BTS Services Informatiques aux Organisations

ÉTUDE DE CAS

CAS H

.

ÉLÉMENTS DE QUESTIONNEMENT

POUR UN SUJET ZÉRO

Le contexte

Les Hospices Civils de la ville de XXX regroupent aujourd'hui 15 établissements pluridisciplinaires ou spécialisés dans le cadre d'un établissement public de type Centre Hospitalier Universitaire (CHU).

Véritable centre de compétences intégrant toutes les disciplines, ils disposent d'une large palette de moyens techniques et logistiques pour assurer ses missions de soins, d'enseignement, de recherche et d'innovation médicale, de prévention et d'éducation pour la santé.

Plus de 22 000 professionnels, dotés des équipements les plus avancés, se consacrent quotidiennement à leur mission.

L'utilisation des nouvelles technologies de l'information dans le milieu hospitalier est indispensable tant pour le personnel médical que pour les autres personnels. Du dossier médical aux détecteurs de fumées en passant par la lingerie ou la restauration, tout est informatisé et connecté au réseau et nécessite une infrastructure réseau performante.

Actuellement, le réseau informatique des Hospices Civils est basé sur une architecture de type métropolitaine qui permet aux établissements de communiquer directement entre eux.

L'informatique des Hospices civils est pilotée par la DSII (Direction du Système d'Information et de l'Informatique) dont les locaux accueillent les services centraux.

Le réseau est géré par l'unité SRT (Système, Réseau et Télécoms) qui s'appuie dans chaque établissement sur des structures locales appelées ALI (Agence Locale Informatique).

C'est dans l'équipe du SRT et dans les locaux de la DSII, que vous avez été intégré(e) et que vous êtes chargé(e) de participer à différentes missions.

Partie 1 - Authentification des professionnels extérieurs

Participation à la production de services

Des bornes Wi-Fi ont été mises en place dans les hôpitaux civils, tant pour assurer des liaisons à des applications métiers dans des locaux anciens rendant difficile ou coûteuse la mise en place d'une solution filaire que pour fournir un accès nomade au personnel médical qui se déplace de chambre en chambre et pour lui permettre de remplir le dossier du patient ou son programme de traitement directement depuis un ordinateur portable ou un *smartphone*.

Un accès Wi-Fi payant est également mis à la disposition des patients hospitalisés afin de leur proposer un accès à internet.

Les besoins pris en charge actuellement par l'authentification Wi-Fi en place

Aujourd'hui, tout le personnel médical a accès au réseau interne des hospices par le biais d'un SSID particulier et non diffusé. Le flux en provenance de ce SSID est redirigé vers le réseau interne.

Les patients ont accès à internet par le biais d'un autre SSID nommé « patient-hospices ». En se connectant à ce SSID, ils sont redirigés vers un portail captif appartenant à la société ACI qui s'occupe des accès internet concernant les patients. Le service informatique des hospices réalise une redirection de flux sans gérer ces accès.

Les besoins non pris en charge

Les Hospices donnent également accès à des services informatiques à des professionnels de santé (médecins, chercheurs, étudiants, etc.) qui ne sont pas membres du personnel de l'hôpital. Ces professionnels accèdent à ces services à l'hôpital à l'occasion d'une visite, ou bien à l'extérieur de l'hôpital depuis leur bureau ou depuis un ordinateur portable. Parmi les services auxquels ils accèdent, on trouve notamment l'accès à toute la base documentaire et aux revues scientifiques et médicales.

Actuellement, ces professionnels de santé extérieurs aux hospices n'ont pas de solution d'accès dédiée.

Un projet a été mis en place pour prendre en charge ce besoin, projet qui va vous amener à assurer différentes missions au cours de sa réalisation, en s'appuyant sur un dossier (**voir les documents associés à la partie 1**) mis à disposition de l'équipe.

TRAVAIL À FAIRE

Mission 1 – Justifier le choix d'une solution

L'équipe a fait le point sur la situation existante et a proposé une solution qui a été discutée au dernier comité de pilotage des SI. Le chef de projet doit cependant fournir un rapport au comité de pilotage, qui demande une justification technique écrite de la solution choisie qui doit souligner son intérêt mais aussi ses insuffisances. Il vous demande d'écrire un argumentaire technique intégrant *un rappel de la notion de VLAN et de SSID et une explication de l'intérêt d'associer un SSID à un VLAN.*

1.1. Rédiger un argumentaire synthétique (30 lignes maximum) permettant de répondre à ces questions :

« Peut-on utiliser les SSID et VLAN existants pour authentifier l'accès des professionnels extérieurs en respectant les contraintes de sécurité ? »

« En quoi une solution de type portail captif est moins lourde techniquement à mettre en œuvre que la solution d'authentification mise en place pour le personnel médical ? »

« En quoi la solution « PEAP » est plus sécurisée que la solution « portail captif » ?

Mission 2 – Étudier une solution

L'argumentaire technique a contribué à la validation par le comité de pilotage de la solution présentée. Le chef de projet souhaite maintenant approfondir certains aspects techniques.

