à se banaliser. Elle est toutefois mise à disposition sur le serveur web d'accueil du réseau WiFi. Une configuration minimale du navigateur, par saisie de l'URL de configuration automatique du proxy, reste cependant nécessaire.

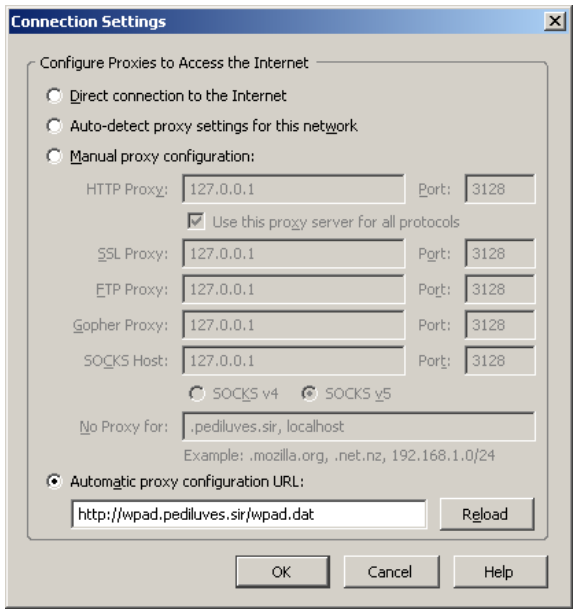

Figure 3 - *Saisie de l'URL de configuration automatique du proxy dans le navigateur.*

La gestion des tunnels applicatifs à travers SSL est assurée de manière centralisée sur le portail *SSL-Explorer*. Les configurations des tunnels sont associées aux profils des groupes d'utilisateurs. A l'issue de la phase d'authentification, elles sont activées automatiquement, sur le poste client, lors du téléchargement de l'agent.

On notera que, sur le domaine de diffusion du réseau WiFi – le VLAN "bac à sable" –, seules les communications à destination du réseau d'établissement (SPIDERNET) passant par le portail sont protégées. Les éventuelles communications directes inter-portables sont considérées comme personnelles et privées, leur protection reste à l'initiative de leurs interlocuteurs.

La version communautaire de *SSL-Explorer* ne gère actuellement qu'un seul domaine administratif (domaine MS-Windows Active Directory, base de comptes spécifiques, ou base de comptes unix). Deux serveurs *SSL-Explorer* distincts (prof.pediluves.sir et elv.pediluves.sir) sont aujourd'hui nécessaires pour assurer l'authentification

de nos deux domaines MS-Windows Active Directory. La virtualisation de ces serveurs nous assurera un meilleur usage des ressources serveur.

4 Evolutions PEDILUVES V2

4.1 Les limitations de la version initiale

La version initiale de PEDILUVES nécessitait, coté poste personnel, la saisie de l'URL HTTPS vers le serveur *SSL-Explorer* relevant de sa communauté pour les phases d'authentification et d'établissement de tunnel. De plus, il était nécessaire de renseigner manuellement la configuration des proxies dans le navigateur, soit par saisie d'une URL pointant sur un fichier de configuration automatique des proxies tel que le montre la Figure 3, soit de spécifier par saisie l'adresse de bouclage (*loopback*) sur le port 3128, point d'entrée du tunnel SSL. Ces opérations initiales, simples pour des utilisateurs aguerris, imposaient une documentation pas à pas détaillée, voire un accompagnement des utilisateurs les moins expérimentés en informatique. Malgré un effort de rédaction et de vulgarisation, dans la documentation d'accompagnement, ces opérations restaient un obstacle pour une part de nos utilisateurs. L'autonomie souhaitée au départ n'étant pas au rendez-vous, le support informatique et réseau se trouvait sollicité et l'utilisateur n'était pas satisfait du fait d'un sentiment de complexité lié à l'utilisation de termes techniques qui lui sont peu familiers.

4.2 Accueil par portail captif

4.2.1 Fonctions d'un portail captif

Les portails captifs [2], développés par les réseaux WiFi communautaires, sont destinés à l'accueil par affichage d'une charte d'usage et la re-direction éventuelle vers un service d'authentification avant d'autoriser le relayage des flux des utilisateurs. Sur un réseau communautaire, le portail captif a, en général, la fonction de routeur par défaut. Toute tentative d'accès direct au web est interceptée par le portail captif qui affiche une page d'accueil et re-dirige le navigateur sur un serveur web d'authentification. Une fois l'authentification réalisée, le portail captif commande au firewall interne d'activer le routage et éventuellement la traduction d'adresse pour l'adresse IP du poste invité. Une des faiblesses de ce type de passerelle est que l'usurpation des adresses MAC ou IP permet à un utilisateur en écoute d'utiliser le portail en lieu et place d'un autre. Dans le cadre de PEDILUVES, nous nous intéressons uniquement à la fonction d'affichage de la page d'accueil du portail captif. La machine supportant le service ne dispose que d'une seule et unique interface réseau connectée au réseau WiFi « bac à sable ». La fonction de routage/firewall est également invalidée. Le confinement du VLAN WiFi n'est donc pas remis en cause avec l'introduction du portail captif.

