E5SR : PRODUCTION ET FOURNITURE DE SERVICES

CAS SAVEOL
Proposition de corrigé

Barème

Partie A	***Fourniture de services***	*48 points*
Partie B	***Production de services***	*52 points*
	Total	100 points

Partie A : Fourniture de services

Mission A.1 – Configuration client/serveur de Puppet

Question A.1.1 : Citer au moins deux arguments qui justifient l'utilisation du service *Puppet* pour réaliser le paramétrage des postes.

1. Éviter les tâches répétitives : on ne réalise le travail de configuration qu'une seule fois.
2. Déployer automatiquement et rapidement des machines.
3. Permettre une configuration homogène de parc ce qui réduit les risques d'erreurs et simplifie la maintenance.
4. S'assurer que les machines conservent leur configuration.
5. Constituer une base de référence (centralisée) sur les configurations modèles des postes.

Question A.1.2 :

a) Lister les risques auxquels s'exposerait Savéol si les échanges entre les nœuds clients et le serveur *puppetMaster* n'étaient pas sécurisés.

- Connexion d'un client non autorisé et possibilité de récupérer les fichiers de configuration du serveur.
- Serveur pirate non authentifié envoyant des configurations erronées ou corrompues au client.
- Écoute sur le réseau et vol des fichiers de configuration.

b) Expliquer les principes mis en œuvre pour sécuriser les échanges entre les nœuds clients et le service *puppetMaster*.

Les échanges entre les clients et le serveur *Puppet* s'appuient sur le protocole SSL/TLS associé à des certificats. Dans le cas de *Puppet*, l'authentification est réalisée par un certificat client **et** un certificat serveur. Ces mécanismes sécurisent les échanges en garantissant:

- l'authentification des homologues (client et serveur) par les *(échanges de)* certificats ;
- la confidentialité des données par chiffrement *(clé publique ou clé de session)*;
- l'intégrité des données (par fonction de hachage et signature) *(clé privée)*.

Question A.1.3
Lister les étapes nécessaires à la mise en œuvre de ce nouveau module

a) Créer le nouveau fichier de configuration *01proxy* afin qu'il prenne en compte le nouveau serveur Proxy.
Acquire::http::Proxy "http://172.16.201.41:3142";

b) Créer l'arborescence sur le serveur pour le module *clientProxy* (création des dossiers *clientProxy*, puis *files* et *manifests)*.

c) Copier le fichier *01proxy* à déployer dans le dossier *files*

d) Définir le nouveau module à référencer dans */etc/puppet/manifests/modules.pp*

e) Compléter le fichier */etc/puppet/manifests/node.pp* afin de permettre à tous les nœuds clients du domaine de mettre à jour leur configuration *Proxy* ou à un nœud créé spécifiquement pour les clients Lubuntu.

```
node '[a-zA-Z]*.saveol.com' {
    include clientProxy
}
```

f) Écrire le *fichier/etc/puppet/manifests/modules/clientProxy/manifests/init.pp* nécessaire à *Puppet* pour déployer *01proxy* sur les clients *Lubuntu* du domaine.

```
class clientProxy {
  file { "/etc/apt/apt.conf.d/01proxy":
  owner => root,
  group => root,
 mode => 644,
 source => "puppet:///clientProxy/01proxy"
 }
}
```

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

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 quel protocole de routage dynamique vous semble adapté à la situation vécue ici ? Justifier votre réponse.

a) Comparer la criticité de cet incident avec celle de la panne « blackout » subie précédemment par le réseau MPLS. Justifier votre réponse.

	blackout	**Ralentissement - latence**
Qualification	Bloquant sur l'activité de l'ensemble des sites distants -> Critique	Perturbant sur l'activité des utilisateurs (parfois, pour certains utilisateurs) mais pas critique (l'activité continue, *éventuellement en mode dégradé*).

b) Indiquer à quel niveau de la gestion des incidents ITIL cet incident sera pris en charge. Justifier.

Le support de niveau 1 n'est certainement pas en capacité de résoudre l'incident puisque ce dernier demande un diagnostic poussé (cause de l'incident non évidente) et ne fait donc pas l'objet d'une procédure de résolution pré-établie. De plus, l'intervention éventuelle ne se fera pas sur les postes clients qui ne sont pas en cause. Le technicien prenant en charge l'incident doit donc le faire remonter au deuxième niveau. La connaissance et l'expertise du personnel de ce niveau permettra ou non le diagnostic et sa résolution ; selon le cas, l'incident sera remonté au niveau 3.

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)

Tests 1 et 2 :

Les commandes ping se déroulent correctement même si on constate des pertes, par conséquent, on peut en déduire que les équipements sont opérationnels ainsi que le routage. Ces résultats ne permettent pas d'identifier la cause du problème.

Test 3 :

La ligne 1 de la commande traceroute permet de constater que les paquets IP sont dirigés vers la passerelle 172.16.201.74 qui est l'adresse interne du routeur de secours.