1.2. Exposer les grands principes de la solution « portail captif » choisie pour les professionnels extérieurs en fournissant notamment un diagramme de séquence de la solution et un schéma de la solution d'infrastructure réseau.

1.3. Préciser en quoi cette solution répond aux exigences de sécurité et aux contraintes légales qui s'imposent aux hospices civils en fournissant un accès internet à des professionnels extérieurs.

Mission 3 – Prototyper la solution choisie

Le chef de projet souhaite s'assurer de la faisabilité de la solution choisie en mettant en place un prototype. Il vous charge de sa réalisation.

1.4. Rédiger une note simple listant les équipements dont vous avez besoin pour monter votre environnement de tests.

Mission 4 - Tester et valider la solution

Le prototype de « portail captif » est maintenant mis en place et vous devez commencer la phase de test. Vous devez pour cela présenter au préalable votre stratégie de test à votre chef de projet.

1.5. Lister les tests à effectuer pour démontrer la validité de la solution pour l'accès des professionnels extérieurs.
1.6. Indiquer les éléments à intégrer dans votre rapport de tests pour démontrer que les professionnels extérieurs « invités » sont bien associés à un VLAN sur le réseau filaire.

Lors de la présentation de votre rapport de test, votre chef de projet s'interroge sur l'intégration de cette solution dans l'infrastructure cible et sur les risques de dégradation du fonctionnement de l'existant.

1.7. Exposer ce qu'il faudrait ajouter à l'environnement de test pour effectuer des tests de non régression.

Mission 5 – Archiver les fichiers d'activité de la solution

Les fichiers d'activité générés par le portail captif et le serveur mandataire doivent être conservés sur de longues périodes. Votre responsable vous demande de lui proposer une solution pour automatiser cet archivage qui précise le choix d'un langage de *scripting* et la structure générale du script à écrire.

1.8. Proposer une solution détaillée prenant en charge l'automatisation de l'archivage des fichiers d'activité

Partie 2 - Résolution d'un problème d'infrastructure

Participation à la fourniture de services

Un dysfonctionnement répétitif a été repéré dans un service : plusieurs utilisateurs se plaignent de ne plus avoir accès au réseau sur les nouveaux matériels installés et connectés en filaire.
Une série de tickets d'incident est parvenue à votre service et votre responsable vous demande de les traiter en urgence.

TRAVAIL À FAIRE

Certaines personnes du bâtiment B n'accèdent pas au réseau. La plateforme d'assistance a repéré qu'ils disposaient tous de matériels nouvellement livrés sans pouvoir en déduire la nature de la panne. Ces matériels ont été testés techniquement et paramétrés par l'équipe informatique de l'ALI et ne présentaient pas de défaillance.

Mission 1 – Identifier, qualifier et diagnostiquer l'incident

Votre responsable vous demande de préciser la démarche que vous avez mise en œuvre pour diagnostiquer les incidents et de comparer le dysfonctionnement décrit avec le comportement normal attendu dans cette situation sous forme d'une note précise et concise qui enrichira la base de connaissances associée à la gestion des tickets.

2.1. Rédiger une note (30 lignes maximum) expliquant pourquoi ces utilisateurs n'accèdent pas au réseau.
2.2. Expliquer techniquement pourquoi l'incident identifié peut se produire avec le protocole concerné

Mission 2 – Résoudre l'incident

Face à l'urgence de la situation, le responsable de l'assistance souhaite mettre en place une solution provisoire permettant aux postes concernés d'accéder au réseau. Pour évaluer le temps de l'intervention, il vous demande de réfléchir à une démarche de résolution qui pourra être déployée par la plateforme d'assistance.

2.3. Proposer le principe d'une solution provisoire permettant aux postes d'accéder au réseau.
2.4. Définir le périmètre du réseau dans lequel l'incident peut se produire.
2.5. Définir une méthode permettant de déterminer l'emplacement de la prise réseau à partir de l'adresse IP de l'équipement exécutant le service en cause.
2.6. Lister les actions à entreprendre pour résoudre l'incident et permettre aux utilisateurs d'accéder normalement au réseau.

Mission 3 – Gérer le problème

La multiplication des incidents de même nature nécessite de rechercher une solution définitive pour les éviter. Vous alertez dans une note votre responsable sur la possibilité d'un incident de type *starvation* en expliquant les conditions de sa réalisation et en montrant les conséquences de celui-ci.

2.7. Rédiger une note (20 lignes maximum) à l'attention du SRT détaillant les actions à entreprendre sur l'ensemble du réseau pour éviter que l'incident se reproduise.

Dossier fourni pour réaliser les missions de la partie 1

Document 1 - le besoin et la solution envisagée

1.1 Le besoin

Les Hospices Civils souhaitent proposer une solution d'accès dédiée aux professionnels de santé extérieurs qui ne sont employés par les hospices.

Tous les services informatiques des hospices s'appuient sur un service d'annuaire pour l'authentification et les habilitations des utilisateurs. Actuellement seuls les employés des hospices sont enregistrés dans cet annuaire. Le processus de création d'un utilisateur dans l'annuaire est donc nécessairement long alors que certains professionnels extérieurs peuvent ne rester que peu de temps sur place. Il n'y a pas d'accès « invité » autorisé. Il y a cependant une exception concernant le service documentaire et les accès aux revues médicales qui sont disponibles sur une zone « DMZ » interne et accessible sans authentification.