4.2.2 Introduction d'un portail captif dans l'architecture

Le couplage du tunnelier *SSL-Explorer* avec le portail captif *NoCatAuth* [3], tel qu'il est schématisé à la Figure 4, abolit la nécessité de spécifier l'URL du serveur PEDILUVES dans le navigateur pour les phases d'authentification et d'établissement du tunnel. Le confort d'accueil des utilisateurs s'en trouve donc amélioré. Dès la première tentative de navigation directe sur Internet, le poste obtient ainsi directement, du portail captif, la page d'accueil de la Figure 5 décrivant PEDILUVES et invitant à s'authentifier ou à se faire établir un compte invité après signature de la charte d'usage. La page d'accueil du portail captif affiche également les différents serveurs d'authentification *SSL-Explorer* pour les différentes communautés d'utilisateurs. Elle assure alors une fonction restreinte de type *WAYF* (Where Are You From) telle que celle que l'on rencontre dans l'architecture *Shibboleth* [4].

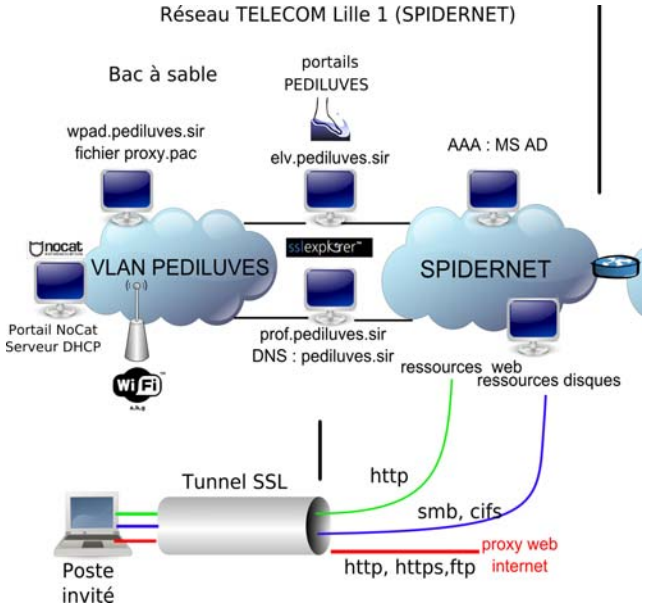

Figure 4 - Architecture PEDILUVES V2.

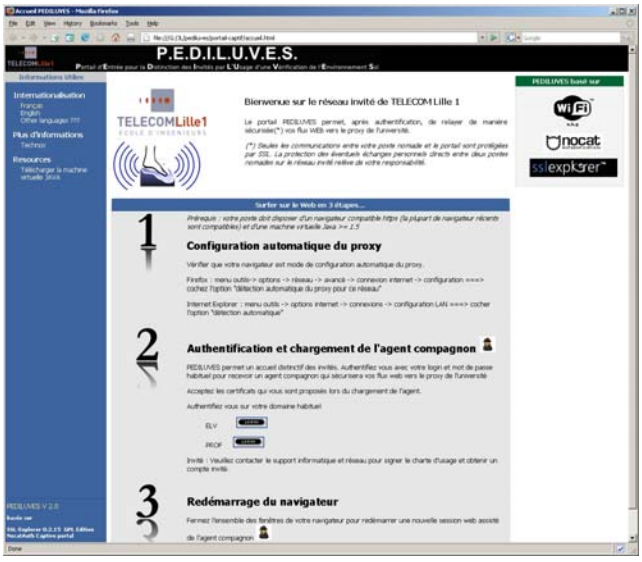

Figure 5 - Accueil PEDILUVES V2.

4.2.3 *Initialisation du poste personnel en trois étapes*

Grâce au portail captif, l'invitation à l'authentification et au téléchargement de l'agent compagnon est automatique si ce dernier n'est pas actif sur le poste . La procédure d'initialisation du poste personnel se déroule en 3 phases :

- vérification du positionnement du navigateur en mode configuration automatique du proxy ;
- authentification et chargement de l'agent compagnon ;
- redémarrage du navigateur.

