

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

E5SR : PRODUCTION ET FOURNITURE DE SERVICES

SESSION 2018

Durée : 4 heures

Coefficient : 5

CAS HSP

Ce sujet comporte 16 pages dont 10 pages de documentation.

Il est constitué de deux parties qui peuvent être traitées de façon indépendante.
La candidate ou le candidat doit vérifier que le sujet qui lui est remis est complet.

Aucun matériel ni document autorisé.

Barème

Partie A	<i>Projet d'extension du réseau Wi-Fi dans la salle de visioconférence</i>	50 points
Partie B	<i>Projet de gestion des risques liés aux attaques virales</i>	50 points
	Total	100 points

Liste de la documentation jointe

Document 1 – Système informatique de l'hôpital HSP	7
Document 2 – Schéma du réseau de l'hôpital HSP	8
Document 3 – Extrait du cahier des charges sur le projet d'extension de la couverture Wi-Fi.....	9
Document 4 – Schéma logique du réseau Wi-Fi de l'hôpital HSP	9
Document 5 – Schémas décrivant l'accès au réseau de la salle de visioconférence	10
Document 6 – Extrait de l'audit interne relatif à la sécurité informatique de l'hôpital HSP	11
Document 7 – Extrait de la documentation des périphériques réseaux de l'hôpital HSP.....	11
Document 7.A - Extrait de la documentation JUNIPER SSG 320	11
Document 7.B - Extrait de la documentation HP Procurve 2810 48G	12
Document 8 – Extrait de la liste des commandes du HP Procurve 2810 48G	12
Document 9 – Extrait du cahier des charges pour prendre en compte des risques liés aux attaques virales.....	13
Document 10 – Solution de déploiement envisagée	14
Document 10.A - Extrait de la documentation du logiciel TM OSCE	14
Document 10.B - Exemple de script PowerShell permettant de vérifier le déploiement	15
Document 11 – Incident lors de la phase de déploiement.....	15
Document 12 – Extrait des règles de filtrage du routeur/pare feu RT-Cx	16
Document 13 – Plan amortissement du serveur (services comptables et financiers).....	16

BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 1/16

Présentation du contexte

Créée en 1984, **La Générale des hôpitaux (GDH)**, dont le siège est situé à Paris, est le premier groupe de cliniques et hôpitaux privés en France. Fort de 40 années d'expérience, GDH a su tirer profit du développement des dernières technologies médicales afin d'offrir aux patients des prestations couvrant une large variété de spécialités.

Inauguré en 1995, l'hôpital privé **HSP** (Hôpital Sud Paris) est le fruit du rattachement de plusieurs établissements indépendants au pôle territorial Paris Sud du groupe GDH. Situé dans la commune de Marreuil sur Seine, à 25km de Paris, l'hôpital compte 90 praticiens et dispose de 289 lits.

Associant des compétences diverses et complémentaires, l'établissement possède :

- un pôle de chirurgie ;
- un pôle de médecine ;
- un pôle de cancérologie ;
- un pôle de maternité ;
- un pôle d'imagerie médicale ;
- un service d'urgences 24h/24 7j/7.

Le réseau informatique de l'hôpital HSP compte près de 350 postes pour des utilisateurs variés (praticiens, employés administratifs, patients...). Sa gestion est sous la responsabilité de la **direction des systèmes informatique (DSI)** qui est en liaison avec le siège de GDH.

Chaque fin d'année, la DSI organise une réunion avec les principaux chefs de service afin de faire un bilan de l'année écoulée. L'objectif est aussi de déterminer les futures évolutions à apporter au système d'information. Suite à la dernière réunion, deux projets sont à l'étude.

Le premier projet concerne l'extension de la couverture du réseau Wi-Fi dans la salle de visioconférence située au 2^{ème} sous-sol.

Le second projet concerne la sécurité du système informatique et fait suite à une attaque virale subie en début d'année. Un virus de type rançongiciel (*ransomware*) a endommagé des machines et entraîné des pertes de données. L'objectif est de centraliser la gestion des antivirus et de mettre à jour la politique de sauvegarde des données.

Le chef du service réseau souhaite profiter de ces projets pour auditer la politique de sécurité informatique de l'hôpital au regard des exigences de la norme **ISO/CEI 27002** relative à la **sécurité de l'information**.

Au sein du service réseau de la DSI de l'hôpital HSP, vous travaillez sur ces deux projets.

Dans un premier temps, votre travail consistera à participer à la proposition de solutions techniques répondant aux besoins définis sur chacun des projets. Dans un second temps, vous participerez à leur mise en œuvre. Pour réaliser les différentes missions, vous vous appuierez sur le dossier documentaire fourni.

BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 2/16

Partie A – Projet d'extension du réseau Wi-Fi dans la salle de visioconférence

Dans le cadre de ce projet, votre participation consiste, dans un premier temps, à étudier les actions à mettre en œuvre afin d'étendre le réseau Wi-Fi existant dans la salle de visioconférence. Dans un deuxième temps, vous passez à la réalisation effective des modifications et aux vérifications de sécurité.

Mission 1 – Étude de la conformité de la solution proposée

Le chef de service vous demande de vérifier la pertinence des modifications envisagées par rapport aux besoins exprimés.