Les Hospices Civils ne souhaitent donc pas intégrer des professionnels extérieurs même temporairement dans cet annuaire pas plus que dans le périmètre réseau dédié aux employés. Ce périmètre réseau n'est d'ailleurs accessible qu'après une authentification dans l'annuaire

Un portail captif est déjà en place actuellement pour les patients. Mais celui-ci est géré par une société extérieure (la société ACI). Si un patient souhaite se connecter à Internet, il doit en faire la demande auprès de cette entreprise lors de l'enregistrement à l'accueil, comme il le fait pour la télévision ou le téléphone. L'accueil fournit au patient les identifiants pour se connecter au portail captif et accéder à internet et cette opération lui est facturée. Les hospices ne souhaitent pas facturer de prestation aux professionnels extérieurs qui sont souvent des médecins, des étudiants ou des chercheurs. Les deux solutions en place ne répondent donc pas au besoin exprimé.

Les hospices souhaitent mettre en place une nouvelle solution dédiée aux professionnels extérieurs, qui dans un premier temps permettra l'accès à Internet puis dans un second temps l'accès à des ressources réseaux.

1.2 La solution à étudier

La solution choisie par les hospices est la mise en place d'un portail captif dédié aux professionnels extérieurs donc distinct de celui des patients.

Ce portail permettrait à partir d'une page d'authentification de se connecter à Internet avec une adresse mail et un mot de passe gérés par un serveur RADIUS intégré au portail. Une fois que le compte de l'utilisateur arrive à expiration dans cette base, celui-ci est supprimé.

La solution choisie est basée sur le logiciel de portail captif « amigopod » qui intègre un serveur Radius, un serveur DHCP et un serveur DNS de type « cache ». Le SSID spécifique aux professionnels extérieurs sera le SSID « Visiteurs ».

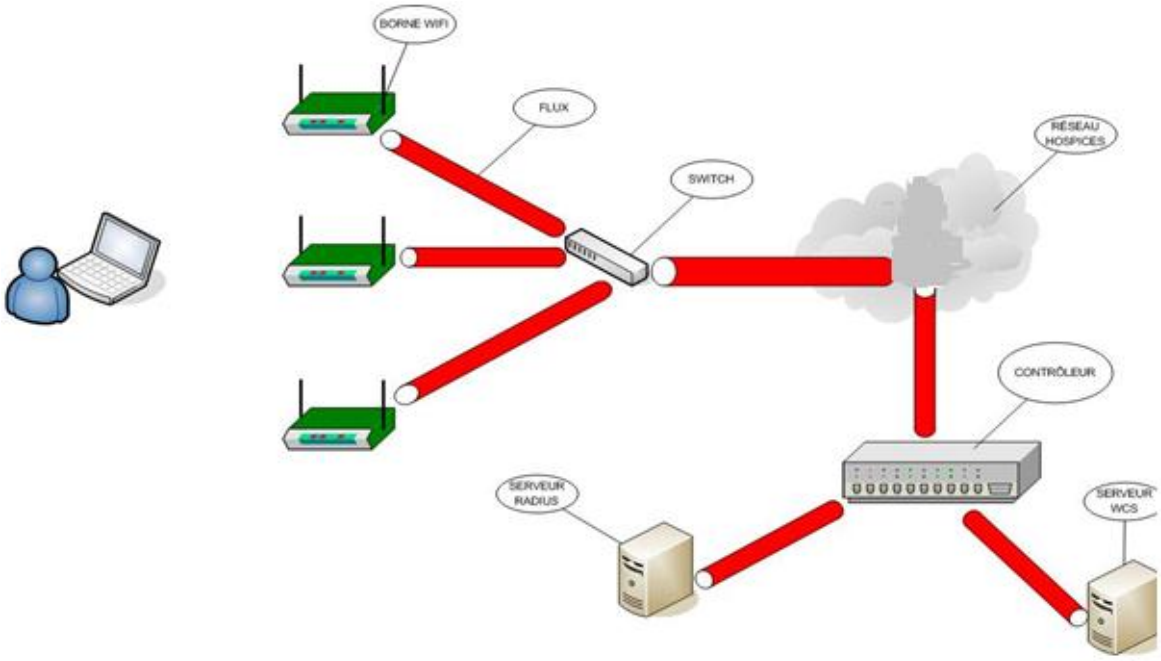
Document 2 - l'architecture Wifi actuelle

2.1 Les bornes légères

Environ 2 000 points d'accès sont installés sur les différents établissements des hospices civils, ce qui fait des Hospices Civils un des premiers utilisateurs de solution Wi-Fi en Europe. Cela implique des choix technologiques performants notamment en matière d'administration des bornes.

