**BTS SERVICES INFORMATIQUES AUX**

**ORGANISATIONS**

CAS HSP

**Liste de la documentation jointe**

[Document 1 – Système informatique de l'hôpital HSP 3](#_Toc472766015)

[Document 2 – Schéma du réseau de l'hôpital HSP 4](#_Toc472766016)

[Document 3 – Extrait du cahier des charges sur le projet d'extension de la couverture Wi-Fi 5](#_Toc472766017)

[Document 4 – Schéma logique du réseau Wi-Fi de l'hôpital HSP 5](#_Toc472766018)

[Document 5 – Schémas décrivant l'accès au réseau de la salle de visioconférence 6](#_Toc472766019)

[Document 6 – Extrait de l'audit interne relatif à la sécurité informatique de l'hôpital HSP 7](#_Toc472766020)

[Document 7 – Extrait de la documentation des périphériques réseaux de l'hôpital HSP 7](#_Toc472766021)

[Document 7.A - Extrait de la documentation JUNIPER SSG 320 7](#_Toc472766022)

[Document 7.B - Extrait de la documentation HP Procurve 2810 48G 8](#_Toc472766023)

[Document 8 – Extrait de la liste des commandes du HP Procurve 2810 48G 8](#_Toc472766024)

[Document 9 – Extrait du cahier des charges pour prendre en compte des risques liés aux attaques virales 9](#_Toc472766025)

[Document 10 – Solution de déploiement envisagée 10](#_Toc472766026)

[Document 10.A - Extrait de la documentation du logiciel TM OSCE 10](#_Toc472766027)

[Document 10.B - Exemple de script PowerShell permettant de vérifier le déploiement 11](#_Toc472766028)

[Document 11 – Incident lors de la phase de déploiement 11](#_Toc472766029)

[Document 12 – Extrait des règles de filtrage du routeur/pare feu RT-Cx 12](#_Toc472766030)

[Document 13 – Plan amortissement du serveur (services comptables et financiers) 12](#_Toc472766031)

**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 2ème 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.

|  |
| --- |
| **Dossier commun aux deux parties** |

# 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 VRRP[[1]](#footnote-1). 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 (OU[[2]](#footnote-2)) regroupent les utilisateurs par VLAN.

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

DN[[3]](#footnote-3) : "OU=angio, DC=hsp-gdh, DC=fr"

