

**E5SR : PRODUCTION ET FOURNITURE DE
SERVICES INFORMATIQUES**

Durée : 4 heures

Coefficient : 5

CAS SAVEOL

Ce sujet comporte 18 pages dont 11 pages de documentation.
Il est constitué de deux parties qui peuvent être traitées de façon indépendante.
La candidate ou le candidat est invité-e à vérifier que le sujet qui lui est remis est complet.

Aucun matériel ni document n'est autorisé

Barème

<i>Partie A</i>	<i>Fourniture de services</i>	<i>48 points</i>
<i>Partie B</i>	<i>Production de services</i>	<i>52 points</i>
	<i>Total</i>	<i>100 points</i>

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 1/18

Liste de la documentation jointe :

Partie A - Fourniture de services	4
Partie B - Production de services.....	6
DOCUMENTATION DES TECHNOLOGIES EN ŒUVRE CHEZ SAVEOL.....	8
Document T1 - Extrait de la gestion des incidents ITIL V2	8
Document T2 - Le logiciel Puppet.....	8
Document T3 - Protocoles de redondance HSRP, VRRP et GLBP	9
DOCUMENTATION COMMUNE AUX DEUX PARTIES	10
Document 1 : Système informatique de Savéol.....	10
Document 2 - Extrait du plan d'adressage IP du siège	11
Document 3 - Schéma de l'infrastructure Réseau & Système de SAVEOL.....	12
DOCUMENTATION POUR LA PARTIE A.....	13
Document A1 - Éléments d'information sur le nouveau serveur <i>proxy-cache</i>	13
Document A2 - Configuration client/serveur de Puppet	13
Document A3 - Utiliser <i>Puppet</i> pour configurer les serveurs NTP	13
Document A4 - Extrait de la fiche d'incident / relevé des tests	14
Document A5 - Extrait des tables de routage	15
DOSSIER DOCUMENTAIRE POUR LA PARTIE B.....	16
Document B1 - Implémentation HSRP sur les routeurs	16
Document B2 - Compte rendu de la réunion VPN du 4 mai 2015	17

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR		SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS		
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 2/18

Présentation générale

En 1981, deux coopératives agricoles de la région brestoise ont fusionné et donné naissance à la société coopérative agricole Savéol (qui signifie « lever de Soleil » en breton). Savéol a été rejointe en 2002 par la coopérative du "Val Nantais" spécialisée notamment dans la culture de mâche ainsi que par la société d'intérêt collectif agricole "Les primeurs du mistral" produisant également des tomates à Lançon de Provence près de Marseille. En deux décennies, Savéol est devenue le leader de la production de tomates en France (plus de 70 000 tonnes par an).

La société Savéol propose des prestations pour environ une centaine de maraichers adhérents, principalement situés dans le département du Finistère. Ces prestations sont les suivantes : gestion la chaîne commerciale (marketing, conditionnement, commercialisation et livraison) ; conseil technique en agronomie ; recherche et développement de nouvelles espèces et de modes de production innovants plus respectueux de l'environnement.

A l'heure actuelle, 80% de la production est commercialisée sur le territoire métropolitain et 20% part à l'export vers les pays limitrophes de la France. La valorisation et la commercialisation des produits frais fragiles que sont les tomates et les fraises nécessitent une organisation et une logistique particulièrement rodées et efficaces. En effet, la récolte quotidienne, qui peut dépasser les 800 tonnes, sera déposée par les producteurs serristes dans l'une des deux stations de conditionnement afin d'être emballée dans un *packaging*¹ adapté au mode de vente et de transport. Les clients de Savéol (des enseignes de grande et moyenne surface ou des grossistes) sont assurés que leur commande sera livrée le lendemain au plus tard.

L'esprit d'innovation qui anime les administrateurs de la coopérative Savéol dans ses choix d'évolution se ressent aussi au niveau du pilotage et de la gestion de son système d'information. Le périmètre d'action de l'équipe du service informatique est diversifié et concerne la gestion de projet, le développement d'applications, l'assistance fonctionnelle utilisateur, la supervision et l'administration ainsi que la maintenance système et réseau.

Le service informatique, sous la direction de M. Netralli, compte une nouvelle chef de projet, Mme Farez, cinq techniciens réseau et système, ainsi que deux personnes en charge des solutions logicielles.

Vous êtes accueilli-e au sein de cette équipe. Il vous est précisé que votre domaine d'intervention concernera les fonctions liées à la gestion et à l'évolution de l'infrastructure système et réseau.

¹L'anglicisme « *packaging* » regroupe les deux notions : le conditionnement et l'emballage

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR					SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS				
SESSION 2015		SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES						
Durée : 4h		Coefficient : 5			Code sujet : SI5SISR			Page : 3/18	

Partie A - Fourniture de services

Éléments du dossier documentaire nécessaires pour la partie A :

- Dossier commun, documents de la partie A et documentation des technologies Savéol

Afin d'économiser la bande passante sur le réseau, le service informatique a décidé de mettre en place un *proxy-cache* pour optimiser le téléchargement des logiciels et des mises à jour.

L'équipe doit réfléchir à l'intégration de ce service dans l'architecture existante et sa prise en charge par l'outil de déploiement de configurations *Puppet* utilisé dans l'entreprise.

Mission A.1 – Configuration du logiciel *Puppet* pour le *proxy-cache*

Tous les postes clients de Savéol sont configurés via le logiciel *Puppet* qui permet notamment un déploiement rapide des fichiers de configuration sur l'ensemble des STA (solutions techniques d'accès) concernées.

M. Netralli vous demande de configurer les postes de travail pour que le téléchargement des logiciels passe par le nouveau service *proxy-cache*.

Question A.1.1

Citer au moins deux arguments qui justifient l'utilisation du service *Puppet* pour réaliser le paramétrage des postes.