Actuellement, l'architecture Wi-Fi des hospices est basée sur un système de bornes légères (qui s'oppose au système de bornes autonomes). Les points d'accès Wi-Fi sont reliés à un contrôleur qui a pour fonction de leur fournir leur configuration. Les points d'accès disposent donc d'un système d'exploitation « minimaliste » qui leur permet de démarrer et de se rattacher à un contrôleur. Toute la partie « intelligente » se trouve au niveau du contrôleur. Le contrôleur se présente sous la forme d'une carte WiSM (*Wireless Services Module*) accompagné d'une carte de supervision le tout dans un châssis.

Tous les contrôleurs Wi-Fi sont gérés à partir du serveur WCS qui possède une interface WEB.



Les bornes Wi-Fi diffusent plusieurs SSID et chaque SSID correspond à un VLAN. Pour la communication avec les commutateurs, le protocole 802.1q (*tag*) est utilisé, chaque trame est donc « marquée » avec le numéro du VLAN correspondant.

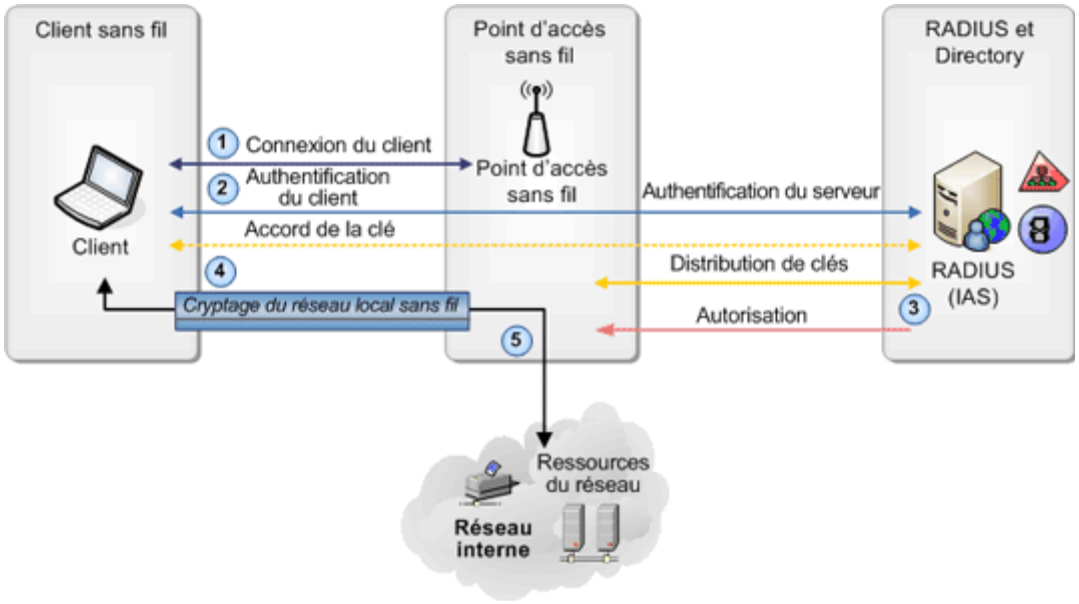
2.2 Schéma de principe de l'authentification du personnel médical

Les informations médicales sont par nature extrêmement confidentielles.
Pour accéder au réseau sans-fil des Hospices, une authentification PEAP est nécessaire. Cette méthode s'appuie sur deux phases principales :

1. Connexion du client au point d'accès
2. Authentification mutuelle
    a. Authentification du point d'accès auprès du client par l'intermédiaire d'un certificat délivré par le serveur Radius contrôlé à l'aide d'un certificat installé localement sur le poste et délivré par une autorité de certification approuvée

b. Authentification du client par le serveur RADIUS par échange d'un login/mot de passe crypté par la clé publique contenue dans le certificat délivré précédemment. La vérification du « login » se fait via un annuaire compatible LDAP.

3. Calcul puis fourniture de la clé de session (symétrique) et autorisations (affectation à un VLAN notamment)
4. Cryptage de la liaison entre le client et le pont d'accès à l'aide de la clé de session
5. Accès au réseau local dans le Vlan autorisé



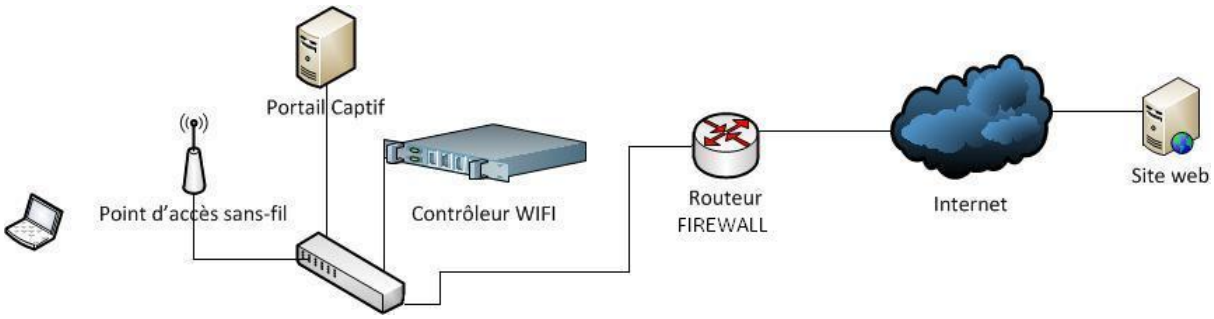
Source du schéma: authentification 802.1X et PEAP sur le réseau local sans fil
(http://technet.microsoft.com/fr-fr/library/dd491890.aspx)

