Etude de cas : sécurité d'un réseau Wifi

Vous êtes stagiaire dans la société SIO (Sans-fil Intelligent et Opérationnel) chargé d'étudier un projet de réseau Wifi sécurisé pour le lycée Marie Curie. Ce r seau Wifi doit permettre l'accès au réseau du lycée aux étudiants et professeurs par l'intermédiaire de toute solution d'accès Wifi (ordinateur portable, smartphone, tablette tactile)

Description de l'infrastructure réseau existant :

Le réseau filaire Ethernet est composé de trois VLAN :

1. Vlan administratif (20 PC)
2. Vlan pédagogique (200 PC)
3. VLAN serveurs. Serveurs existants :
   Serveur Web (S-WEB),
   Serveur d'authentification ldap : contrôleur de domaine Active Directory (S-AD)
   Serveur d'application (S-APP)

L'accès à internet se fait par l'intermédiaire du routeur-parefeu R-EOLE connecté directement à internet. L'accès à internet est contrôlé en fonction du login de l'utilisateur par un proxy installé sur R-EOLE.

Descriptif du projet :

La solution préconisée consiste en un portail captif couplé à une authentification Radius/LDAP.
L'installation de bornes wifi sera effectuée. Les bornes seront reliées à un commutateur Ethernet indépendant du reste du réseau local. Le portail captif utilisé sera la solution libre Chillispot qui sera installé sur une nouvelle passerelle linux équipée de deux cartes réseau et nommée R-WLAN placée entre le commutateur du réseau des bornes Wifi et le réseau local Ethernet filaire existant. Chillispot n'intègre ni serveur Web, ni serveur Radius. Le serveur Apache existant déjà sur le réseau (S-WEB) sera utilisé. Il n'intègre pour l'instant que le protocole HTTP donc il sera sécurisé par SSL. Le serveur Radius libre Freeradius sera installé sur la passerelle R-WLAN. L'authentification des utilisateurs wifi sera effectuée sur le contrôleur de domaine Active Directory existant (S-AD).

1. Dessinez le schéma de l'infrastructure réseau existante
2. Dessinez le schéma de l'infrastructure réseau intégrant le projet de réseau wifi sécurisé.

Le chef de travaux du lycée Marie Curie à qui vous avez transmis le descriptif du projet vous a renvoyé une série de questions par mail:

Pourquoi la solution nécessite-t-elle la présence d'un serveur Web ? En quoi consiste sa sécurisation ?
Est-ce que la solution assure les trois fonctions de sécurité AAA ? (Vous rappellerez quelles sont ces trois fonctions)
Quel est le rôle du serveur Radius ? Ou est le client Radius ? Les échanges entre le client et le serveur Radius sont-ils sécurisés?
Comment garantir que les mots de passe des utilisateurs ne transitent pas en clair sur le réseau wifi?
Quelles sont les étapes de l'authentification d'un utilisateur nomade ?
Sur quel serveur devra-t-on créer le compte (login et mot de passe) d'un nouvel utilisateur ?

Rédigez une explication détaillée du projet complétée éventuellement par des schémas permettant de répondre aux questions du chef de travaux.

ANNEXE 1 : Portail captif

La technique des portails captifs consiste à forcer les clients HTTP d'un réseau de consultation à afficher une page web spéciale (le plus souvent dans un but d'authentification) avant d'accéder à Internet normalement.

