

ÉTUDE DE CAS

CAS H

ÉLÉMENTS DE QUESTIONNEMENT

POUR UN SUJET ZÉRO

Commentaire [AVS1]: Il ne s'agit pas d'un modèle mais d'exemples de questionnement possible montrant les exigences attendues.

Le contexte

Les Hospices Civils 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 nécessite un réseau informatique performant.

Actuellement, le réseau informatique des Hospices Civils de XXX 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.

Commentaire [rs2]: Un contexte général qui précise l'organisation et ses objectifs, la place de l'étudiant dans cette organisation, le rôle et l'importance du SI

Commentaire [rs3]: Organisation et objectifs

Commentaire [rs4]: Rôle et importance du SI

Commentaire [rs5]: Situation de l'étudiant. Ici il est dans un service interne à l'organisation et non dans une organisation prestataire extérieure.

Partie 1 - Authentification des personnels extérieurs

Participation à la production de services

Vous participez, en tant que membre d'une équipe projet, à toutes les étapes de la mise en place d'une solution d'infrastructure concernant la prise en charge de l'authentification des accès Wifi du personnel extérieur aux Hospices civils, du choix de la solution à la réalisation et aux tests d'intégration. Pour cela vous vous appuyez sur différents dossiers documentaires : le dossier spécifique à la partie 1 et le glossaire

Mission 1 – Justification du choix d'une solution d'authentification

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. Il vous demande de lui préparer un argumentaire technique.

1.1. Préparer une liste d'arguments justifiant le choix de la solution technique, en intégrant la réponse aux questions suivantes :

- « Qu'est ce qu'un VLAN ? »
- « Qu'est ce qu'un SSID ? »
- « Quel est l'intérêt d'associer un SSID à un VLAN ? »
- « Peut-on utiliser les SSID et VLAN existants pour authentifier l'accès des personnels 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 ? »

Dans ce comité de pilotage seront aussi abordés les aspects juridiques de la nouvelle solution. C'est pourquoi votre chef de projet vous demande de compléter votre argumentaire.

1.2. Préciser en quoi la solution proposée répond aux contraintes légales qui s'imposent aux hospices civils en fournissant un accès internet à des personnels extérieurs.

Mission 2 – Prototypage de 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.

1.3. Justifier le nombre de connexions IP théoriques que peut fournir le portail captif
1.4. Donner un exemple de configuration IP du portable après une connexion réussie.
1.5. Donner un exemple de configuration IP d'une borne légère et déterminer la plage d'adresses utilisables par les bornes légères.

Commentaire [rs6]: Un projet général avec un objectif bien identifié auquel participe l'étudiant. Ce projet est découpé en missions à prendre en charge donnant lieu à des situations professionnelles qu'il va rencontrer.

→ l'étudiant peut ne pas prendre en charge la totalité d'une mission.

Commentaire [rs7]: La partie 1 est orienté processus 1

Commentaire [rs8]: Les missions d'une partie s'enchaînent logiquement. Toutes les missions du projet ne seront pas forcément traitées par l'étudiant.

Commentaire [rs9]: Pour qui et pourquoi ?

Commentaire [rs10]: Une question commence par un verbe d'action. Elle représente une activité plus ou moins complexe à réaliser au sein d'une mission.

Commentaire [rs11]: La forme est libre mais les réponses sont contraintes par les sous-questions.

Commentaire [rs12]: Il s'agit du socle de connaissances sur lequel s'appuie la compréhension de la question. Il peut aussi être aussi demander d'explicitier chaque notion utilisée.

Commentaire [rs13]: Pourquoi ne peut-on pas utiliser l'existant ?

Commentaire [rs14]: Pourquoi la solution proposée est intéressante et répond au besoin ?

Commentaire [rs15]: On est dans la même mission, mais après la situation professionnelle précédente.

Commentaire [rs16]: Changement de perspective et nouvelle situation professionnelle.