Pour sécuriser la connexion entre les clients et le serveur, le logiciel *Puppet* utilise des tunnels SSL/TLS. Ces derniers nécessitent une phase d'initialisation à réaliser une seule fois lors de la configuration du client.

Mme Farez ne connaissant pas l'outil *Puppet*, M. Netralli vous demande de l'informer sur la sécurité de cet outil.

Question A.1.2

- Lister les risques auxquels s'exposerait Savéol si les échanges entre les nœuds clients et le serveur *puppetMaster* n'étaient pas sécurisés.
- Expliquer les principes mis en œuvre pour sécuriser les échanges entre les nœuds clients et le service *puppetMaster*.

La nouvelle configuration doit être implémentée sur tous les clients du domaine équipés du système d'exploitation *Lubuntu*. Le nouveau module pour *Puppet* se nommera *clientProxy*.

Vous êtes chargé-e de préparer l'intervention.

Question A.1.3

Lister les étapes nécessaires à la mise en œuvre de ce nouveau module.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 4/18

Mission A.2 – Résolution d'un dysfonctionnement des accès distants

Le 5 mai 2015, suite à une rupture d'alimentation dans un local technique situé à Quimper, le réseau MPLS de l'opérateur a subi une panne de type *blackout* (coupure électrique générale) sur l'ensemble du département du Finistère. Cette panne a paralysé, pendant tout un après-midi, les accès des sites distants de Savéol au site informatique du siège.

Consécutivement à la remise en service du réseau MPLS, les routeurs de tous les sites Savéol ont été redémarrés avec leur dernière configuration enregistrée. Les jours suivant la panne du réseau étendu MPLS, plusieurs utilisateurs des sites distants ont signalé qu'ils constataient parfois des lenteurs anormales lors des accès aux serveurs du siège.

Un contact pris avec l'opérateur MPLS prouve que son infrastructure n'est pas en cause.

Afin de diagnostiquer l'origine du problème, les commandes et les relevés de configuration sur les équipements ont été réalisés et consignés dans la fiche d'incident qui vous a été transmise. La prise en charge et la résolution de cet incident vous sont confiées.

Question A.2.1

- a) Comparer la criticité de cet incident avec celle de la panne *blackout* subie précédemment par le réseau MPLS. Justifier votre réponse.
- b) Indiquer à quel niveau de la gestion des incidents ITIL cet incident sera pris en charge. Justifier.
- c) Identifier la raison des lenteurs signalées par les utilisateurs lors des accès aux ressources du siège et en exposer la(les) cause(s) possible(s).
- d) Donner une solution pour résoudre à chaud ce problème.
- e) Expliquer en quoi un protocole de routage dynamique éviterait ce problème à l'avenir.
- f) Indiquer le protocole de routage dynamique adapté à la situation vécue ici. Justifier votre réponse.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS		
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES			
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR		Page : 5/18

Partie B - Production de services

Éléments du dossier documentaire nécessaires pour la partie B :

- Dossier commun, dossier partie B et documentation des technologies Savéol

Mission B.1 – Tolérance aux pannes des accès externes

Suite à différents incidents, l'administrateur M. Netralli souhaite améliorer la tolérance aux pannes de la liaison entre le siège et les sites distants.

Mme Farez, en charge du pilotage du projet, envisage les choix suivants :

- les sites distants MPLS seront secourus en mode actif/passif avec HSRP ;
- l'accès internet du siège sera secouru en mode actif/actif avec GLBP.

M. Netralli se demande si la mise en œuvre du protocole GLBP ne serait pas aussi intéressante pour assurer la tolérance aux pannes des routeurs d'accès au réseau MPLS.

Mme Farez vous demande de préparer la réunion qui évaluera ces propositions.

Question B.1.1

- Justifier l'utilité d'un dispositif de tolérance aux pannes sur chacune des connexions (MPLS et internet).
- Définir les termes de continuité de service et d'équilibrage de charge et comparer les protocoles HSRP et GLBP sur ces deux critères.
- Justifier la pertinence du choix du protocole de tolérance aux pannes proposé par Mme Farez pour l'accès au MPLS ainsi que celui proposé pour l'accès internet du siège de SAVEOL.

À l'issue de la réunion, une série de tests sont faits sur un prototype de la solution.

Mme Farez désire valider la configuration HSRP de tolérance aux pannes mise en œuvre sur les routeurs MPLS. Pour cela, elle vous soumet les résultats des étapes de configuration ainsi que les tests de vérification effectués et vous demande de finaliser la solution.

Question B.1.2

À partir des configurations et des tests fournis par Mme Farez :

- Relever les indications vous permettant d'affirmer que le système est correctement paramétré pour le VLAN « Bureaux ».
- Indiquer les paramétrages nécessaires pour rendre la solution opérationnelle sur l'autre VLAN.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 6/18

Mission B.2 – Mettre en place un accès sécurisé distant pour les administrateurs réseaux

Un accès VPN géré par l'opérateur MPLS est prévu pour permettre aux personnels nomades de l'entreprise d'accéder aux ressources centrales.

M.Netralli et Mme Farez souhaitent mettre en place un accès VPN indépendant, réservé au service informatique et permettant de prendre la main sur les différents équipements actifs et sur les serveurs.

Dans la continuité des choix technologiques actuels, une solution basée sur le logiciel libre *OpenVPN* est étudiée.

Une première réunion rapide a défini les orientations principales.

Le serveur *OpenVPN* de test a été paramétré. On vous demande de préparer la fiche d'intervention pour compléter le prototype correspondant au schéma prévu.