- | | |
|-------|--|
| A.1.1 | Expliquer comment l'architecture proposée répond aux besoins suivants :
a) isolation des flux Wi-Fi des autres flux de visioconférence ;
b) priorisation des flux de visioconférence sur les flux du réseau Wi-Fi ;
c) tolérance de panne garantissant une disponibilité de l'accès au serveur d'application du siège de GDH. |
| A.1.2 | Expliquer comment le commutateur SW-Ax pourra différencier les trames en fonction de leur VLAN lorsqu'elles entrent ou sortent par le port F1. |

Le contrôleur de points d'accès n'est pas configuré pour attribuer des adresses IP, il transmet les demandes de configuration IP des clients sans fil vers le serveur DHCP localisé dans le VLAN « **SERVEURS** ».

- | | |
|-------|--|
| A.1.3 | Expliquer pourquoi les datagrammes de découverte des serveurs DHCP, envoyés par les ordinateurs du réseau sans fil, peuvent traverser le cluster de routeurs RT-Cx et atteindre le serveur DHCP. |
|-------|--|

Votre chef de service vous demande de participer à la préparation d'une série de vérifications qui serviront à valider les travaux effectués.

- | | |
|-------|---|
| A.1.4 | Donner un exemple de configuration reçue par un client pour chacun des 2 réseaux Wi-Fi à étendre : PRATICIEN et PATIENT. L'exemple de configuration indiquera le SSID, la plus petite adresse IP de la plage d'hôtes, le masque et la passerelle. |
|-------|---|

Mission 2 – Mise en œuvre de la solution

Dans cette mission, vous passez à la phase de réalisation effective des modifications permettant d'étendre la couverture du réseau Wi-Fi dans la salle de visioconférence.

Après avoir réparti les tâches à effectuer, votre chef de service vous demande d'intervenir sur le commutateur SW-Ax.

- | | |
|-------|--|
| A.2.1 | Donner et expliquer toutes les modifications à réaliser sur le commutateur SW-Ax pour obtenir le fonctionnement attendu dans la nouvelle configuration du réseau de la salle de visioconférence. |
| A.2.2 | Citer, en les justifiant, les commandes de vérification à utiliser sur le commutateur SW-Ax afin de vérifier que les configurations effectuées répondent aux besoins exprimés. |

Mission 3 – Évaluation des risques liés à la fourniture d'un service

Afin de prendre en compte la norme ISO/CEI 27002 relative à la sécurité de l'information, vous participez à la réalisation d'un audit sur la sécurité du réseau.

Un premier document a été élaboré afin de recenser les menaces de sécurité susceptibles d'être rencontrées.

- A.3.1 a) Classer les menaces de sécurité figurant dans l'extrait du rapport d'audit en fonction des quatre couches du modèle TCP/IP : accès réseau, réseau (ou internet), transport et application.
- b) Préciser si le routeur RT-Cx dispose d'options permettant la détection des flux associés à du trafic malicieux (virus, scans de ports, attaques réseaux...).

Partie B – Projet de gestion des risques liés aux attaques virales

Vous participez aux différentes étapes permettant d'aboutir à une gestion centralisée des risques liés aux virus informatiques : déploiement d'une solution cohérente, sauvegarde de données et accord de niveau de service (ANS).

Mission 1 – Proposition d'une solution de déploiement d'un logiciel antivirus

Votre chef de service propose de déployer la solution TM OSCE (*Office Scan Corporate Edition*) sur l'ensemble des machines à protéger (PC, ordinateurs portables, machines virtuelles) via la configuration de stratégies de groupe (GPO¹).

Dans un premier temps, vous devez valider la proposition de déploiement envisagée.

B.1.1 Argumenter sur la conformité de la solution proposée avec les besoins exprimés dans le cahier des charges en justifiant :

- a) le choix du logiciel TM OSCE comme solution de protection antivirus ;
- b) le choix d'utiliser les stratégies de groupe (GPO) comme solution de déploiement du logiciel TM OSCE.

Vous devez ensuite prévoir un script qui permettra de tester l'efficacité de l'opération de déploiement afin de pouvoir identifier les machines n'ayant pas appliqué la stratégie de groupe. Un exemple est fourni.

B.1.2 Écrire le contenu du script PowerShell qui permettra de contrôler le résultat de l'opération de déploiement liée au VLAN « LABO ».

Mission 2 – Plan de sauvegarde et accord de niveau de service

L'attaque virale a entraîné des pertes de données sur des postes de travail utilisés par le **personnel administratif**. Le plan de sauvegarde existant ne concerne que la partie serveur et non les documents stockés sur les répertoires personnels des utilisateurs. La DSI a souhaité tirer profit de cette attaque pour auditer et mettre à jour sa politique de sauvegarde.

B.2.1 Rappeler l'intérêt de faire des sauvegardes incrémentales.

Il est prévu de mettre en place des répertoires partagés accessibles depuis les postes de travail du personnel administratif afin que les données de chaque utilisateur soient sauvegardées sur un serveur de fichiers.

B.2.2 Calculer, compte tenu du masque de sous-réseau utilisé dans le VLAN « ADMINISTRATIF » :

- a) le nombre maximum de postes de travail que ce réseau peut comporter ;
- b) le volume maximum de données qui peut remonter vers le serveur chaque soir.

1 Fonctions de gestions centralisées des ordinateurs et des utilisateurs dans un environnement Active Directory : règles à appliquer, déploiement de packages MSI (Microsoft System Installer)...

L'hôpital HSP utilise une solution de gestion de parc et d'incidents afin d'optimiser la gestion de son patrimoine informatique et le processus de gestion des incidents.

- B.2.3 a) Donner des critères permettant de fixer le degré de priorité d'un incident.
b) Fixer un degré de priorité de l'incident correspondant à l'attaque virale en justifiant votre choix parmi les possibilités suivantes : priorité basse, moyenne, haute ou majeure.