Commentaire [rs17]: C'est un impératif du métier

Commentaire [rs18]: • On reste dans le cadre de la proposition d'une solution d'infrastructure → C3.1.1.1 Lister les composants matériels et logiciels nécessaires à la prise en charge des processus, des flux d'information et de leur rôle
• C3.1.1.2 Caractériser les éléments d'interconnexion, les services, les serveurs et les équipements terminaux nécessaires

1.6. Expliquer la configuration des ports (*tagged, untagged, Vlan associés*) du commutateur auxquels seront connectés le point d'accès, le contrôleur Wifi, le portail captif et le routeur. Justifier votre réponse.

Mission 3 – Évaluation des risques associés à la nouvelle solution d'authentification

La solution retenue ne prend pas en charge PEAP. Votre chef de projet vous demande d'identifier les risques potentiels notamment concernant les points d'accès pirates.

1.7 Expliquer pourquoi le protocole PEAP protège contre les points d'accès pirates dans la solution d'authentification des personnels.

Mission 4 – 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 calculer la taille prise par la sauvegarde de ces fichiers d'activités.

1.8 Donner la formule permettant de calculer cette taille.

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. Pour cela vous vous appuyez sur différents dossiers documentaires : le dossier spécifique à la partie 2 et le glossaire

Commentaire [rs19]: Les missions s'enchaînent logiquement. Toutes les missions du projet réel ne seront pas forcément traitées par l'étudiant.

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 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 résolution, 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. Proposer 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 Wifi dans les hôpitaux civils.

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 permettre un accès à internet.

1.2 L'authentification de l'accès au réseau Wifi

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.

1.3 Le besoin

Actuellement, les personnels extérieurs aux hospices n'ont pas de solution dédiée. Ces personnels peuvent être notamment des médecins ne travaillant pas aux Hospices Civils et souhaitant utiliser un ordinateur portable personnel pour accéder à internet et à des services des Hospices Civils. Parmi ces services il y a notamment l'accès à Internet mais aussi et surtout l'accès à toute la base documentaire et aux revues scientifiques et médicales.

On ne souhaite pas authentifier les personnels extérieurs à travers l'annuaire déjà en place aux hospices.

Les personnes se trouvant dans cet annuaire sont exclusivement des employés internes. En effet tous les services informatiques des hospices s'appuient pour l'authentification et les habilitations sur l'annuaire. Le processus de création d'un utilisateur dans l'annuaire est donc nécessairement long alors que les personnels extérieurs restent peu de temps. 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 ne souhaitent donc pas intégrer des personnes extérieures même temporairement dans cet annuaire pas plus que dans le périmètre réseau dédié aux employés internes. 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 pour la télévision ou

Commentaire [rs20]: On présente ici le projet dans ces objectifs généraux.

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 personnels 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 personnels extérieurs, qui dans un premier temps permettra l'accès à Internet puis dans un second temps l'accès à des ressources réseaux.

1.4 La solution retenue à étudier

La solution choisie par les hospices est la mise en place d'un portail captif dédié aux personnels 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 personnels extérieurs sera le SSID « Visiteurs ».

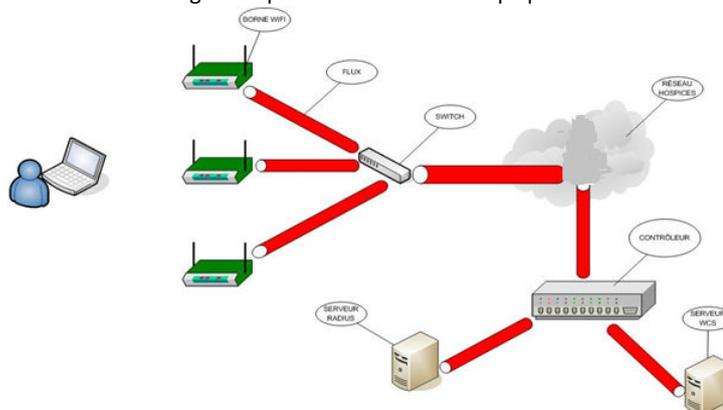
Document 2 - l'architecture Wifi actuelle

2.1 Une architecture Wifi centralisée basée sur le protocole CAPWAP

Il y a environ 2 000 points d'accès installés sur les différents établissements des hospices civils, ce qui en 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. Les points d'accès Wi-Fi sont reliés à un contrôleur . L'échange entre la borne légère et le contrôleur Wifi est gérée par le protocole CAPWAP. 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.