Question B.2.1

- a) Lister, en les justifiant, les installations à réaliser sur le poste de travail prévu pour le test.
- b) Détailler les configurations à réaliser sur le pare-feu Zyxel pour que le serveur *OpenVPN* soit accessible.
- c) Indiquer les adresses IP (source et destination) et les numéros de ports que devrait contenir un paquet émis par le poste de test, capturé à l'entrée du pare-feu Zyxel.

Mme Farez désirerait aussi valider le choix du serveur physique destiné à accueillir le serveur VPN dans une machine virtuelle. Elle s'inquiète notamment de savoir si les différents paramètres ayant concouru à la détermination du TCO (*total cost of ownership* ou coût total de possession) et de la valeur actuelle nette, ont été correctement évalués.

Question B.2.2

Rédiger, en argumentant, les éléments de réponse aux questions que Mme Farez se pose :

- a) Expliquer les éléments pris en compte dans le calcul du coût total de possession (TCO) et comment ce dernier va évoluer dans le temps.
- b) Justifier l'intérêt qu'a Savéol d'opter pour le renouvellement sur deux ans de la garantie au-delà des trois ans initialement prévus dans le contrat.
- c) Valider le montant de la valeur nette comptable du serveur au 31/12/2014 en détaillant les calculs pour l'obtenir.
- d) Indiquer si cette valeur nette comptable correspond à la réalité de la valeur du serveur.
- e) Indiquer l'intérêt ou les risques à continuer à utiliser le serveur au-delà de son cycle de vie estimé.

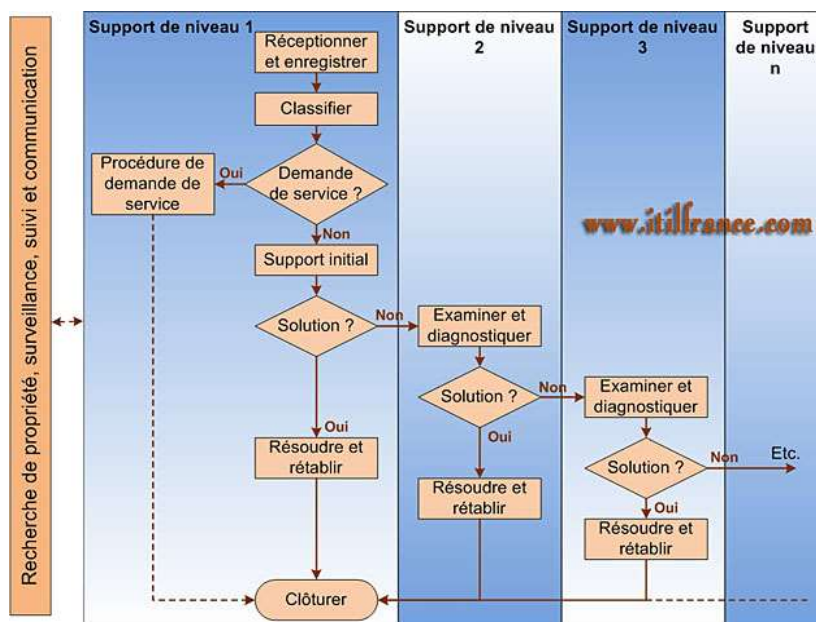
EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 7/18

DOCUMENTATION DES TECHNOLOGIES EN ŒUVRE CHEZ SAVEOL

Document T1 - Extrait de la gestion des incidents ITIL V2

ITIL (Information Technology Infrastructure Library) est une collection de documentation qui recense, synthétise et détaille les meilleures pratiques dans la fourniture de services informatiques.

Le schéma (classique) d'escalade d'un incident sur les différents niveaux de support, à commencer par le Centre de services, est le suivant :



La priorité d'un incident est déterminée par :

- **l'impact sur l'activité de l'entreprise** : l'impact représente la criticité sur l'activité métier (incident ou problème). Certaines définitions de la criticité (ou niveau de risque) précisent qu'il y a 3 facteurs : fréquence, gravité, probabilité de non-détection. L'impact est souvent mesuré au nombre de personnes ou de systèmes affectés.
 - **l'urgence à mettre en place une solution** définitive ou de contournement (urgence : effort attendu et vitesse nécessaire pour résoudre l'incident).
- Les incidents majeurs** sont ceux pour lesquels le degré d'impact sur l'ensemble des utilisateurs est extrême.

Document T2 - Le logiciel Puppet

Le logiciel *Puppet* offre la possibilité de centraliser la configuration système des machines au sein d'un référentiel unique puis de déployer cette configuration sur les machines autorisées.

Puppet fonctionne sur le principe de clients appelés **Nœuds**, installés sur les machines du parc et d'un service appelé **puppetMaster**, installé sur le serveur *srvpuppet*. Un agent, appelé **puppet agent**, est installé sur chaque machine nœud, soit en tant que service lancé au démarrage, soit en tant que logiciel exécutable par une commande manuelle ou dans une tâche planifiée. À intervalle régulier, l'agent se connecte au *puppetMaster* et vérifie la configuration actuelle du nœud par rapport à la configuration de référence définie sur le *puppetMaster* pour ce nœud. Si nécessaire l'agent modifie la configuration du nœud pour la rendre identique à celle définie sur le *puppetMaster*.

Puppet permet ainsi de s'assurer qu'à un instant t, toutes les machines clientes sont dans l'état de configuration désiré défini sur le serveur.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR		SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES	
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR
		Page : 8/18	

Document T3 - Protocoles de redondance HSRP, VRRP et GLBP

Source : Cisco Press - CCNP BCMSN Self Study

T3.1 Protocoles de redondance de routeurs : HSRP (Hot Standby Router Protocol) et VRRP (Virtual Router Redondancy Protocol)

HSRP est un protocole propriétaire de CISCO et VRRP est un protocole standard décrit par l'IETF dans la RFC 579.