La DSI fait le constat que les utilisateurs ont pris l'habitude de signaler les incidents par l'envoi d'un courriel ou par téléphone. Ils utilisent très peu l'outil de gestion d'incidents et sa fonction d'assistance aux utilisateurs. C'est notamment ce qui s'est passé lors du signalement de l'attaque virale. Vous remarquez ainsi que cet outil n'a jamais fait l'objet d'une véritable politique de formation auprès des utilisateurs.

- B.2.4 Rédiger une note présentant les avantages, pour le service réseau et pour les utilisateurs de l'utilisation de la solution de gestion de parc et d'incidents.

Mission 3 – Prise en charge d'un incident

Lors du déploiement de l'antivirus, un échec a été constaté sur les postes du VLAN « OPHTALMO ». Sur les autres VLAN, le déploiement a été réalisé avec succès.

- B.3.1 a) Expliquer les causes de cet échec de déploiement.
b) Proposer une solution pour résoudre cet incident.

Mission 4 – Renouvellement d'un serveur

En concertation avec les services comptables et financiers de l'hôpital, la DSI s'interroge sur le renouvellement d'un serveur physique.

- B.4.1 Préparer les réponses aux questions suivantes que se pose la DSI sur le renouvellement du serveur :
- a) Notre serveur a-t-il déjà couvert sa période d'amortissement ?
 - b) Dispose-t-on, dans notre parc informatique, des outils permettant d'avoir une idée précise du nombre, de la nature et du coût des interventions de maintenance subies par ce serveur ?
 - c) Y a-t-il des risques à utiliser ce serveur au-delà de son cycle de vie prévu ?

Document 1 – Système informatique de l'hôpital HSP

Le cœur de réseau de l'hôpital HSP est constitué de deux routeurs de type JUNIPER SSG 320 (RT-Cx) implémentant le protocole VRRP². L'accès au réseau est assuré par des commutateurs de type HP PROCURVE 2810/48G.

Chaque service est dans un VLAN. Les VLAN sont gérés de façon statique. Le protocole VTP (*VLAN Trunking Protocol*) n'est donc pas utilisé au sein de l'hôpital.

Les trois cent cinquante postes clients sont sous système d'exploitation Windows et l'infrastructure serveur est virtualisée autour de la solution VMware ESXi. L'hôpital dispose aussi de quelques tablettes sous système d'exploitation Windows Professionnel.

L'adressage IPv4 est géré de manière dynamique pour l'ensemble des clients de l'infrastructure. Les serveurs sont en adressage fixe. Les serveurs présents sont les suivants :

Serveur RADIUS	172.16.123.69
Serveur PROXY	172.16.123.70
Serveur PORTAIL CAPTIF	172.16.123.71
Serveur AD (LDAP)/DNS/DHCP	172.16.123.72
Serveur SUPERVISION	172.16.123.73
Serveur de gestion de parc et d'incidents	172.16.123.74
Serveur FICHIERS	172.16.123.75

Un serveur mandataire (PROXY) filtre les accès à internet en fonction des URL.

Les utilisateurs sont gérés par un contrôleur de domaine sous Windows server avec comme nom de domaine : *hsp-gdh.fr*. Des unités d'organisation (OU³) regroupent les utilisateurs par VLAN.

Exemple de localisation des utilisateurs du VLAN « ANGIO » dans l'annuaire :

DN⁴ : "OU=angio, DC=hsp-gdh, DC=fr"

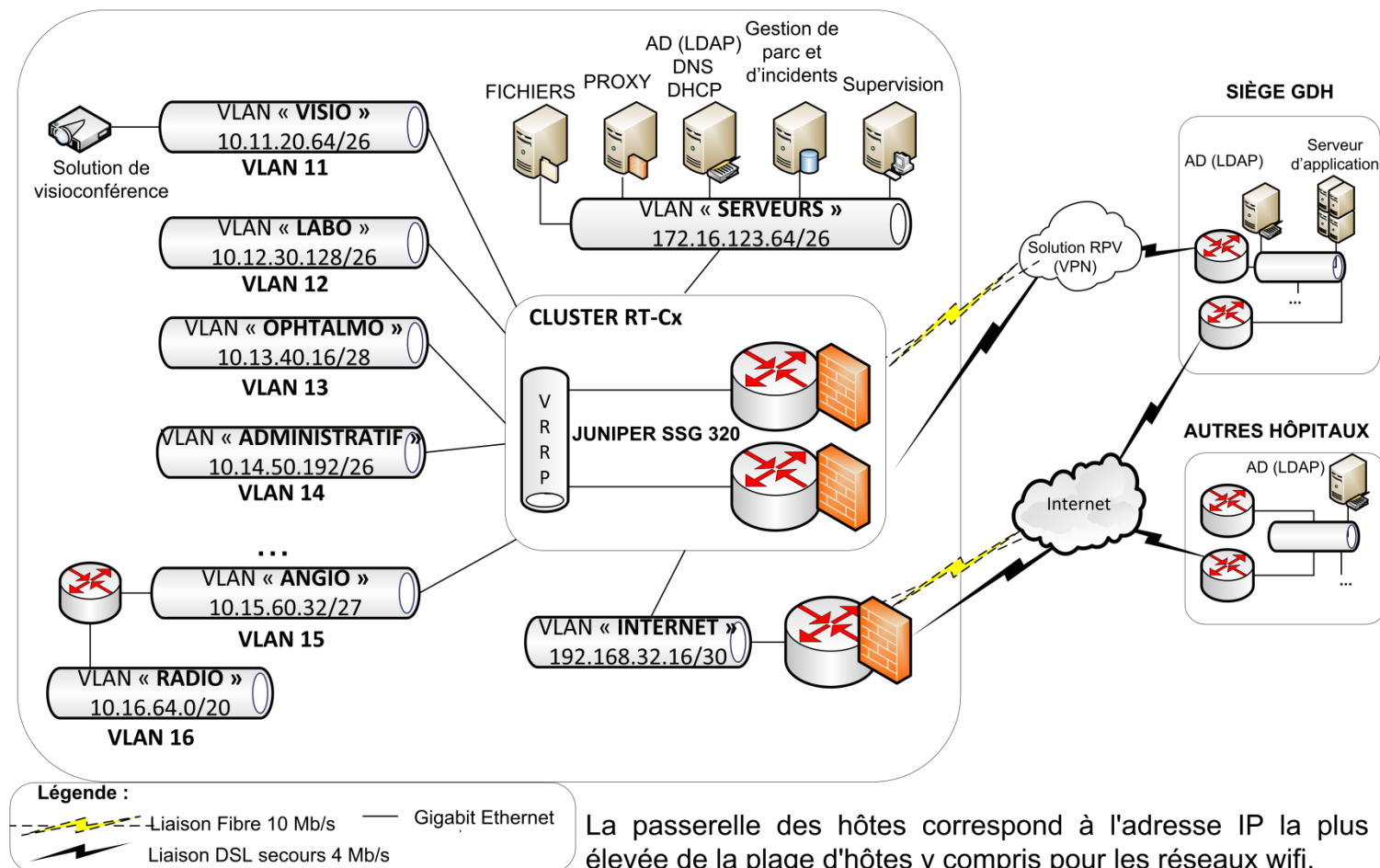
2 Protocole de redondance de routeur (*Virtual Router Redundancy Protocol*) assurant la haute disponibilité de la passerelle par défaut.