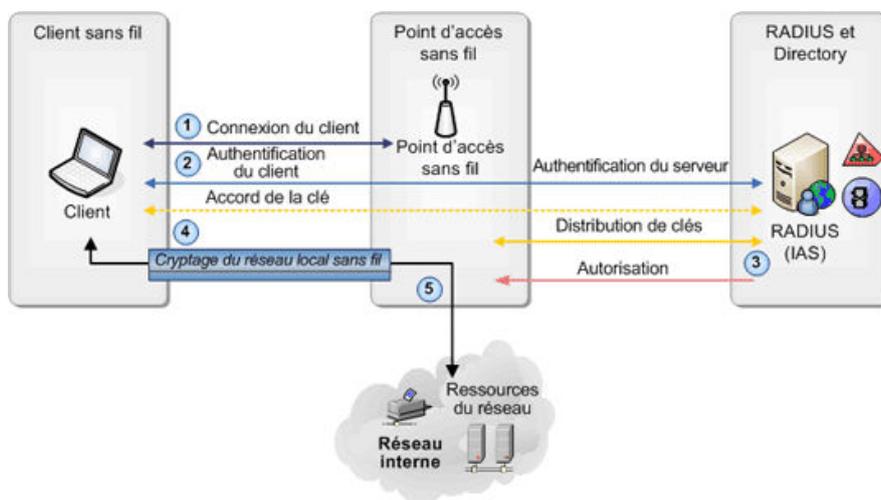


Les bornes Wi-Fi diffusent plusieurs SSID et chaque SSID correspond à un VLAN. Pour la communication avec les commutateurs, le protocole 802.1q (*tag*) est utilisé, chaque trame est donc « marquée » avec le numéro du VLAN correspondant.

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 point d'accès à l'aide de la clé de session
5. Accès au réseau local dans le Vlan autorisé



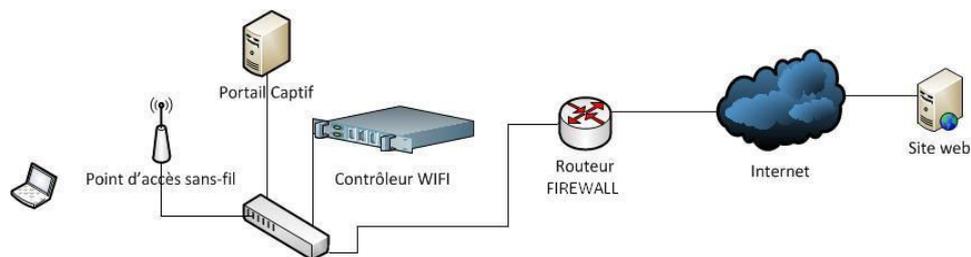
Source : authentification 802.1X et PEAP sur le réseau local sans fil

(<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.

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 personnels extérieurs

La solution préconisée par la DSII pour les authentifications des personnels 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 Wi-Fi du personnel extérieur au point d'accès via le SSID « visiteurs »
2. Transmission de la demande au contrôleur Wi-Fi par le point d'accès
3. Positionnement dans le VLAN « visiteurs » par le contrôleur Wi-Fi 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 Wi-Fi
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.

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

4.1 Rappel sur les obligations légales

D'après <https://www.cdse.fr/wifi-et-conservation-des-donnees.html>

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 Wi-Fi, 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 Wi-Fi » de recueillir des informations qui, mises bout à bout, constituent un faisceau d'indices permettant l'identification ...

4.2 Contrôle des accès Internet des personnels 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 personnels 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 transparent*) qui devra conserver dans un fichier d'activité (*log*) les données suivantes « adresse IP + date + heure + URL ».

Tous les accès routés par le portail Wi-Fi 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 Gestion des fichiers d'activité (log)

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`.

Ils appuieront sur 2 outils présents sur les systèmes utilisés : **cron** et **logrotate**.