En cas de panne de la passerelle par défaut nominale, HSRP ou VRRP bascule sur un routeur de secours pour assurer la continuité et ce, de façon transparente pour les utilisateurs finaux.

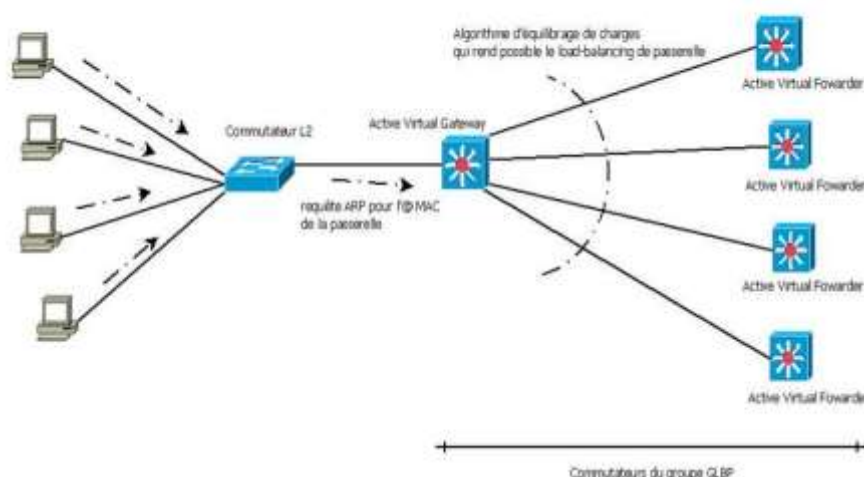
Pour cela, on place plusieurs routeurs au sein d'un même groupe logique auquel on assigne une adresse IP et une adresse MAC virtuelles uniques pour le groupe ; un des routeurs est désigné comme routeur actif (nominal), les autres sont dans un mode passif (Standby). En s'envoyant régulièrement des messages HSRP/VRRP (hello), les routeurs du groupe surveillent la présence effective et opérationnelle du routeur actif. S'ils ne reçoivent plus de message du routeur actif pendant un délai défini, le routeur passif du groupe ayant la priorité la plus élevée prend le statut de routeur actif.

Un routeur peut agir en mode *préemptif* : si le routeur R1 (actif) est tombé en panne et qu'un routeur R2 (passif) a pris le rôle actif, lors de son redémarrage, R1 reprendra automatiquement le rôle actif.

HSRP et VRRP ne gèrent pas nativement l'équilibrage de charge sur les passerelles par défaut.

T3.2 GLBP : Gateway Load Balancing Protocol

Implémentation de GLBP : Architecture logique



GLBP est un protocole propriétaire Cisco qui reprend les concepts de base de HSRP et VRRP en ajoutant un mécanisme de répartition de charge (*load-balancing*).

Contrairement à ces 2 protocoles, tous les routeurs du groupe GLBP définis participent activement. À l'intérieur du groupe GLBP, le routeur ayant la plus haute priorité ou la plus

haute adresse IP du groupe prendra le statut de "AVG" (*active virtual gateway*) ; ce routeur va intercepter toutes les requêtes ARP effectuées par les clients pour avoir l'adresse MAC de la passerelle par défaut et, grâce à l'algorithme d'équilibrage de charge préalablement configuré, il va renvoyer l'adresse MAC virtuelle d'un des routeurs du groupe GLBP.

C'est le routeur AVG qui va assigner les adresses MAC virtuelles aux routeurs du groupe. Ainsi ils ont le statut "AVF" (*active virtual forwarder*). Un maximum de 4 adresses MAC virtuelle est défini par groupe, les autres routeurs ayant des rôles de *backup* en cas de défaillance des AVF.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS		
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES			
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR		Page : 9/18

DOCUMENTATION COMMUNE AUX DEUX PARTIES

Document 1 : Système informatique de Savéol

L'efficacité du SI de Savéol repose sur le PGI (progiciel de gestion intégré) "Sage X3" qui pilote la quasi totalité des processus de gestion de la coopérative (les achats, la préparation des commandes, la gestion des stocks). Les activités contrôlées par le PGI, se répartissent sur plusieurs sites interconnectés au siège de Savéol par l'intermédiaire de liaisons privées de type MPLS (*multiprotocol label switching*) louées auprès d'un opérateur :

- le siège, qui héberge le cœur du site informatique et occupe les locaux de l'une des deux coopératives fondatrices "La presqu'île" sur la commune de Plougastel-Daoulas. Au total, 40 collaborateurs travaillent sur ce site, répartis au sein des services de la direction, commercial, administratif, conseil, R&D, agronomique et le service informatique ;
- deux stations de conditionnement, l'une située à 2 km du siège sur la même commune de Plougastel-Daoulas et l'autre distante de 20 km sur la commune de Guipavas ;
- un entrepôt de logistique localisé à Feillens près de Macon permet un stockage intermédiaire au plus près des clients de l'est de la France ;
- les deux coopératives adhérentes (Val Nantais et Mistral).

Parc matériel

Le parc informatique se compose principalement de :

- 10 serveurs physiques de type *cluster* Vmware mutualisant l'hébergement d'une quarantaine de serveurs virtuels ;
- 80 ordinateurs de type PC basés sur la distribution Linux Ubuntu.
- 70 imprimantes dont 50 pour éditer les étiquettes code à barres.

Au sein des unités de conditionnement, sont déployés une cinquantaine de terminaux de type *symbol Motorola MC900* connectés en Wifi permettant de scanner les étiquettes à code à barres et de saisir les données.