3 Objet de l'annuaire pouvant contenir des objets du domaine (*utilisateurs, ordinateurs...*).

4 Nom distinctif permettant de localiser un ou plusieurs objets dans l'annuaire Active Directory.

Document 2 – Schéma du réseau de l'hôpital HSP

HÔPITAL HSP



Dossier spécifique à la partie A

Document 3 – Extrait du cahier des charges sur le projet d'extension de la couverture Wi-Fi

Situation existante

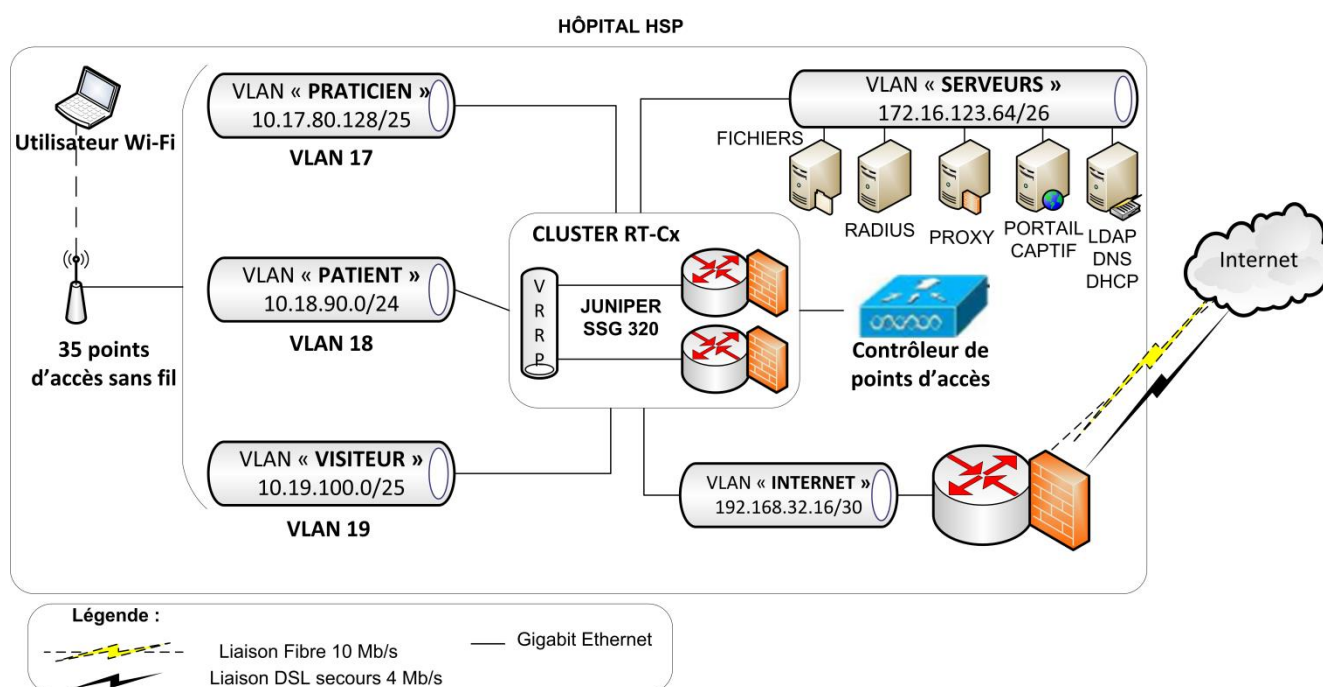
L'hôpital HSP est composé de deux bâtiments s'étendant sur 5 niveaux (niveaux -2 à 3). L'accès au réseau Wi-Fi est disponible pour trois catégories d'utilisateurs : praticiens, patients et visiteurs. Le réseau Wi-Fi est couvert par 35 points d'accès gérés par un contrôleur. La salle de visioconférence, située au niveau -2, n'est pas couverte par les ondes Wi-Fi. Le commutateur qui la dessert ne fait transiter que les flux associés au réseau de visioconférence. Elle comprend une vingtaine de machines autour d'un écran géant et d'un équipement de vidéoprojection.

