

P. E. D. I. L. U. V. E. S.

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



Jacques Landru, Tovoherizo Rakotonavalona

TELECOM Lille 1
Cité scientifique, rue G. Marconi
59658 Villeneuve d'Ascq, cedex - France
<http://www.telecom-lille.eu>
email : {landru, tovo}@telecom-lille1.eu



Contexte

- Réseau WiFi :
 - banalisation des accès internet dans les espaces communs (hot-spots)
 - couverture événementielle
- Accès internet de courtoisie :
 - exigence des invités, disposer d'un accès minimal (HTTPS, HTTP)
- Diversité matérielle et logicielle :
 - matérielle : PC portables, PDAs, tel. Mobiles, MID (Mobile Internet Device)...
 - logicielle : OS multiples dans diverses versions personnalisées
- Diversité culturelle des invités :
 - du technophobe...
 - ... au geek confirmé
- Absence de contrôle des postes personnels :
 - état sanitaire (version d'antivirus)
 - droits administratifs locaux étendus (root, administrateur, super utilisateur)

- Solution dominante :
 - Protocoles 802.1x, EAP associés à un système AAA de type Radius

Objectifs

- Zéro configuration :
 - absence d'intervention directe sur les postes personnels
 - absence de logiciel client
 - pré-requis minimalistes : navigateur HTTPS et JVM >= 1.5
- Indépendance vis à vis des technologies réseau :
 - WiFi 802.11 a,b,g, filaire (aujourd'hui)
 - 802.11n, CPL (à venir)
- Indépendance matérielle :
 - PC portable, PDA...
- Indépendance logicielle :
 - OS : Windows, Unix, GNU/Linux, MacOS, BSD, Solaris...
 - navigateurs compatibles HTTPS (Mozilla Firefox, Konqueror, MS-IE...)
- AAA :
 - accès authentifiés
 - gestion de divers profils d'autorisation
 - audit et journalisation
- Accès sécurisés à un nombre limité de services :
 - HTTPS, HTTP, FTP, CIFS
- Outils ouverts et libres

Approche nouvelle

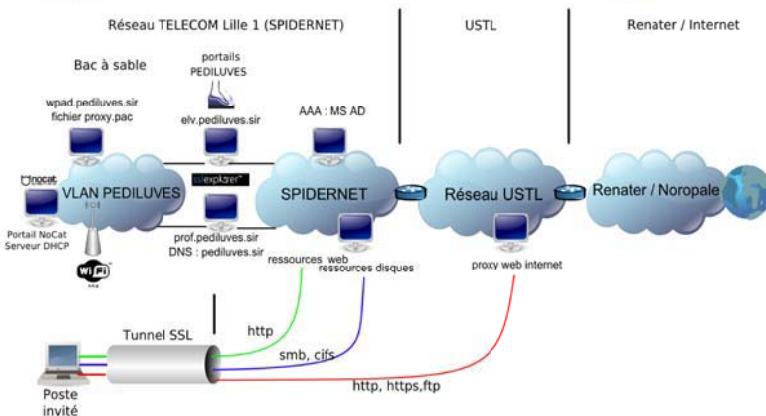
- Confinement dans un réseau « bac à sable »

- portail captif

- tunnels SSL sans client à installer



Architecture



Principes

- Confinement dans un réseau restreint de type bac à sable :
 - VLAN dédié et isolé
 - réseau ip non routé (absence d'équipement de routage)
- Accueil des utilisateurs :
 - portail captif NoCatAuth en mode ouvert mais avec absence de routage
 - adressage DHCP
 - configuration automatique proxy (WPAD, fichier PAC) pour redirection sur le tunnel SSL
- Tunnelier SSL (SSL-Explorer en version communautaire GPL) :
 - Authentification et autorisation sur annuaires Active Directory existants
 - Création dynamique de tunnels SSL vers les ressources du réseau d'établissement
 - gestion centralisée des tunnels en fonction des profils des utilisateurs
 - téléchargement de la configuration sur le poste : applet java signé

Limitations

- Version communautaire de SSL-Explorer limitée à 1 seul domaine administratif (realm)
- Sécurisation SSL uniquement entre le poste et le portail SSL-Explorer

Évolutions et perspectives

- 802.11n (mimo), CPL ...
- Virtualisation des serveurs portail SSL-Explorer (Linux KVM, XEN ?)
- Sslexplorer-pam :
 - <http://sourceforge.net/projects/sslexplorer-pam>
 - authentification Radius : accueil des communautés partenaires ?
- Délégation d'authentification :
 - « shibbolethiser » SSL-Explorer pour l'accueil en confiance de nouvelles communautés partenaires