Organisation de connexions sortantes

- L'interconnexion des différents sites de la coopérative Savéol s'appuie principalement sur des liaisons privées de type MPLS louées à un opérateur. Le siège est connecté au réseau MPLS par une liaison principale SDSL à 4 Mbps secourue par un accès SDSL à 1 Mbps. Le basculement sur le routeur de secours se fait manuellement en cas de panne du routeur principal.
- Tous les autres sites disposent d'un lien principal au MPLS de l'opérateur le plus souvent de type SDSL et d'une liaison de secours en 3G ou ADSL.
- Les routeurs connectés au réseau internet sont configurés en routage statique. Les deux routeurs ont un débit identique de 2 Mbps.
- Les accès Internet pour les équipements de tous les sites sont contrôlés et sécurisés via le pare-feu Zykel.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 10/18

Document 2 - Extrait du plan d'adressage IP du siège

2.1 Plan d'adressage et VLAN du siège

Service	VLAN	Adresse sous-réseau
Bureaux	200	172.16.200.0/24
Infra&serveur	201	172.16.201.0/24
DMZ	254	172.16.254.0/24
Management	255	172.16.255.0/24
Internet	N/A	109.3.130.32/29
iSCSI	16	192.168.16.0/24
LAN MIRROR	N/A	10.0.10.0/24

2.2 Plan d'adressage des hôtes

Hôte	de	À
Serveurs	172.16.201.1	172.16.201.50
Éléments actifs	172.16.201.51	172.16.201.80
STA (Ordinateurs, PDA)	172.16.200.1	172.16.200.99
imprimantes	172.16.200.100	172.16.200.200

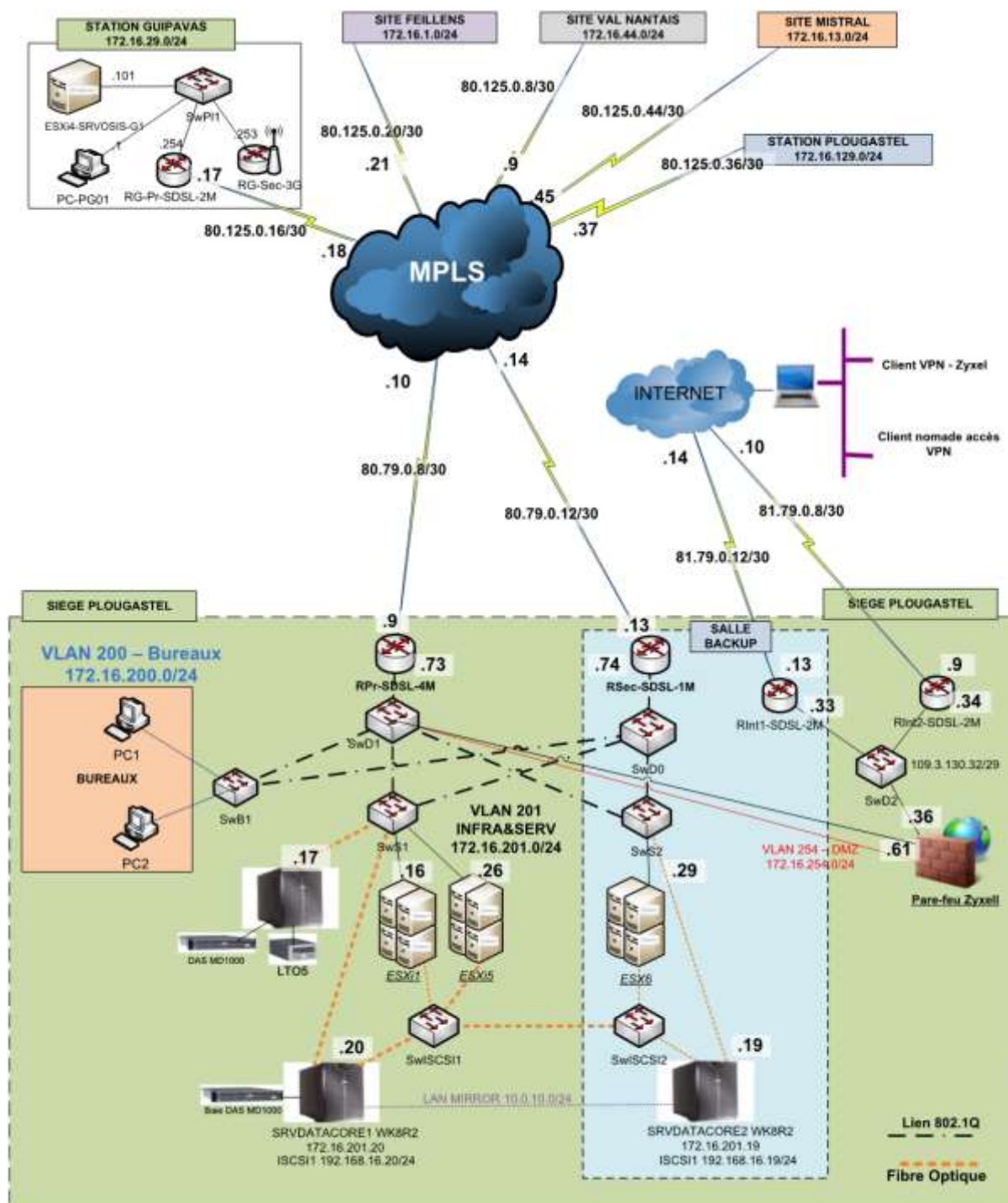
2.3 Extrait de la table d'adressage des équipements