Logrotate est paramétrée avec un période d'une journée et un cycle de rotation de 366. La transmission des fichiers vers le serveur **BacLog**, se fera tous les jours vers 23h30. Les fichiers d'activité sont compressés avec un taux de 50%. On estime que la taille maximum d'un fichier d'activité n'excédera pas les 1,5 Go.

Les fichiers d'activité se trouvent dans les répertoires `/var/log/radius` et `/var/log/proxy` sur les serveurs correspondant. .

Document 5 : Éléments à prendre en compte pour le prototypage

5.1 Vlan

Les différents Vlan à prendre en compte sont :

- Vlan administration Wifi 530
- Vlan Personnel 532
- Vlan Patients 534
- Vlan Visiteurs 536
- Vlan accès Internet Wifi 538

5.2 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 personnels 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 transparent* 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). Le pare-feu disposera d'une seule interface physique et de plusieurs interfaces virtuelles.

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

Les points d'accès sont paramétrés avec un adressage dynamique. Ils sont intégrés au Vlan d'administration Wifi 53. Sur ce Vlan ils reçoivent une adresse dans le réseau 10.64.208.0/22.

Mais la règle en vigueur concernant l'adressage sur le réseau de classe A des hospices, stipule que les 130 premières adresses de chaque Vlan sont réservées aux adresses IP fixes. Les 20 adresses suivantes constituent une réserve d'adresse de secours utilisables par le service ALI pour des besoins ponctuels

Le contrôleur wifi a **la dernière adresse IP disponible fixe** sur le réseau 10.64.208.0/22 (soit la 130^{ème} adresse). Il distribue l'ensemble des SSID et des Vlan au point d'accès.

5.3 Consignes

La solution « portail captif » spécifique aux personnels 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 du point 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).

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

On ne prendra pas en compte l'intégration au logiciel les 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 : noplay@support-HCL.fr
Réponse à : noplay@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

Note concernant le matériel touché par l'incident : Il s'agit d'un matériel nouvellement livré dans le bâtiment B. Il a été testé techniquement et paramétré par l'équipe informatique de l'ALI et ne présentait aucune défaillance.

Document 2 - structure logique du réseau

2.1 Les VLAN

Le réseau est découpé en VLAN. Chaque VLAN autorise mille adresses IP.

Les 130 premières adresses de chaque Vlan sont réservées aux adresses IP fixes. Les 20 adresses suivantes constituent une réserve d'adresse de secours utilisables par le service ALI pour des besoins ponctuels.

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 640 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 routeur possède une interface virtuelle par VLAN et ils disposent d'agent relais DHCP. L'affectation d'un port à un Vlan est faite en 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'à 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.

Document 3 - documentation associée aux commutateurs CISCO

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 sur un port.:

<i>(config)#ip dhcp snooping</i>	<i>Activation de la fonctionnalité</i>
<i>(config)#ip dhcp snooping vlan 11</i>	<i>Activation sur le VLAN</i>
<i>(config)#int fast 0/1</i>	<i>Configuration du port</i>
<i>(config-if)#ip dhcp snooping trust</i>	<i>Le port est autorisé à émettre des réponses DHCP</i>
<i>(config-if)#ip dhcp snooping limit rate 10</i>	<i>Le port n'accepte que 10 requêtes DHCP par seconde</i>