# Document 2 – Schéma du réseau de l'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.

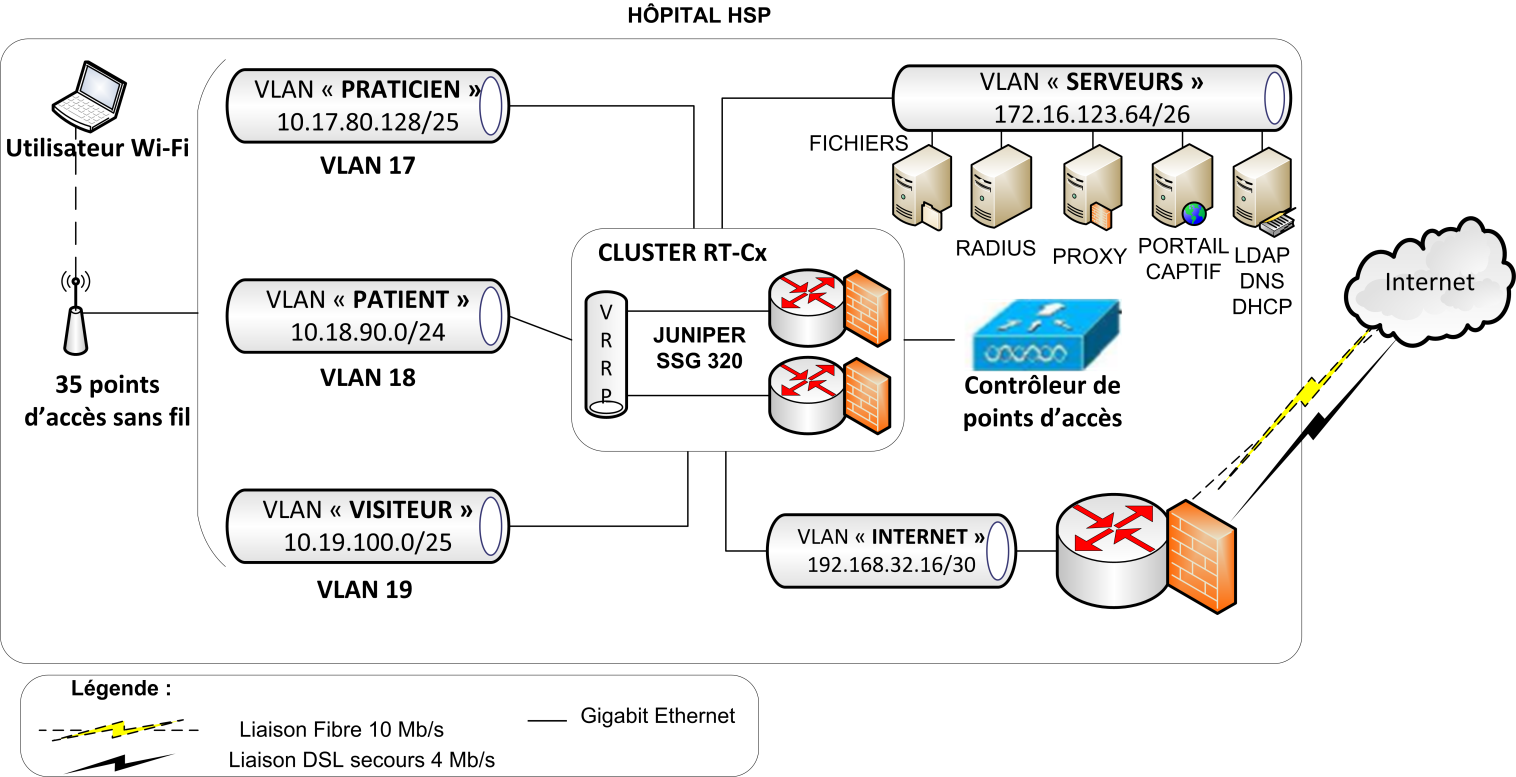
Le réseau Wi-Fi est couvert par 35 points d'accès gérés par un contrôleur. La salle de visioconférence, située au niveau -2, n'est pas couverte par les ondes Wi-Fi. Le commutateur qui la dessert ne fait transiter que les flux associés au réseau de visioconférence. Elle comprend une vingtaine de machines 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 »).