Équipement	Interface	VLAN	Adresse IP	Masque sous-réseau	Passerelle par défaut
RPr-SDSL-4M	S0/0	N/D	80.79.0.9	255.255.255.252	N/D
	Fa0/1	Pas d'adresse IP			
	Fa0/1.200	200	172.16.200.73	255.255.255.0	N/D
	Fa0/1.201	201	172.16.201.73	255.255.255.0	172.16.201.61
RSec-SDSL-1M	S0/0	N/D	80.79.0.13	255.255.255.252	N/D
	Fa0/1	Pas d'adresse IP			
	Fa0/1.200	200	172.16.200.74	255.255.255.0	N/D
	Fa0/1.201	201	172.16.201.74	255.255.255.0	172.16.201.61
FW Zyxel	Giga0	254	172.16.254.61	255.255.255.0	N/D
	Giga1	201	172.16.201.61	255.255.255.0	N/D
	Fa0/0	1	109.3.130.36	255.255.255.248	109.3.130.33
ESXi1-VS5.0	Giga0	N/D	192.168.16.16	255.255.255.0	N/D
	Giga1	201	172.16.201.16	255.255.255.0	172.16.201.73
ESXi2-VS5.0	Giga0	N/D	192.168.16.26	255.255.255.0	N/D
	Giga1	201	172.16.201.26	255.255.255.0	172.16.201.73
PC1	eth0	200	172.16.200.1	255.255.255.0	172.16.200.73
PC2	eth0	200	172.16.200.2	255.255.255.0	172.16.200.73

N/D : non défini

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 11/18

Document 3 - Schéma de l'infrastructure Réseau & Système de SAVEOL



Notes :

- Les numéros ".xx" correspondent à la valeur du 4^{ème} octet sur le réseau correspondant. Ainsi, par exemple, le routeur de Guipavas RG-Pr-SDSL-2M possède les adresses 172.16.29.254 et 80.125.0.17.
- Pour des raisons de lisibilité, l'ensemble du réseau DMZ n'est pas représenté sur ce schéma.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 12/18

DOCUMENTATION POUR LA PARTIE A

Document A1 - Éléments d'information sur le nouveau serveur *proxy-cache*

Le serveur *proxy-cache* a pour adresse **172.16.201.41** et écoute sur le port **3142**.

Pour configurer le client, un nouveau fichier, que l'on nommera "*01proxy*", sera à créer dans son dossier */etc/apt/apt.conf.d/*. Il contiendra la ligne suivante :

```
Acquire::http::Proxy "http://<adresse IP serveur>:<n°Port>";
```

Document A2 - Configuration client/serveur de Puppet

Pour homogénéiser et faciliter la maintenance de son parc, Savéol utilise le logiciel *Puppet*.

L'agent *Puppet* sur un nœud client est configuré via le fichier */etc/puppet/puppet.conf*. La machine hôte qui héberge le service *puppetMaster* s'appelle *srvpuppet*.

La communication est authentifiée par un certificat serveur et un certificat client. Les échanges sont sécurisés par les mécanismes SSL/TLS.

Document A3 - Utiliser *Puppet* pour configurer les serveurs NTP

Toute la configuration (référentiel) de *Puppet* est centralisée dans l'arborescence */etc/puppet* du serveur. C'est dans ce répertoire que sont définis le site (réseau), les nœuds (machines) et les modules (actions de configuration) à appliquer lors de la mise en configuration.

Voici une rapide description des fichiers contenus dans ce répertoire :

- */etc/puppet/manifests/site.pp* : définit le premier fichier analysé par *puppetMaster* pour définir son référentiel.
- */etc/puppet/manifests/node.pp* : définit chaque nœud (ou ensemble de nœuds via des méta-caractères) et lui associe les configurations.
- */etc/puppet/manifests/modules.pp* : liste les modules présents sur le serveur *Puppet*.
- */etc/puppet/modules/<module>* : représente le sous répertoire contenant la définition du module *<module>* (action de configuration). À savoir :
 - *<module>/manifests/init.pp* : fichier qui contient la définition du module c'est à dire qui précise les actions que l'on doit faire sur la machine cliente ;
 - *<module>/files/* : répertoire qui contient l'ensemble des fichiers nécessaires à l'exécution de ce module, notamment les fichiers de configuration à copier sur les nœuds clients.

Exemple du service NTP :

NTP (*Network Time Protocol* ou *Protocole d'Heure Réseau*) est un protocole qui permet de synchroniser l'horloge locale d'ordinateurs sur l'horloge d'un serveur de référence.

Définition des modules référencés dans *Puppet*

Le fichier *ntp.conf* contient la configuration du service NTP qui devra être copiée sur le serveur NTP quand il se synchronisera avec le serveur *Puppet*.

Le fichier */etc/puppet/manifests/modules.pp* contiendra notamment la ligne suivante :

```
/etc/puppet/manifests/modules.pp
```

```
1 import 'ntp'
```

Arborescence :

```
# tree /etc/puppet
/etc/puppet
├── auth.conf
├── files
├── fileservers.conf
├── manifests
│   ├── modules.pp
│   ├── node.pp
│   └── site.pp
├── modules
│   └── ntp
│       ├── files
│       │   ├── ntp.conf
│       │   └── manifests
│       │       └── init.pp
```

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS		
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES			
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR		Page : 13/18

Définition des nœuds (machines clientes *Puppet*)

Définition du nœud nommé 'optiplex790' auquel on applique le module NTP dans le fichier */etc/puppet/manifests/node.pp* en y ajoutant les lignes 1 à 3 :

<i>/etc/puppet/manifests/node.pp</i>	
1	node 'optiplex790.saveol.com' {
2	include ntp
3	}
4	node 'SRVNAGIOS.saveol.com' {
5	include nagios
6	}
7	node '[a-zA-Z]*.saveol.com' {
8	include imprim
9	}

Le client 'Optiplex790.saveol.com' recevra ainsi la configuration prévue pour NTP, le client SRVNAGIOS recevra la configuration Nagios et toutes les machines du domaine recevront la configuration d'impression appelée imprim.