2.3 Schéma de principe de l'authentification des patients

L'authentification des patients se fait par un portail captif. C'est une méthode qui consiste à forcer les clients à passer par une page HTML obligatoire pour s'authentifier généralement avant de pouvoir naviguer sur internet. Le navigateur web devient ainsi un support d'authentification.
Ceci est réalisé en interceptant toutes les communications (les paquets), jusqu'à ce que l'utilisateur ouvre son navigateur et tente d'accéder à Internet. À ce moment-là le navigateur est redirigé vers une page qui peut exiger une authentification et/ou un paiement, ou simplement afficher une charte d'utilisation et demande à l'utilisateur d'accepter celle-ci.

Les portails captifs sont très présents dans les lieux publics comme les *fastfoods* qui permettent en entrant un code présent sur le ticket de caisse d'accéder à internet.

Le schéma logique de l'architecture du portail captif pour les patients des Hospices est la suivante :

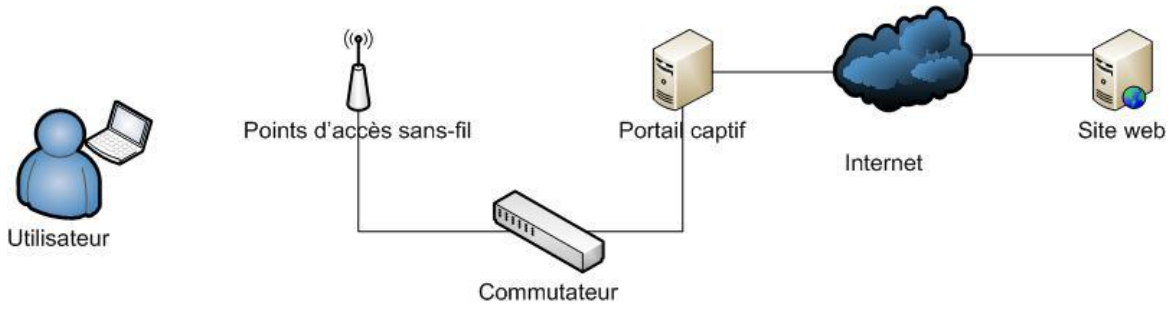


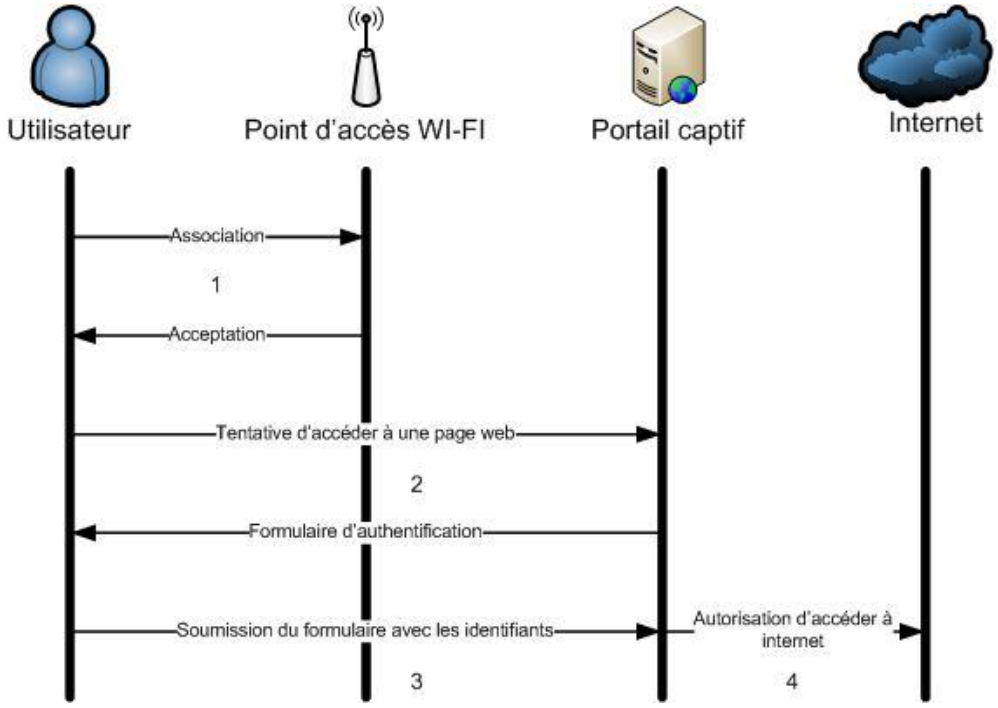
Les obligations légales concernant le contrôle des accès Internet sont gérées par la société ACI.

Document 3 - principes de la nouvelle solution d'authentification des professionnels extérieurs

3.1 Schéma et diagramme de séquence de l'authentification par un portail captif standard

3.2





1. Lors de la première étape l'utilisateur se connecte à la borne à partir d'un SSID.
2. Lorsque l'utilisateur veut accéder à une URL sur Internet, le portail captif envoie un formulaire d'authentification
3. Le formulaire comportant les champs d'authentification est transmis au portail captif
4. Si l'authentification est correcte le portail autorise l'accès à Internet.