Modifications envisagées

La direction de l'hôpital souhaite que la salle de visioconférence soit couverte par les réseaux Wi-Fi des praticiens et des patients. Pour arriver à cet objectif, la DSI a mis en avant les besoins de modification suivants :

- intégration d'un nouveau point d'accès, couvrant la salle de visioconférence, sur le modèle des 35 autres points d'accès déjà présents ;
- configuration de l'accès aux réseaux Wi-Fi sur le commutateur desservant la salle de visioconférence (accès aux réseaux Wi-Fi, priorisation des flux du vlan « VISIO »).

Document 4 – Schéma logique du réseau Wi-Fi de l'hôpital HSP

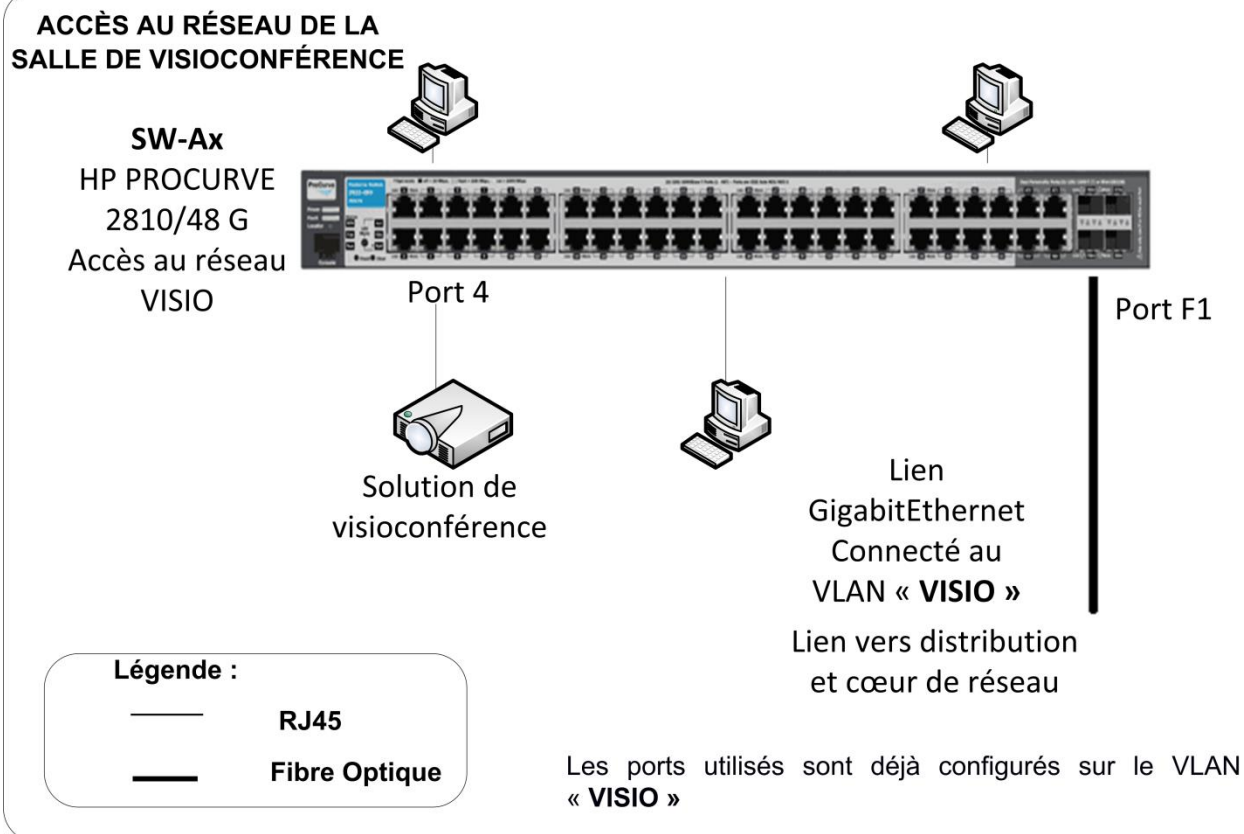


Les SSID des réseaux Wi-Fi portent le même nom que leur VLAN.