Définition des modules

Définition de l'action de configuration NTP dans le fichier */etc/puppet/modules/ntp/manifests/init.pp* avec le contenu suivant :

<i>/etc/puppet/modules/ntp/manifests/init.pp</i>	
1	class ntp {
2	file { ["/etc/ntp.conf":
3	owner => root,
4	group => root,
5	mode => 644,
6	source => "puppet:///ntp/ntp.conf"
7	}
8	}

Lors de la synchronisation entre le client 'Optiplex790' et le service *puppetMaster*, le module **NTP** va donc vérifier l'existence sur la machine cliente d'un fichier */etc/ntp.conf* :

- appartenant à l'utilisateur **root** ;
- appartenant au groupe **root** ;
- avec les droits **644** ;
- et dont le contenu doit être égal au fichier */etc/puppet/modules/ntp/files/ntp.conf* disponible sur le serveur *Puppet*.

Document A4 - Extrait de la fiche d'incident / relevé des tests

1. Après avoir pris le contrôle à distance du poste PC-G01 d'adresse IP 172.16.29.1 d'un employé de la station de Guipavas ayant signalé des difficultés, les deux tests d'accessibilité exécutés depuis ce poste ont donné les résultats suivants :

A] PC-G01>ping 172.16.201.16 [Esxi1]

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

B] PC-G01>ping 172.16.201.73 [Routeur siege RPr-SDSL-4M]

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 14/18

2. Les commandes exécutées depuis le routeur principal du siège ont donné les résultats suivants :

RPr-SDSL-4M#ping 172.16.29.1 [Poste PC-G01]

.!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 3/6/15 ms

RPr-SDSL-4M #traceroute 172.16.29.1[Poste PC-G01]

```

1  172.16.201.74    2 msec  0 msec  0 msec
2  80.79.0.14       4 msec  2 msec  2 msec
3  80.125.0.17      2 msec  2 msec  2 msec
4  172.16.29.1      0 msec  3 msec  10 msec

```

Document A5 - Extrait des tables de routage

Les tables de routage des routeurs du siège et de celui de Guipavas ont été relevées suite au signalement du ralentissement.

Routeur siège RPr-SDSL-4M

Destination	Passerelle	Interface
80.79.0.8/30	directly connected	Serial0/0
80.79.0.12/30	172.16.201.74	FastEthernet0/1.201
172.16.1.0/19	172.16.201.74	FastEthernet0/1.201
172.16.29.0/24	172.16.201.74	FastEthernet0/1.201
172.16.200.0/24	directly connected	FastEthernet0/1.200
172.16.201.0/24	directly connected	FastEthernet0/1.201
0.0.0.0/0	172.16.201.61	FastEthernet0/1.201

Routeur siège RSec-SDSL-1M

Destination	Passerelle	Interface
80.79.0.8/30	80.79.0.14	Serial0/1
80.79.0.12/30	directly connected	Serial0/1
172.16.1.0/24	80.79.0.14	Serial0/1
172.16.29.0/24	80.79.0.14	Serial0/1
172.16.200.0/24	directly connected	FastEthernet0/1.200
172.16.201.0/24	directly connected	FastEthernet0/1.201
0.0.0.0/0	172.16.201.61	FastEthernet0/1.201

Routeur Guipavas RG-Pr-SDSL-2M

Destination	Passerelle	Interface
80.125.0.16/30	directly connected	Serial0/0/0
172.16.1.0/24	80.125.0.18	Serial0/0/0
172.16.29.0/24	directly connected	FastEthernet0/1
172.16.200.0/24	80.125.0.18	Serial0/0/0
172.16.201.0/24	80.125.0.18	Serial0/0/0
0.0.0.0/0	80.125.0.18	Serial0/0/0

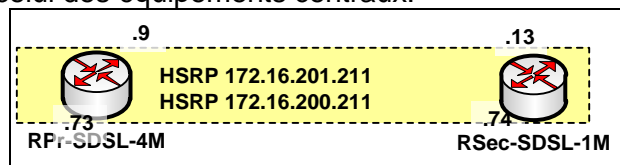
EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 15/18

DOSSIER DOCUMENTAIRE POUR LA PARTIE B

Document B1 - Implémentation HSRP sur les routeurs

B1.1 Objectifs à atteindre

L'équipe informatique a implémenté HSRP comme protocole de tolérance aux pannes sur les routeurs d'accès MPLS. La situation visée permettra au système de proposer comme passerelle une adresse virtuelle 172.16.200.211 pour le VLAN des bureaux et 172.16.201.211 pour celui des équipements centraux.



Cette adresse virtuelle devra diriger les postes et serveurs vers le routeur MPLS principal, le secondaire prenant le relais en cas de défaillance du principal.

B1.2 Paramétrage de test

La chronologie des principales étapes réalisées par l'administrateur lors de la configuration du groupe HSRP pour le VLAN 200 (VLAN « Bureaux ») est décrite ci-dessous :

1. Configurer HSRP sur les 2 routeurs :

RPr-SDSL-4M

```
(config)#interface Fa0/1.200          #sous-interface 200 sur l'interface Fa0/1
(config-if)#standby 1 ip 172.16.200.211 #crée l'adresse virtuelle HSRP
(config-if)#standby 1 priority 150      #définit la priorité de l'interface
(config-if)#standby 1 preempt          #le routeur agit en préemptif
```

RSec-SDSL-1M

```
(config)#Interface Fa0/1.200
(config-if)#standby 1 ip 172.16.200.211
(config-if)#standby 1 priority 100
```

2. Activer le "débogage" des paquets ICMP sur les deux routeurs

```
#debug ipicmp
ICMP packet debugging is on
```

3. Exécuter la commande ping 172.16.200.211 depuis le poste PC1 du VLAN « Bureaux »

```
>ping 172.16.200.211
Reply from 172.16.200.211: bytes=32 time=0ms TTL=255
...
```