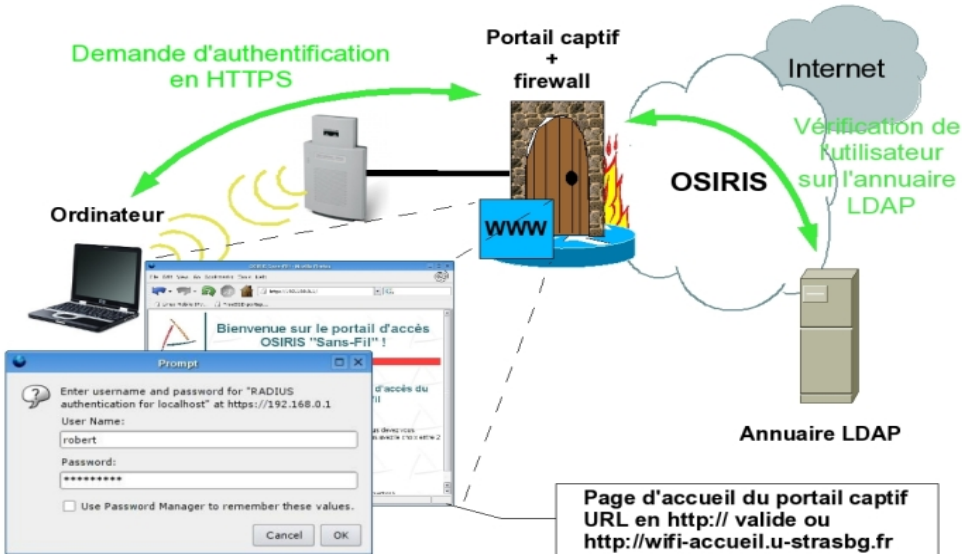
Cela est obtenu en interceptant tous les paquets par une passerelle quelles que soient leurs destinations jusqu'à ce que l'utilisateur ouvre son navigateur web et essaie d'accéder à Internet. Le navigateur est alors redirigé par la passerelle vers une page web qui peut demander une authentification et/ou un paiement ou tout simplement demander d'accepter les conditions d'utilisation du réseau. Cette technique est souvent employée pour les accès Wi-Fi et peut aussi être utilisée pour l'accès à des réseaux filaires (ex. hôtels, campus etc.).

Le client se connecte au réseau par l'intermédiaire d'une connexion filaire ou au point d'accès pour du wifi. Ensuite un serveur DHCP lui fournit une adresse IP ainsi que les paramètres de la configuration du réseau. A ce moment là, le client à juste accès au réseau entre lui et la passerelle, cette dernière lui interdisant, pour l'instant, l'accès au reste du réseau. Lorsque le client va effectuer sa première requête de type web en HTTP ou HTTPS, la passerelle le redirige vers une page web d'authentification (hébergée sur un serveur web local) qui lui permet de s'authentifier grâce à un login et un mot de passe. Cette page est cryptée à l'aide du protocole SSL pour sécuriser le transfert du login et du mot de passe. Le système d'authentification va alors contacter par l'intermédiaire d'un serveur d'authentification RADIUS en général, une annuaire contenant la liste des utilisateurs autorisés à accéder au réseau. Enfin le système d'authentification indique, plus ou moins directement selon les portails captif, à la passerelle que le couple MAC/IP du client est authentifié sur le réseau. Finalement le client est redirigé vers la page Web qu'il a demandé initialement; le réseau derrière la passerelle lui est dorénavant accessible.

Le portail captif, grâce à divers mécanismes comme une fenêtre pop-up sur le client rafraîchie à intervalles réguliers ou des requêtes Ping vers le client, est en mesure de savoir si l'utilisateur est toujours connecté au réseau. Au bout d'un délai d'absence sur le réseau, le portail captif va couper l'accès à cet utilisateur.

La différence entre un simple parefeu et un portail captif réside dans le fait que le portail captif ne refuse pas une connexion mais la redirige plutôt vers une page d'authentification

Exemple de portail captif avec une authentification sur un annuaire LDAP :



ANNEXE 2 : Authentification centralisée avec les protocoles RADIUS et LDAP

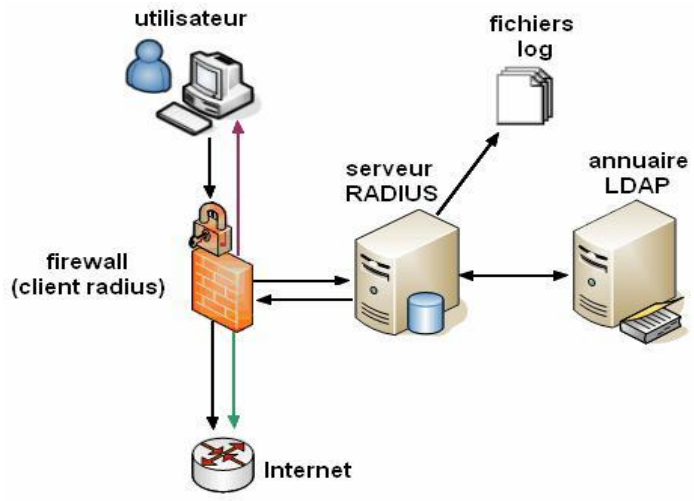
Sécurisation des systèmes d'informations :
La sécurisation des systèmes d'informations repose souvent sur la protection des ressources du système contre toute utilisation malveillante qui peut nuire au fonctionnement et à la rentabilité du système. Ceci s'effectue par un contrôle d'accès à ces ressources ce qui sous-entend l'authentification des utilisateurs, l'attribution des droits d'accès et la « journalisation » du trafic.