Lors de son démarrage, le poste reçoit classiquement par DHCP la configuration de la pile IP qui comprend : adresse IP, masque d'adresse, passerelle par défaut qui pointe sur le portail captif, l'adresse du serveur de noms ainsi que l'URL du fichier de configuration automatique du proxy (fichier wpad.dat ou proxy.pac). La première tentative d'accès au web, lors de l'ouverture du navigateur, provoque le chargement et l'exécution du fichier de configuration automatique du proxy. Celui-ci spécifie que le proxy est à l'écoute sur le port 3128 de la machine locale et que si ce dernier ne répond pas alors l'accès est direct. L'agent *SSL-Explorer* n'ayant pas encore été chargé, le navigateur déclenche une résolution DNS et tente le chargement direct de la page. La requête est alors routée vers le portail captif (passerelle par défaut), qui l'intercepte et affiche la page d'accueil de la Figure 5. L'utilisateur, en s'authentifiant, reçoit l'agent compagnon qui s'active automatiquement. Le proxy local sur le port 3128 est alors opérationnel. Toutefois le code des navigateurs intègre un paramètre « proxy failover ». Celui ci désactive le proxy pour 30 minutes, avant de tester de nouveau son accessibilité. La RFC 3143 [5] déplore que ce paramètre « proxy failover » soit codé en dur au sein des navigateurs et l'absence de moyen commun de ré-initialisation. Il faut donc redémarrer le navigateur après activation de l'agent compagnon, ce qui a pour unique fonction de réinitialiser le paramètre « proxy failover » quel que soit le navigateur. Sans ce paramètre non modifiable, la procédure d'accueil serait réduite à deux étapes au lieu de trois.

Cette nouvelle architecture nécessite d'étendre les fonctions du serveur DNS intégré au VLAN. Alors que dans la version initiale de PEDILUVES le serveur DNS ne référençait que les serveurs du domaine privé « pediluves.sir », la nouvelle architecture nécessite en plus un relayage des requêtes DNS, afin que le navigateur puisse tenter un accès web direct qui sera intercepté par le portail captif. Ce service DNS est donc maintenant hébergé sur un des serveurs *SSL-Explorer*, seules machines du bac à sable disposant d'un double attachement permettant le relayage.

5 Intérêt de PEDILUVES

PEDILUVES offre la facilité et le confort d'accueil des réseaux s'appuyant sur les portails captifs, sans sacrifier la confidentialité des flux sur l'espace WiFi. Celle-ci est assurée non pas au niveau liaison de données, comme c'est le cas pour les architectures basées sur le trio 802.1x-EAP-Radius mais au niveau transport au moyen des tunnels SSL. L'absence de client à configurer coté poste personnel est un atout majeur dans un contexte d'accueil de machines hétérogènes aux OS variés. Comparativement le standard 802.1x, nécessite un client, généralement dénommé « supplicant » qui manque de disponibilité ou de maturité pour certaines versions d'OS. Enfin l'absence de routeur sur le domaine de diffusion du réseau WiFi, contribue à son confinement sans nécessiter de firewall ou de filtrage complexe.

6 Évolutions et perspectives

L'activité autour de la version communautaire de *SSL-Explorer*, nous laisse espérer l'activation d'autres mécanismes d'authentification. Un projet d'étudiants de TELECOM Lille 1 a abouti à une extension *SSL-Explorer*-pam [6] permettant l'authentification par l'intermédiaire des modules PAM d'Unix [7]. Dès lors il devient envisageable d'accueillir sur le réseau WiFi les partenaires disposant des mécanismes d'authentification couverts par les modules PAM, notamment ceux disposant d'une authentification Radius. Toutefois il ne semble pas que PEDILUVES soit éligible pour la communauté eduroam.fr [8]. Cette dernière impose une protection 802.1x des réseaux WiFi, et n'accorde pas sa confiance aux mécanismes de portail captif. Une autre opportunité d'élargissement d'accueil à de nouvelles communautés serait de développer les extensions nécessaires à *SSL-Explorer* pour déléguer en confiance l'authentification à *Shibboleth* [4].

Bibliographie

[1] *SSL-Explorer* community edition
http://sourceforge.net/projects/sslexplorer/
http://3sp.com/showSslExplorerCommunity.do?referrer=sslexplorer

[2] portail captif
http://en.wikipedia.org/wiki/Captive_portal

[3] *NoCatAuth*
http://nocat.net/

[4] *Shibboleth*
http://shibboleth.internet2.edu/

[5] I. Cooper, J. Dilley Request for Comments: 3143 Known HTTP Proxy/Caching Problems RFC 3143 2.3.1 User agent/proxy failover page 17
http://www.ietf.org/rfc/rfc3143.txt

[6] Eric Ptak, Quentin Devriendt, Sslexplorer-pam
http://sourceforge.net/projects/sslexplorer-pam

[7] Linux PAM
http://www.kernel.org/pub/linux/libs/pam/

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