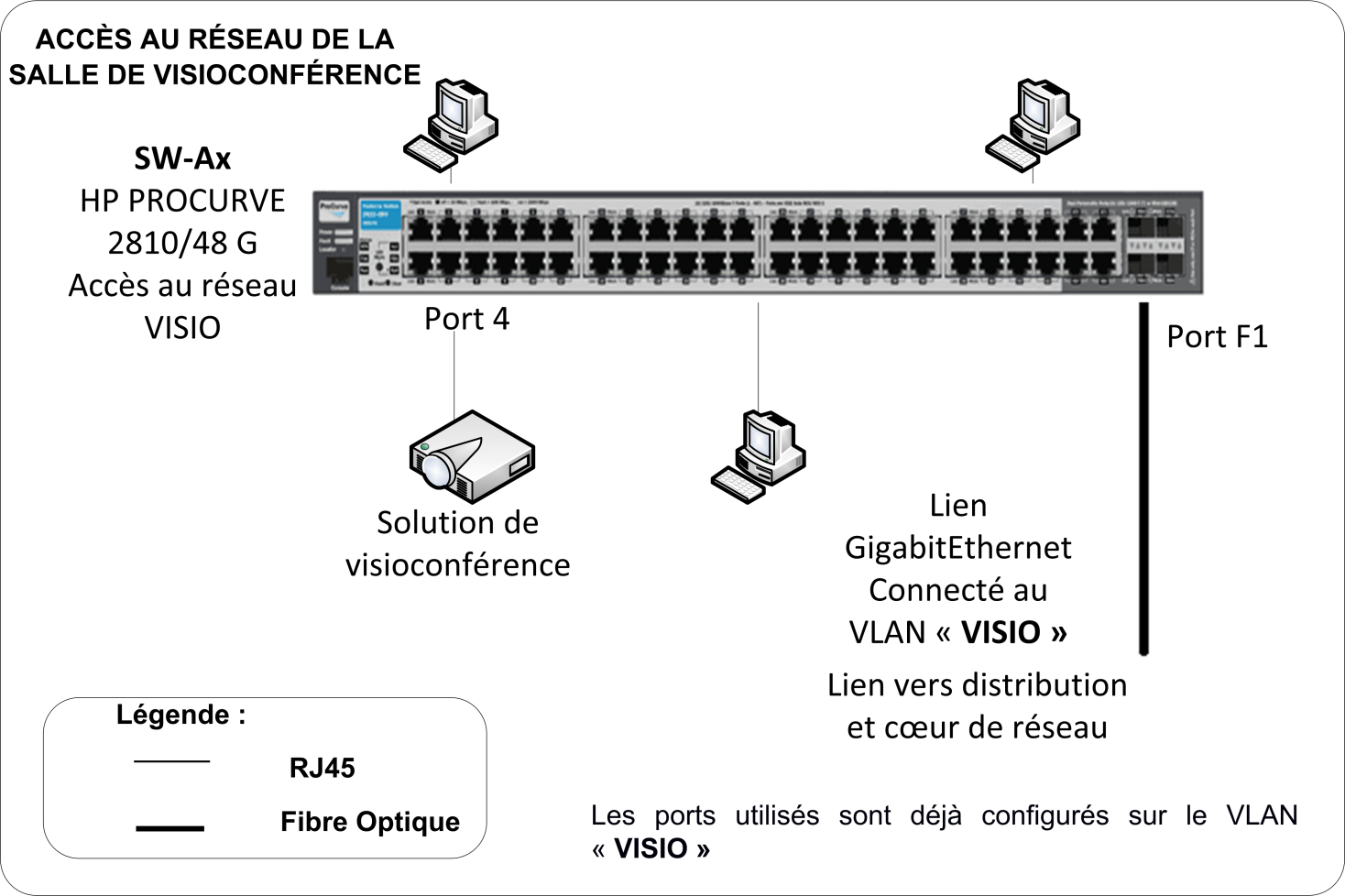
# Document 4 – Schéma logique du réseau Wi-Fi de l'hôpital HSP