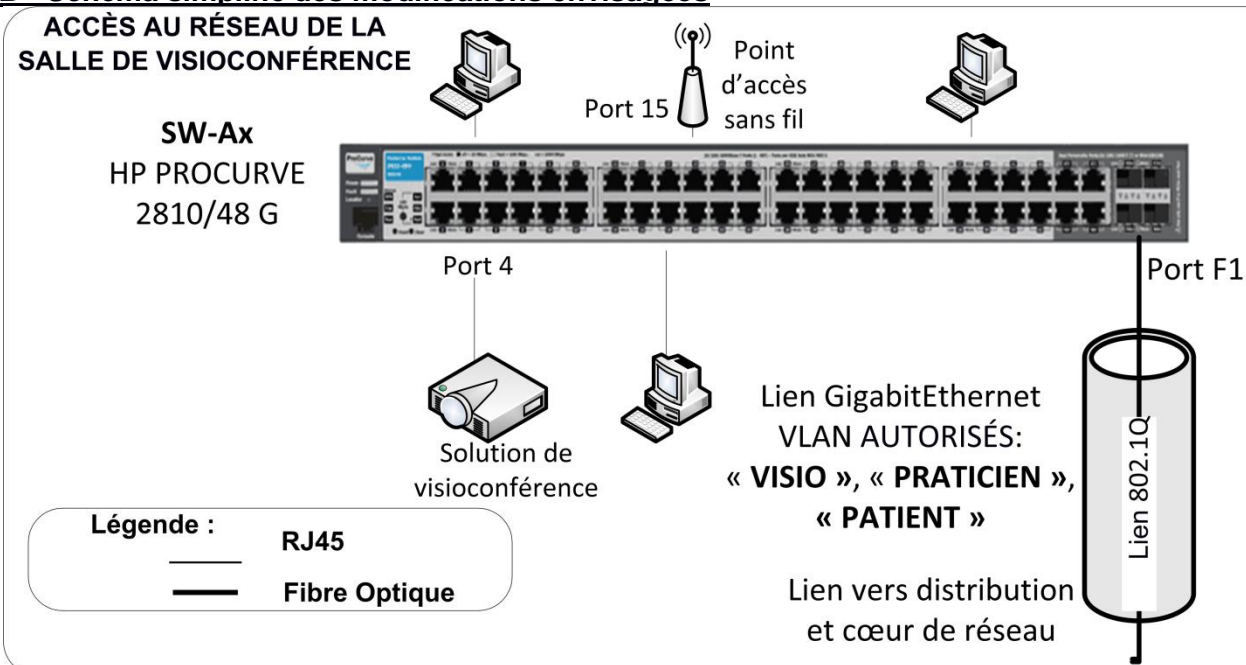
BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 9/16

Document 5 – Schémas décrivant l'accès au réseau de la salle de visioconférence

5A - Schéma simplifié de l'architecture existante



5B - Schéma simplifié des modifications envisagées



BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 10/16

Document 6 – Extrait de l'audit interne relatif à la sécurité informatique de l'hôpital HSP

Objectif

Prendre en compte les exigences de la norme ISO/CEI 27002 relative à la sécurité de l'information compte tenu de la croissance continue de l'informatique au sein des processus de soins.

Typologie des risques et des menaces (extrait)

- Menace 1 : un utilisateur appartenant au réseau Wi-Fi des patients parvient à exécuter des commandes *ping* qui ont abouti vers des machines appartenant au VLAN « LABO », ce qui est normalement interdit ;
- Menace 4 : un utilisateur connecté au réseau réalise une attaque de type MAC Flooding⁵ ;
- Menace 7 : un utilisateur du réseau accède à des sites web dont l'hôpital souhaite interdire l'accès (sites publicitaires, piratage, réseaux sociaux...).

Document 7 – Extrait de la documentation des périphériques réseaux de l'hôpital HSP

Document 7.A - Extrait de la documentation JUNIPER SSG 320

Source *juniper.net*

La gamme de routeurs JUNIPER SSG 320 est conçue pour satisfaire les exigences des clients en matière de réseau et de sécurité. Ces routeurs offrent 4 interfaces fixes 10/100/1000 ainsi que des emplacements PIM (*Physical Interface Module*) permettant une évolution vers des liaisons de type LAN SFP et WAN ADSL/ADSL2/ADSL2+ et G.SHDSL.

Dimension et alimentation

- dimensions (largeur, hauteur, profondeur) : 44,5x6,6x38,3 cm ;
- unité de rack : 1,5 ;
- blocs d'alimentation à sorties multiples : bloc d'alimentation qui fournit du courant au moyen de deux sorties principales, dont une de secours.

Routing

- routage IP statique, protocoles de routage dynamique : RIPv1/RIPv2, OSPF, RIPv6 ;
- agent relais DHCP ;
- traduction d'adresses réseau NAT/PAT ;
- IP virtuelles.

Gestion unifiée des menaces

- pare feu : des listes de contrôle d'accès (ACL) permettent de filtrer le trafic en fonction de l'adressage IP source et destination ainsi que des numéros de ports ;
- antivirus : antiespionnage (*antispyware*), antipublicité (*antiadware*), antienregistreur de frappe (*antikeystroke*)... ;
- antipourriels (*antispam*) ;
- intègre un système de prévention des intrusions. Les IPS (*Intrusion Prevention System*) écoutent le trafic afin de vérifier l'intégrité et la cohérence des échanges et peuvent prendre des mesures en cas de suspicion d'intrusion (blocage de ports, alerte courriel, etc.)

Qualité de service (QoS)

- mécanisme DiffServ (*Differentiated Services*) permettant de classer et de prioriser les flux dans le cadre de la qualité de service.

Haute disponibilité

- protocole VRRP (*Virtual Router Redundancy Protocol*).

5 *Attaque visant à saturer un commutateur de milliers d'entrées associant une adresse MAC à un port (inondation). Le but étant d'obtenir un épuisement des ressources du commutateur.*

BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 11/16

Document 7.B - Extrait de la documentation HP Procurve 2810 48G

Source *hp.com*

Les commutateurs HP PROCURVE 2810 48G offrent 44 ports 10/100/1000 ainsi que 4 ports de type mini-GBIC pour des liaisons fibres Gigabit Ethernet. Idéal pour les applications hautes performances, ces commutateurs offrent des options de sécurité et de surveillance du trafic.

Connectivité

- ports double personnalité : 4 ports 10/100/1000 ports ou slots SFP pour la connexion fibre (Gigabit-SX, LX, et LH, ou 100-FX).

