Atelier 802.1x / RADIUS / Wi-Fi

Florian Fainelli

/tmp/lab
Vitry sur Seine

17 juillet 2008

Sommaire I

Rappels

- technologie normalisée IEEE sous le groupe 802.11
- fonctionne en 2.4 et 5Ghz
- support sans-fil, donc problème d'accès au média
- fonctionne comme un hub sans-fil (pas de commutation)

Sécurité disponible

- WEP : Wired Equivalent Privacy 64 ou 128 bits
- WEP utilise RC4, problèmes liés à l'algo de chiffrement
- WPA : Pre-shared Key ou Entreprise
- possibilité de faire du brute-force

802.1x

- système tri-partite : supplicant, NAS, serveur RADIUS
- indépendant du média de connexion
- disponible dans la plupart des points d'accès, DSLAM, et switchs niveau 2/3 intelligents

Supplicant

- logiciel installé sur un poste client : xsupplicant, wpa supplicant, service Windows, MacOSX
- gère l'envoi du login mot de passe avec forme appropriée : EAP-TLS, PEAP, LEAP, MD5 ...
- trames envoyées sur la couche MAC avec Ethertype EAPOL
- ne recoit que les Access-Accept ou Access-Reject

Network Authenticator Station

4 répertoires principaux

- gère l'accès à la couche réseau (OSI 3) depuis la couche accès (OSI 2)
- transmet les requetes d'authentification au RADIUS
- rajoute et vérifie des attributs : adresse MAC station émettrice, comptabilité
- si Access-Accept : couche réseau disponible : IP, DHCP ...
- si Access-Reject : désassociation (Wi-Fi), fermeture port (Switch ethernet) ...
- envoi des requetes d'authentification au niveau UDP/IP vers le serveur RADIUS

Serveur RADIUS

- Remote Authentication Dial-In User System
- séparation de la gestion des utilisateurs, des attributs et comptabilité
- gestion simultanée de plusieurs méthodes d'authentification : EAP-TLS, EAP-TTLS ...
- Authentication, Authorization, Accounting
- gestion de différentes backends : SQL, LDAP, fichiers

Déploiement

- choix de la méthode d'authentification : dépendante de l'OS et des contraintes sur les postes
- choix recommandés : EAP-MSCHAPv2 pour Windows, EAP-TTLS pour MacOSX/Linux/xBSD
- choix du backend utilisateurs et support accounting
- configuration et distinction des NAS en fonction du support de connexion/collecte de données

Installation

- utilisation de FreeRADIUS : complet, documenté, mature
- utilisation d'une base MySQL : rapide à installer, requetes faciles à modifier
- authentification avec EAP-TTLS : gestion du certificat serveur uniquement

Configuration du point d'accès

- configuration d'un OpenWrt brcm-2.4
- le programme nas fait office de NAS
- paramètres : IP serveur RADIUS, port 1812, 1813, secret partagé

Comptabilité, analyse, fine tuning

- demande des infos de comptabilité au NAS
- analyse des informations stockées : phpradadmin
- configuration avancée de RADIUS : actions post/pre authentification
- nombre de threads
- analyse de logs