3.3 Exposé de la solution d'authentification pour les professionnels extérieurs

La solution préconisée par la DSII pour les authentifications des professionnels extérieurs sera basée sur un portail captif intégrant un serveur DHCP et un serveur RADIUS gérant sa propre base de comptes. Celui-ci validera l'accès à internet et à des ressources réseaux. La séquence sera donc la suivante :

1. Demande d'association du portable Wifi du personnel extérieur au point d'accès via le SSID « visiteurs »
2. Transmission de la demande au contrôleur Wifi par le point d'accès
3. Positionnement dans le VLAN « visiteurs » par le contrôleur Wifi qui autorise uniquement l'accès au portail captif (pas de demande d'authentification par le contrôleur).
4. Requête DHCP au portail captif
5. Réponse DHCP qui envoie une adresse IP privée uniquement routable par le portail captif
6. Demande de connexion à une URL par le portable Wifi
7. Soumission d'un formulaire d'authentification par le portail captif
8. Envoi du couple « *login*/mot de passe » au portail captif
9. Le couple « *login*/mot de passe » saisi par l'utilisateur est transmis par le portail captif via une requête *Radius-Request* sur le port 1812 du serveur Radius intégré.
10. Après vérification, si la demande est acceptée le portail captif envoie un paquet de type *Radius-Accept* sinon un paquet de type *Radius-Reject*. Le serveur Radius enregistre dans son fichier d'activité (*log*) les éléments suivants : « *login*, adresse IP, date/heure, réponse ».
11. Si l'authentification est valide l'accès Internet est ouvert.

3.4 Plan d'adressage IP de la solution d'authentification des accès extérieurs

Le réseau IP des hospices est basé sur un adressage privé de classe A. L'adressage choisi pour l'accès des professionnels extérieurs sera basé sur un adressage privé de classe C.

La plage d'adresses distribuées par le serveur DHCP intégré au portail captif est [192.168.10.10/24, 192.168.10.210/24], la passerelle 192.168.10.250, et le serveur DNS 192.168.10.250.

L'adresse du serveur portail captif et serveur Radius sera 192.168.10.250/24.

L'adresse du pare-feu et du *proxy* coté VLAN « visiteurs » sera 192.168.10.254/24.

L'adresse publique du pare-feu permettant l'accès Internet sera de type 80.x.x.x. Le pare-feu prendra en charge la translation d'adresses (NAT/PAT).

L'adresse privée du pare-feu permettant l'accès aux ressources internes sera de type 10.x.x.x.

Document 4 - mise en place des éléments nécessaires au suivi du fonctionnement de la nouvelle solution d'authentification des professionnels extérieurs

4.1 Rappel sur les obligations légales

D'après le site cdse.fr

La loi pour la confiance dans l'économie numérique du 21 juin 2004 (dite LCEN) impose aux FAI la conservation des données « de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elle est prestataire » (article 6 II)…
L'article L.34-1 du code des postes et des communications électroniques (CPCE), modifié par la loi du 23 janvier 2006, tend à soumettre les personnes offrant au public à titre professionnel une connexion à l'Internet aux mêmes obligations que les opérateurs de communications électroniques classiques, s'agissant des obligations de conservation de données permettant l'identification des personnes utilisatrices des services fournis. Ainsi, en fournissant un accès Wifi au public à partir d'une connexion Internet, l'on endosse les mêmes responsabilités que le FAI….
Les données concernées sont, à titre d'exemple, les « log » de connexions (heures de connexion et durée de la connexion), l'adresse IP …
…le décret du 24 mars 2006 n'a pas retenu l'hypothèse consistant à demander aux exploitants de « cybercafés », d'hôtels ou de bars qui offrent une connexion Wifi, de relever l'identité de leurs clients. Il prévoit seulement la conservation des « données permettant l'identification ». Il s'agit donc, pour ces « fournisseurs de Wifi » de recueillir des informations qui, mises bout à bout, constituent un faisceau d'indices permettant l'identification …

4.2 Contrôle des accès Internet des professionnels extérieurs

Le Proxy utilisé par les hospices et traçant les accès à Internet s'appuie sur l'annuaire des hospices. On ne peut donc utiliser cette solution pour les accès des professionnels extérieurs.
Une solution spécifique, accessible uniquement au VLAN « Visiteurs », sera mise en place.
Elle sera composée d'un pare-feu (*firewall*) intégrant un serveur mandataire transparent à l'utilisateur (*proxy*) qui devra conserver dans un fichier d'activité (*log*) les données suivantes « adresse IP + date + heure + URL ».

Tous les accès routés par le portail Wifi sont transmises au pare-feu.
Les règles de filtrage du pare-feu n'autorisent que les accès Internet en provenance du *proxy*.
Le pare-feu autorise aussi les accès aux bases de données documentaires, aux revues médicales en ligne et autorise l'accès à certains services comme l'impression par exemple.