Qualité de service

- qualité de service (QoS) via l'affectation de priorités (couche 2 et 3) : *Class of Service* (Cos), *Type of Service* (ToS) et DiffServ ;
- priorisation basée sur la couche 4 : configuration de priorités en fonction des ports TCP/UDP ;
- implémentation de la norme 802.1p : classification du trafic en temps réel avec huit niveaux de priorité numérotés de 0 (moins prioritaire) à 7 (priorité maximale), la priorité par défaut étant 0.

Fonctionnalités de couche 2

- gestion des VLAN, norme IEEE 802.1Q ;
- support des trames géantes : prise en charge de trames allant jusqu'à 9220 octets pour améliorer la performance du transfert de données volumineux.

Sécurité

- sécurité des ports : filtrage des adresses MAC (affectation statique ou apprentissage dynamique), limitation du nombre d'adresses MAC apprises ;
- VLAN privés : permet d'isoler un port des autres ports d'un même VLAN. Le port isolé peut communiquer avec la passerelle (liaison montante) ou avec des ressources partagées ;
- méthode d'authentification : norme IEEE 802.1X qui fait appel à un serveur RADIUS.

Document 8 – Extrait de la liste des commandes du HP Procurve 2810 48G

COMMANDE	EXPLICATION
show VLAN show VLAN <VLAN-id>	Affiche la liste des VLAN configurés sur le commutateur. En précisant l'identifiant de VLAN, la commande affiche des informations spécifiques sur un VLAN (ports, statut, mode...).
show running-config	Affiche la configuration en cours du commutateur (mémoire volatile).
show spanning-tree	Affiche les informations relatives à la configuration du protocole <i>spanning tree</i> (STP).
show qos vlan-priority	Affiche les priorités affectées aux différents VLAN.
show timep show sntp	Affiche la configuration associée à la synchronisation temporelle (protocole NTP).
show radius	Affiche la configuration associée à l'authentification RADIUS.
show logging	Affiche la liste des messages de journaux (logs) enregistrés.
show snmp-server	Affiche des informations sur la capture des événements associés au protocole SNMP.

BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 12/16

Document 9 – Extrait du cahier des charges pour prendre en compte des risques liés aux attaques virales

Situation existante

Antivirus

Le parc informatique de l'hôpital HSP comprend plusieurs logiciels antivirus gérés indépendamment sur chaque machine. Ce manque d'uniformité et de centralisation de la politique antivirale a été soulevé lors de la dernière réunion annuelle. Plusieurs points posent problème :

- l'absence de solution cohérente et centralisée : l'administrateur doit gérer indépendamment chaque antivirus sur l'ensemble des machines. Certaines installations proviennent d'opérations de maintenance non documentées. Parfois, plusieurs antivirus sont installés sur la même machine ;
- l'absence de suivi des mises à jour : les mises à jour régulières de chaque antivirus ne sont pas garanties et sont difficiles à suivre sur chaque machine.

Cette absence de cohérence et de centralisation a été signalée comme étant un facteur aggravant le risque d'attaque virale.

Sauvegarde

L'hôpital HSP dispose d'un plan de sauvegarde efficace et éprouvé de ses serveurs via une solution de sauvegarde. Cette solution offre en effet une sauvegarde puissante et performante des machines virtuelles VMware, une restauration rapide et flexible ainsi que des fonctionnalités avancées de réplication. La combinaison de cet outil avec la protection unifiée offerte par les périphériques de cœur de réseau JUNIPER SSG 320 a permis d'éviter la propagation, dans le VLAN « SERVEURS », de l'attaque virale subie au niveau des postes de travail administratifs.

Pour des raisons organisationnelles, chaque personnel administratif se voit affecter un bureau sur lequel un poste de travail est mis à sa seule disposition. Ces utilisateurs ont pris l'habitude de stocker des fichiers sur des répertoires locaux à leur poste de travail (brouillons, documents importants de travail stockés généralement dans le répertoire « *Mes Documents* »). Ce sont ces fichiers qui ont été endommagés suite à l'attaque virale. La DSI souligne que l'utilisation de supports amovibles pour la sauvegarde de ces fichiers est vecteur de contamination virale.

Besoins exprimés

Lors de la réunion, plusieurs demandes ont été formulées :

Concernant la politique antivirale :

- déployer une solution antivirale cohérente et centralisée sur un serveur :
 - ✓ la solution proposée devra se déployer sur l'ensemble des machines du parc informatique ;
 - ✓ les machines ayant subi un échec de déploiement devront être recensées automatiquement ;
 - ✓ le déploiement de l'antivirus devra se faire via des outils déjà présents dans le parc informatique de l'hôpital afin d'éviter l'achat d'un nouveau logiciel spécifique ;

BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 13/16

- garantir une protection spécifique contre les virus de type rançongiciel (*ransomware*) à l'origine de l'attaque subie par l'hôpital ;
- minimiser l'impact des analyses virales et des mises à jour sur les performances des machines et le trafic réseau ;
- pouvoir étendre la protection aux périphériques nomades de l'hôpital.

Concernant la politique de sauvegarde :

- prévoir la création de répertoires de partage sur un serveur de fichiers. Les données sauvegardées seront ainsi incluses au plan de sauvegarde existant qui prévoit des sauvegardes totales et incrémentales. Deux types de répertoires de partage sont nécessaires :
 - ✓ des répertoires personnels, propres à chaque utilisateur (lecture et écriture), avec un quota de 200 méga-octets chacun.
 - ✓ un répertoire commun, uniquement accessible en lecture seule, disposant d'un quota de 100 méga-octets.
- seuls les membres du VLAN « ADMINISTRATIF » (VLAN 14) seront concernés par la mise en place de ces partages.