Glossaire

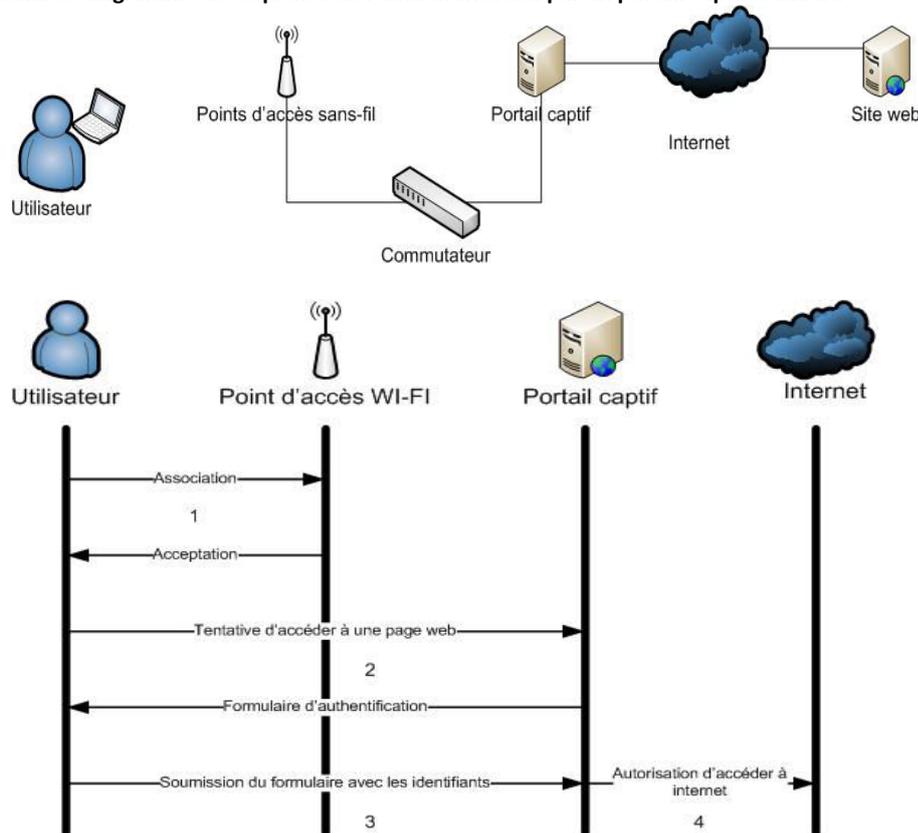
Portail captif

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

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



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

Le protocole CAPWAP (Control and Provisioning of Wireless Access Points)

Les solutions WiFi traditionnelles s'appuient sur points d'accès autonomes.

Ceux-ci, configurés individuellement, gèrent l'ensemble des paramètres (physiques, logiques, sécurité .etc.)

L'**architecture Wifi centralisée** propose une approche différente, le logiciel (*firmware*) et les paramètres de configuration du point d'accès (appelé ici borne légère Lightweight Access Point) sont chargés automatiquement à la mise sous tension de l'AP à partir d'un contrôleur chargé de gérer dynamiquement la configuration de ces bornes.

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

Selon le protocole CAPWAP de communication entre les points d'accès et leur contrôleur (RFC 5415 - 5418) standardisé depuis 2009, le fonctionnement (volontairement simplifié) est le suivant :

- le point d'accès s'allume et envoie une requête DHCP
- le serveur DHCP du contrôleur envoie :
 - une adresse IP de management
 - les SSID avec les VLANs associés

CRON

Cron est le nom d'un programme qui permet d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiées à l'avance, ou selon un cycle défini à l'avance.

Logrotate

Logrotate est le nom d'un programme permettant de faire des rotations sur les fichiers d'activités et de les sauvegarder à un endroit précis.

Une rotation signifie qu'au bout d'une période déterminée par un paramètre, le fichier d'activité en cours est copiée avec une extension correspondant à son numéro de rotation avant d'être réinitialisée.

Exemple :

Les paramètres de logrotate fixent la journée comme période et 2 comme nombre de rotations

le fichier proxy.log est sauvegardé tous les jours à 23h59 avec une rotation de 2 par une tâche cron.

On aura le premier jour un fichier proxy.log et un fichier proxy.log1, le 2^{ème} jour un fichier proxy.log et 2 fichiers proxy.log1 et proxy.log2 (il s'agit de l'ancien fichier proxy.log1) ., le 3^{ème} jour . un fichier proxy.log et 2 fichiers proxy.log1 et proxy.log2 (il s'agit de l'ancien fichier proxy.log1), l'ancien fichier proxy.log2 ayant été détruit.

DHCP snooping

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 pour éviter les serveurs DHCP illicites. Cette fonctionnalité permet de se prémunir contre les attaques de type DHCP *snooping* ou DHCP *starvation* Elle permet au *switch* d'accès de retenir certaines informations sur les ports configurés *untrust*.

DHCP starvation

Il s'agit d'une attaque par déni de service par l'intermédiaire de multiples requêtes DHCP qui réduisent le nombre d'adresses restantes.