4.3 Supervision de l'infrastructure spécifique à l'authentification des professionnels extérieurs

L'ensemble des infrastructures Wifi est supervisé par un logiciel de supervision « propriétaire ». Celui-ci utilise entre autre chose, le protocole SNMP.
Tous les éléments participant à l'infrastructure Wifi sont testés périodiquement par le superviseur ou peuvent déclencher des alertes.
En cas d'incident un *mail* et un *sms* sont envoyés aux différents administrateurs en charge de l'infrastructure. Un ticket d'incident est automatiquement généré sur le gestionnaire d'incidents.
La nouvelle solution pour les professionnels extérieurs doit être intégrée dans le dispositif de supervision existant.
Cependant le prototype utilisé pour les tests ne comportera pas ce dispositif qui sera testé et mis en place dans l'infrastructure définitive.

4.4 Gestion des fichiers d'activité

Les fichiers d'activités (log) du portail captif et du serveur Radius doivent être archivés sur le serveur de sauvegarde **BacLog** dans le répertoire /var/log/VisiteursCaptifs.
Les fichiers d'activité se trouvent dans les répertoires /var/log/radius et /var/log/proxy sur les serveurs correspondant. Il peut y avoir plusieurs fichiers d'activité si le service a été démarré.
Ce serveur est accessible via le protocole SSH. L'accès via SSH est protégé par un cryptage asymétrique basé sur une clé privée située sur le client SSH et sur une clé publique située sur le serveur SSH.
Avant transmission les fichiers d'activité doivent être compressés. Quel que soit le nombre de fichiers d'activité il y aura un seul fichier compressé transmis qui sera préfixé par la date du jour.
La transmission des fichiers se fera tous les jours vers 23h30.

Document 5 : Éléments à prendre en compte pour l'environnement de tests

5.1 Consignes pour les tests de la solution

La solution « portail captif » spécifique aux professionnels extérieurs, basée sur le logiciel « amigopod » doit être testée.
Celle-ci est disponible sous la forme d'une machine virtuelle qui permet de la tester avant de la mettre en œuvre.
Le test doit se dérouler dans un espace indépendant du réseau de production.
Le plan d'adressage actuel doit être respecté.
On souhaite que le test montre une connexion au SSID « visiteurs ».
On souhaite tester la configuration des points d'accès et du contrôleur Wi-Fi, l'accès contrôlé à Internet et aux ressources internes (ce dernier sera simulé par un serveur http d'adresse 10.10.10.100/26 pour les tests).

5.2 Éléments qui seront testés ultérieurement lors de l'intégration à l'infrastructure existante

On ne prendra pas en compte l'intégration au logiciel de supervision, ni les accès aux autres VLAN d'authentification. Lors de l'intégration, il faudra vérifier que la nouvelle solution ne perturbe pas le fonctionnement de l'infrastructure existante.

Dossier fourni pour réaliser les missions de la partie 2

Document 1 - déclaration de l'incident

Sujet : Incident N°12-3066
De : noply@support-HCL.fr
Réponse à : noply@support-HCL.fr
Date : 11:12
Pour : Estelle.durand@pediatrie-hcl.fr

Bonjour,

Cet appel concerne :

Pédiatrie – B1 – Bâtiment B
Site Pasteur
04 27 40 2842

Contact :

Melle. Estelle Durand
Poste 4523
Estelle.durand@pediatrie-hcl.fr

Objet de l'appel : Poste qui n'a plus accès au réseau

Paramètres IP transmis :
IP 192.168.0.26
Masque 255.255.255.0
Passerelle 192.168.0.254
DNS 192.168.0.254
DHCP 192.168.0.254

Ceci est un message automatique, veuillez ne pas répondre

Document 2 - structure logique du réseau

2.1 Les réseaux virtuels (VLAN)

Le réseau est découpé en VLAN. Chaque VLAN autorise mille adresses IP. Les 150 premières adresses de chaque Vlan sont réservées aux adresses IP fixes.
Les hospices différencient deux types de VLAN : des VLAN géographiques (exemple : Bâtiment A →VLAN 3, Bâtiment B →VLAN 4) et des VLAN métiers (exemple : Vidéosurveillance, imagerie, etc.). Pour les différencier les VLAN de 2 à 50 sont dédiés aux VLAN géographiques et de 51 à 64 aux VLAN métier.
Il y a deux plages DHCP par VLAN distribuées par deux serveurs DHCP d'adresses 10.64.200.1 et 10.64.200.2.
Chaque VLAN possède une interface virtuelle sur le routeur et les routeurs disposent d'agent relais DHCP. L'affectation d'un port à un Vlan est faite en ligne de commandes par un paramétrage de chaque commutateur effectué par les ALI. Le VLAN par défaut est le « VLAN 1 ». Les ports d'interconnexion des différents *switch* peuvent transporter des trames des différents VLAN, ils sont donc en mode *tagged* (norme 802.1q). Les autres ports n'appartenant qu'a un seul VLAN sont affectés au VLAN en *untagged*.