Document 10 – Solution de déploiement envisagée

Le déploiement du logiciel TM OSCE (*Office Scan Corporate Edition*) est envisagé via la configuration d'une stratégie de groupe (GPO) de déploiement. Un script (*PowerShell*) sera utilisé afin de vérifier le succès du déploiement.

Document 10.A - Extrait de la documentation du logiciel TM OSCE

Source : docs.trendmicro.com

TM OSCE allie des technologies de sécurité antivirus sur site et dans le cloud pour protéger les serveurs de fichiers, les postes de travail physiques et virtuels et les ordinateurs portables. Cette solution est adaptée aux moyennes et grandes entreprises. L'installation se fait à l'aide de l'outil Client Packager qui propose la création de 3 types de pack : installation, mise à jour et composant MSI (*Microsoft System Installer*). Les principales caractéristiques sont :

Visibilité et contrôle centralisé

- centralise la gestion des postes de travail physiques et virtuels, ordinateurs portables, serveurs de fichiers et ordinateurs MAC au moyen d'une console web unique qui gère le serveur de déploiement ;
- permet d'étendre la protection des Solutions Techniques d'Accès (STA) aux smartphones et tablettes via le déploiement de *TM Mobile Security* (licence supplémentaire requise).

Sécurité optimale pour les infrastructures de postes de travail virtuels

- empêche les conflits de réseau, de processeur et de stockage en sérialisant les analyses anti-virales et les mises à jour ;
- réduit le temps d'analyses des postes de travail virtuels en établissant une liste blanche des images de base et des contenus précédemment analysés ;
- détecte et bloque les activités de chiffrement des rançongiciels (*ransomware*).

BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 14/16

Document 10.B - Exemple de script PowerShell permettant de vérifier le déploiement

Exemple de script permettant de contrôler le résultat d'exécution d'une GPO de déploiement :

```
Import-Module ActiveDirectory

Get-ADComputer -SearchBase 'OU=Test, dc=mycompany, dc=local' `
  -Filter '*' | foreach {

      Get-GPResultantSetOfPolicy -Computer $_.name `

      -ReportType Html `

      -Path E:\Data\rsop\$_name.htm

  }
```

La commande PowerShell Get-ADComputer permet de récupérer un ou des ordinateurs de l'annuaire Active Directory.

Les principaux paramètres sont :

- SearchBase : permet d'indiquer la partie de l'annuaire où effectuer la recherche en indiquant le DN (*Distinguished Name*);
- Filter : permet de préciser des critères de filtrage de la recherche (* signifie tous).

La commande PowerShell Get-GPResultantSetofPolicy permet d'afficher le résultat du jeu de stratégie de groupe (GPO) configuré sur une machine, un utilisateur ou les deux.

Document 11 – Incident lors de la phase de déploiement

A l'aide d'un script de vérification en PowerShell utilisant la commande PowerShell Get-GPResultantSetOfPolicy, vous constatez que le déploiement du logiciel antivirus a échoué sur toutes les machines du VLAN « OPHTALMO ».

Vous effectuez une commande *ping* d'une machine du VLAN « OPHTALMO » vers le serveur LDAP assurant la fonction de déploiement. Cette commande aboutit avec succès.

Vous contrôlez également le point de distribution logicielle (un dossier du serveur FICHIERS partagé sur le réseau). Il contient les fichiers nécessaires (notamment le paquet d'installation MSI).

En outre, le chef de service vous indique qu'il est intervenu récemment sur le routeur/pare feu RT-Cx.

BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 15/16

Document 12 – Extrait des règles de filtrage du routeur/pare feu RT-Cx

Les règles sont appliquées en sortie de l'interface associée au VLAN « SERVEURS ».

N°	Adresse source	Port source	Adresse destination	Port destination	Protocole	Décision
	
5	10.13.40.16/28	*	172.16.123.72/32	88 (KERBEROS)	TCP	Autoriser
6	10.13.40.16/28	*	172.16.123.72/32	389 (LDAP)	TCP	Autoriser
7	10.13.40.16/28	*	172.17.123.75/32	445 (SMB)	TCP	Autoriser
8	10.13.40.16/28		172.16.123.64/26		ICMP	Autoriser
	
14	10.14.50.194/32	*	172.16.123.64/26	22 (SSH)	TCP	Autoriser
15	10.14.50.192/26	*	172.16.123.72/32	53 (DNS)	UDP	Autoriser
	
Défaut	*	*	*	*	*	Refuser

Document 13 – Plan amortissement du serveur pour les services comptables et financiers

PLAN D'AMORTISSEMENT			
Nature de l'immobilisation : serveur (srv compt./financ.) Valeur d'origine : 9000 €			
Valeur amortissable : 6000 €		Taux d'amortissement : 0,2	
Date d'acquisition : 10/11/2016		Durée d'amortissement : 5 ans	
Date de mise en service : 15/11/2016		Prix de revente estimée : 3 000 €	
Années (date)	Annuités d'amortissement		Valeur nette comptable en fin d'exercice
	Montant	Montant cumulé	
31/12/2016	150 €	150 €	8 850 €
31/12/2017	1 200 €	1 350 €	7 650 €
31/12/2018	1 200 €	2 550 €	6 450 €
31/12/2019	1 200 €	3 750 €	5 250 €
31/12/2020	1 200 €	4 950 €	4 050 €
31/12/2021	1 050 €	6 000 €	3 000 €

La garantie serveur inclut trois ans pour les pièces, trois ans pour la main-d'œuvre et trois ans d'assistance sur site.

BTS services informatiques aux organisations		Session 2018
E5 : Production et fourniture de services informatiques	Code : SI5SISR	Page 16/16