Problématique : Un système d'information est une structure qui évolue perpétuellement selon les besoins. De nouvelles ressources peuvent êtres ajoutées, de nouveaux utilisateurs peuvent être créés et donc de nouveaux droits d'accès et de nouvelles règles d'exploitation doivent être définis. Ceci entraîne une multitude de données pour l'utilisateur final du système aussi bien que pour son administrateur. Par conséquent, le risque d'oubli, de confusion, de réplication augmente et rend l'interaction avec le système très complexe.

Solution : Il est intéressant de centraliser la gestion des données d'authentification et d'unifier ses sources. Ceci se traduit par la mise en œuvre d'une structure du type SSO (Single Sign On) ou un utilisateur accède aux différentes ressources du système d'information par un seul couple login/password.

Principe de la solution : La solution décrite dans le paragraphe précédent repose sur l'interfaçage de deux serveurs d'authentification centralisée : un serveur RADIUS et un serveur LDAP. Le serveur RADIUS servira à authentifier les utilisateurs par délégation de l'authentification au serveur LDAP qui gère un annuaire électronique contenant les identités des différents utilisateurs.
L'accès aux différentes ressources sera conditionné par une authentification RADIUS. Chaque utilisateur sera invité à s'authentifier pour pouvoir utiliser une ressource donnée et dans le cas d'une authentification réussie, cet accès sera journalisé et l'utilisateur pourrait être comptabilisé.

Exemple de mise en œuvre de la solution RADIUS/LDAP : Dans un réseau d'entreprise l'accès à Internet est conditionné par une politique de sécurité mise en œuvre sur le firewall. Cette politique conditionne l'accès à Internet par une authentification RADIUS. On suppose qu'un utilisateur veut se connecter à Internet. Il est invité à saisir son nom d'utilisateur et son mot de passe dés qu'il lance son navigateur web. Cette action se traduit par une demande d'accès envoyé par le client RADIUS, qui est le firewall dans notre cas, vers le serveur RADIUS. Ce dernier entame une opération de vérification de l'identité en demandant au serveur LDAP de chercher dans l'annuaire une entrée dont le nom correspond à celui de l'utilisateur et d'extraire son mot de passe. Selon le résultat de cette vérification d'identité, le serveur RADIUS répond son client par une acceptation d'accès ou par un rejet. A son tour, le client autorise le client à se connecter à Internet ou l'invite à une nouvelle authentification. Dans le cas où l'utilisateur est autorisé, le serveur RADIUS déclenche une étape de « journalisation » qui consiste à collecter des informations relatives à cette connexion pour éventuellement comptabiliser l'utilisateur.



Avantages de la solution RADIUS/LDAP :

- Unification de la source d'authentification : un seul serveur, le serveur RADIUS, permet d'authentifier tous les utilisateurs pour tous les services disponibles (Internet, impression, messagerie, etc.).
- Exclusivité de l'administration : un seul utilisateur a le privilège d'administrer les serveurs RADIUS et LDAP.
- Garantie de l'intégrité et de la confidentialité des données échangées :
  - chiffrement des transactions par une clé partagée entre les clients et les serveurs,
  - utilisation des mécanismes de chiffrement PAP et CHAP ou EAP pour protéger les mots de passe des utilisateurs,
  - utilisation des connexions sécurisées (canaux SSL).
- Facilité de l'analyse des performances et de la détection d'anomalies : les informations contenues dans les fichiers journaux servent de base pour d'éventuelles analyses.