2.2 **Extrait de la liste des VLAN des Hospices Civils**

N° VLAN	Désignation	Réseau	*Gateway*	Plage Adresse Fixe Serveur	Plage Adresse Fixe PC / IMPR	Plage DHCP Serveur 1	Plage DHCP Serveur 2
3	VLAN_BAT_A	10.64.8.0/22	10.64.8.11/22		10.64.8.1 10.64.8.150	10.64.8.151 10.64.10.75	10.64.10.76 10.64.11.254
4	VLAN_BAT_B	10.64.12.0/22	10.64.12.11/22		10.64.12.1 10.64.12.150	10.64.12.151 10.64.14.75	10.64.14.76 10.64.15.254
5	VLAN_BAT_C	10.64.16.0/22	10.64.16.11/22		10.64.16.1 10.64.16.150	10.64.16.151 10.64.18.75	10.64.18.76 10.64.19.254
6	VLAN_BAT_F	10.64.20.0/22	10.64.20.11/22		10.64.20.1 10.64.20.150	10.64.20.151 10.64.22.75	10.64.22.76 10.64.23.254
7	VLAN_BAT_G	10.64.24.0/22	10.64.24.11		10.64.24.1 10.64.24.150	10.64.24.151 10.64.26.75	10.64.26.76 10.64.27.254
8	VLAN_BAT_I	10.64.28.0/22	10.64.28.11		10.64.28.1 10.64.28.150	10.64.28.151 10.64.30.75	10.64.30.76 10.64.31.254
51	VLAN serveurs	10.64.200.0/22	10.64.200.11	10.64.200.1 10.64.203.200		10.64.203.201 10.64.203.224	10.64.203.225 10.64.203.254
56	VLAN_Imagerie	10.64.220.0/22	10.64.220.11		10.64.220.1 10.64.223.200	10.64.223.201 10.64.223.224	10.64.223.225 10.64.223.254
60	VLAN_Cuisine	10.64.236.0/22	10.64.236.11		10.64.236.1 10.64.239.200	10.64.239.201 10.64.239.224	10.64.239.225 10.64.239.254
62	VLAN_Administration	10.64.244.0/22	10.64.244.11		10.64.244.1 10.64.247.200	10.64.247.201 10.64.247.224	10.64.247.225 10.64.247.254
64	VLAN_Video_Surveillance	10.64.252.0/22	10.64.252.11		10.64.252.1 10.64.255.200	10.64.255.201 10.64.255.224	10.64.255.225 10.64.255.254
541	VLAN_Visio_Conférence	10.64.212.0/24	10.64.212.11		10.64.212.1 10.64.212.254		

2.3 **Raccordement des bâtiments au cœur de réseau**

Chaque bâtiment dispose d'un local technique avec plusieurs commutateurs dont un est relié au cœur de réseau de l'hôpital nommé « Auto 1 ». Les commutateurs sont administrables à travers les protocoles SNMP et SSH.

Les prises des bandeaux de brassage dans les locaux techniques sont numérotées. Ces numéros correspondent aux numéros des prises réseaux sur lesquelles se connectent les équipements terminaux.

Le tableau suivant présente un extrait des ports *taggés* sur chacun des commutateurs.

VLAN	**Bat K** **252.1**	**Bat K2** **252.18**	**Auto1** **10.250.1.21**	**Bat I** **252.26**	**Bat G** **252.4**	**Bat F** **252.5**	**Bat F2** **252.14**	**Bat C** **252.8**	**Bat C2** **252.20**	**Bat B** **252.6**	**Bat B2** **252.12**	**Bat B3** **252.13**
4	/	/	1/1/2		/	/		/		E26 E25	E49 E50	E25 E26
5	/	/	1/1/3		/	/		E25 E26 E2	E26			
6	/	/	2/1/2		/	E25 E26	E25	/				
7	/	/	2/1/3		E25	/		/				
8	/	/	2/1/4	?	/	/		/				
9	E26 E25	E26	3/1/1		/	/		/				

Document 3 – extrait de la documentation des commutateurs CISCO

3.1 Prise en charge des problèmes de sécurité associés au service DHCP par les commutateurs CISCO

Le DHCP *snooping* consiste à définir sur quels ports du *switch* il est normal de recevoir des paquets DHCP OFFER et ACK émis par les serveurs DHCP lorsqu'ils sont sollicités. Cette fonctionnalité permet de se prémunir contre les attaques de type :

- DHCP *snooping* (serveur DHCP illicite)
- DHCP *starvation* (de multiples requêtes DHCP qui réduisent le nombre d'adresses restantes, en fait une attaque de type déni de service)

Elle permet au *switch* d'accès de retenir certaines informations sur les ports configurés *untrust*.

3.2 Exemple de configuration du *DHCP snooping* sur un commutateur CISCO

Ici on définit une interface *trust* (resp. *untrust*) (ex : un port relié à un serveur DHCP légitime, ou un port *trunk* vers un *switch* de distribution) puis on limite le nombre de paquets DHCP par seconde émis sur un port ; enfin, on active la fonctionnalité sur tout un VLAN :

- *(config)#ip dhcp snooping*
- *(config-if)#ip dhcp snooping trust*
- *(config-if)#ip dhcp snooping limit rate 10*
- *(config)#ip dhcp snooping vlan 11*