4. Lecture des messages de log suivants sur les routeurs

RSec-SDSL-1M	RPr-SDSL-4M
Pas de message	ICMP: echo reply sent, src 172.16.200.211, dst 172.16.200.101 ICMP: echo reply sent, src 172.16.200.211, dst 172.16.200.101

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 16/18

5. Éditer sur les routeurs les informations HSRP. On obtient les résultats ci-dessous :

RSec-SDSL-1M	RPr-SDSL-4M
FastEthernet0/1.200 - Group 1 (version 2) State is Standby Virtual IP address is 172.16.200.211 Local virtual MAC address is 0000.0C9F.0F01 Preemption disabled Active router is 172.16.200.73, priority 100 Standby router is local Priority 100 (default 100)	FastEthernet0/1.200 - Group 1 (version 2) State is Active Virtual IP address is 172.16.200.211 Local virtual MAC address is 0000.0C9F.0F01 Preemption enabled Active router is local Standby router is 172.16.200.74, priority 150 Priority 150 (configured 150)

Document B2 - Compte rendu de la réunion VPN du 4 mai 2015

Participants : M. Netralli, Mme Farez, 2 techniciens réseau et le candidat

Objet : Cadrage de la solution VPN spécifique au service

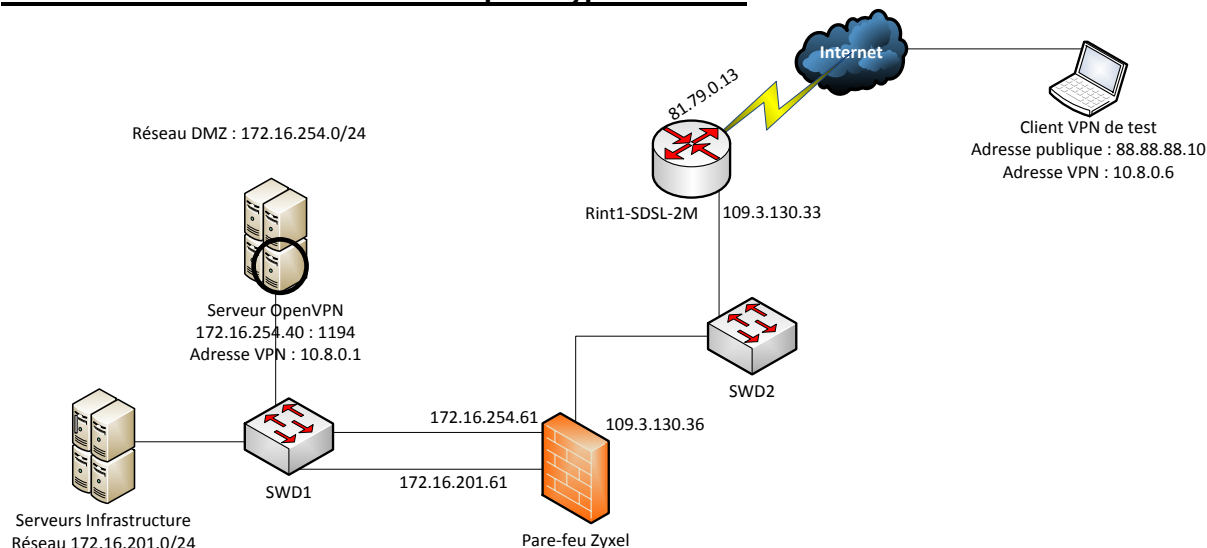
Le serveur VPN sera un serveur *OpenVPN* basé sur une distribution Linux Debian 7.2. Il gèrera sa propre autorité de certification ainsi que le certificat de l'autorité de certification. Il disposera ainsi d'un certificat.

Les clients VPN seront installés sur des machines *Lubuntu* et chacune disposera d'un certificat client spécifique.

Le serveur sera placé dans la DMZ et aura pour adresse IP 172.16.254.40 : on conservera le port par défaut 1194. Il sera accessible via l'adresse publique du pare-feu Zykel 109.3.130.36.

Les clients VPN recevront une adresse sur le réseau par défaut 10.8.0.0/24 et auront accès au réseau 172.16.201.0/24.

Schéma indicatif de la solution du prototype à valider



Le serveur physique sur lequel il est prévu d'implanter la machine virtuelle accueillant le serveur VPN est un Dell PowerEdgeT420. Il a nécessité 2 interventions en 2012 occasionnant 2 légères interruptions de services. En 2013, une mise à niveau de la mémoire vive et de la capacité de stockage a été nécessaire. La même année, Mme Farez a bénéficié d'une formation interne de 2 jours.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 17/18

Les éléments financiers du serveur physique sont issus du logiciel de gestion de parc :

Valeur d'achat : 4 200 € (y compris 500 € de garantie) Date d'achat : 15/10/2012 Durée de la garantie (pièces et main d'œuvre) : 3 ans (renouvelable 2 ans pour 1 200 €)	Mode d'amortissement* : linéaire Date de mise en service : 01/11/2012 TCO (<i>total cost of ownership</i> ou coût total de possession) : 6 830 € Valeur nette comptable au 31/12/2014 : 2 380 € Valeur résiduelle : 0 €
--	--

**L'amortissement est la répartition du montant d'un actif amortissable selon le rythme de consommation des avantages économiques attendus en fonction de son utilisation probable.*

Savéol renouvelle les postes de travail tous les 4 ans et les serveurs tous les 5 ans. Sensibilisée par les problématiques de développement durable et de fracture numérique, elle a pour politique de reconditionner et de donner aux associations, aux établissements scolaires ou bien aux espaces publics numériques (EPN), le matériel informatique à la fin de leur cycle de vie.

EXAMEN : BREVET DE TECHNICIEN SUPERIEUR			SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2015	SUJET	ÉPREUVE : E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES		
Durée : 4h	Coefficient : 5		Code sujet : SI5SISR	Page : 18/18