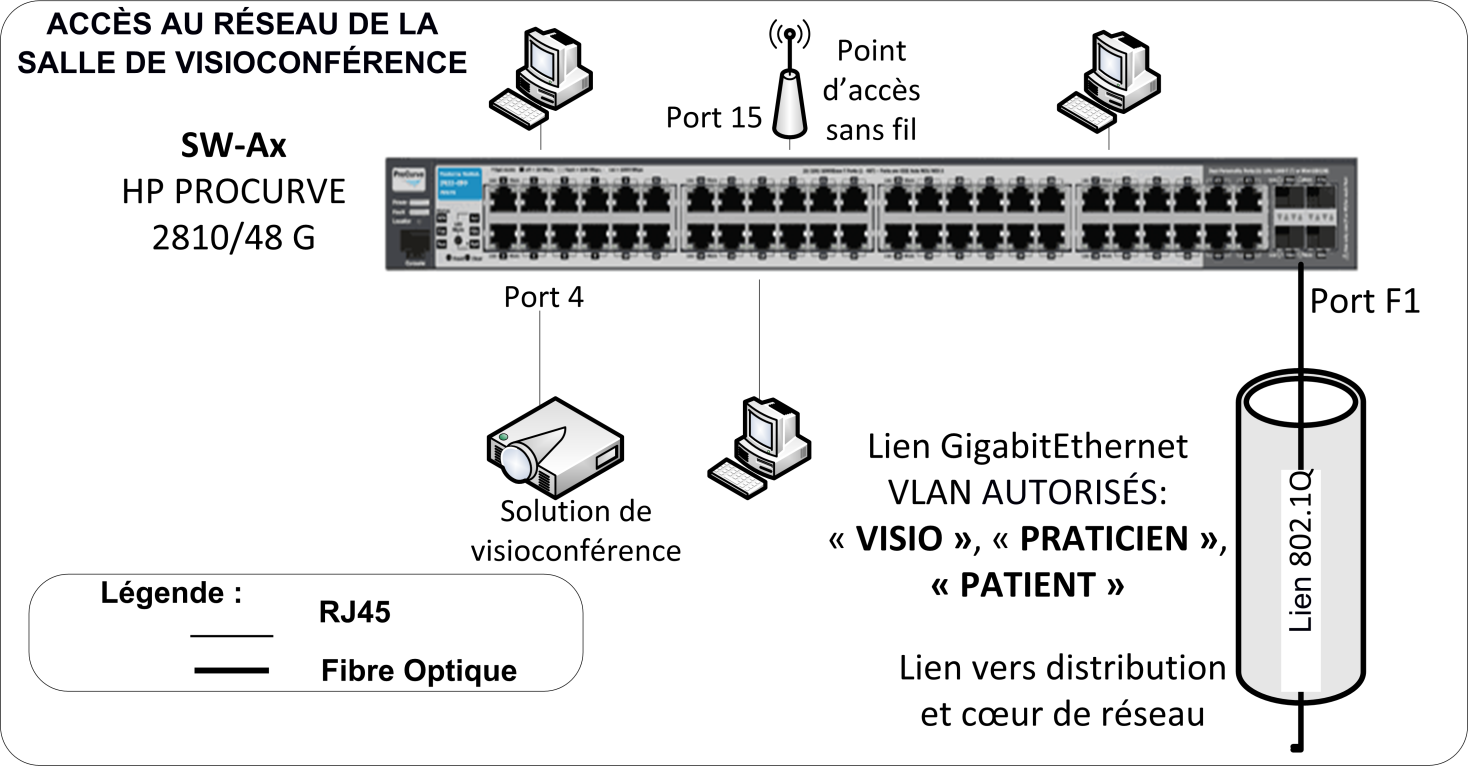
Les SSID des réseaux Wi-Fi portent le même nom que leur VLAN.

# 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**

****

# 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 Flooding[[4]](#footnote-4) ;
* 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) : 44,5х6,6х38,3 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.

Routage

* routage IP statique, protocoles de routage dynamique : RIPv1/RIPv2, OSPF, RIPng ;
* 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 : antiespiongiciel (*antispyware*), antipubliciel (*antiadware*), antienregistreur de frappe (*antikeylogger*)... ;
* 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*).

## 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 *spanning tree* (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. |

|  |
| --- |
| **Dossier spécifique à la partie B** |

# 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 ;
* 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 Packagerqui 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*).

## 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.

# 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 compta./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.

1. *Protocole de redondance de routeur (*[*Virtual Router Redundancy Protocol*](https://en.wikipedia.org/wiki/Virtual_Router_Redundancy_Protocol)*) assurant la haute disponibilité de la passerelle par défaut.* [↑](#footnote-ref-1)
2. *Objet de l'annuaire pouvant contenir des objets du domaine (utilisateurs, ordinateurs...).* [↑](#footnote-ref-2)
3. *Nom distinctif permettant de localiser un ou plusieurs objets dans l'annuaire Active Directory.* [↑](#footnote-ref-3)
4. *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.* [↑](#footnote-ref-4)