- *La bande passante de la liaison SDSL du routeur de secours est de 1Mbps soit une capacité 4 fois moindre que la liaison SDSL principale à 4Mbps. Ce qui représente un goulot et peut expliquer que lors des périodes de fortes demandes des lenteurs puissent être constatées.*
- *Le candidat pourra de manière moins pertinente relever qu'on ajoute un intermédiaire (saut) supplémentaire dans l'acheminement*

Document A4 :

*La table du routeur **RPr-SDSL-4M** possède une route vers le réseau 172.16.29.0 du site de Guipavas*

172.16.29.0/24	*172.16.201.74*	*FastEthernet0/1.201*

- *Cette route transfère les paquets destinés au réseau 172.16.29.0 par la sous interface Fa0/1.201 par l'intermédiaire de l'adresse de passerelle 172.16.201.74 qui correspond à l'interface Fa0/1 du routeur RSec-SDSL-1M.*
- *Ce qui signifie que les paquets à destination des hôtes du 172.16.29.0 transitent par le routeur de secours au lieu d'être acheminés directement sur le réseau MPLS.*

Raisons possibles des lenteurs

- La route vers Guipavas passe par le routeur de secours.
- Le débit du routeur de secours est inférieur à celui du routeur principal.
- Un saut supplémentaire.

Cause possible du dysfonctionnement

Le fichier de configuration du routeur RPr-SDSL-4M sauvegardé ne correspondait pas à celui qui était en exploitation et lors du redémarrage suite au blackout c'est cette configuration erronée qui s'est exécutée ou alors il s'agit d'une erreur de manipulation lors de la panne.

d) Solution pour résoudre à chaud le problème

Corriger l'erreur dans la configuration courante des routeurs en corrigeant les routes du routeur RPr-SDSL-4M vers les sites distants pour que l'on sorte directement par la connexion MPLS (*interface serial0/0 et passerelle 80.79.0.10*).

e) Expliquer en quoi un protocole de routage dynamique éviterait ce problème à l'avenir

Pour éviter la survenue d'un tel problème un protocole de routage dynamique permettra une réactualisation correcte des routes sans intervention manuelle *après une période de convergence*.

f) Indiquer quel protocole de routage dynamique vous semble adapté à la situation vécue ici. Justifier votre réponse.

- Il faut que le protocole proposé prenne en compte les débits entre les différents routeurs, ce qui exclut le protocole RIP qui travaille uniquement sur le nombre de sauts.
- On s'oriente vers OSPF ou EIGRP (matériel Cisco) ou, plus généralement, un protocole à état de liens.

Partie B : PRODUCTION DE SERVICES

Mission B.1 – Tolérance aux pannes des accès distants

Question B.1.1

a) Justifier l'utilité d'un dispositif de tolérance aux pannes sur chacune des connexions (MPLS et internet).

b) Définir les termes de continuité de service et d'équilibrage de charge et comparer les protocoles HSRP et GLBP sur ces deux critères.

c) 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.

a) Utilité d'un dispositif de tolérance aux pannes

La réponse doit faire apparaître l'intérêt de l'automaticité de la bascule entre les dispositifs pour garantir la disponibilité (continuité de service acceptée).

Chacune des connexions est utilisée par l'ensemble des utilisateurs de Savéol, pour des usages professionnels en lien direct avec l'activité de l'entreprise.
Une panne d'une des connexions empêcherait une partie importante de l'activité et aurait un impact important en termes économiques.

La connexion MPLS permet aux sites distants d'accéder aux ressources internes au siège (serveurs, applications, messagerie) ainsi qu'à la sortie internet. Elle est le cœur des échanges entre les entités de l'entreprise.

La connexion internet, outre les fonctions habituelles (messagerie, accès Web et mises à jours diverses de logiciels et système d'exploitation) est aussi utilisée pour les acteurs nomades vie la VPN (et prochainement pour l'administration distante).

b) Comparaison en termes de continuité de service et de répartition de charge

Définitions

- **Continuité de service :** capacité à une interruption minimale ressentie par les utilisateurs.
- **Répartition de charge :** technique pour distribuer le travail entre différents équipements d'un groupe de façon transparente pour l'utilisateur.

Il existe deux modes principaux de basculement (fail over) :

- *actif/actif qui s'apparente plus à de l'équilibrage de charge (load-balancing);*
- *actif/passif (mode classique couramment répandu) où l'équipement secondaire (passif) est en mode veille tant que l'équipement primaire (actif) ne rencontre aucun problème.*

Les deux modes reposent sur un principe de tolérance aux pannes basé sur de la redondance par ajout d'équipements supplémentaires pour assurer une meilleure disponibilité d'un service.

Le mode actif/passif

- *Dans le secours passif, L'équipement actif prend l'ensemble de la charge tandis que l'équipement passif placé en réserve (en secours, en « spare ») écoute l'état de*

l'équipement actif en vue d'une potentielle reprise d'activité si une défaillance survient.

- ***Avantage :*** *peu de dégradation du service en cas de panne, si l'équipement de secours est de performance comparable au nominal.*
- ***Inconvénient :*** *légère interruption de service le temps de la détection de la panne et de mise en service de l'équipement de secours. Capacité d'un équipement sous utilisé.*

Le mode actif/actif

- *Dans un principe de secours actif, le composant de secours est déjà opérationnel avant d'être requis. Il est en surnombre, mais assure malgré tout une part de la fonction. Le secours actif est associé aussi à un dispositif de passage en mode secours transparent ou automatisé. On parle d'un secours « à chaud ». Les disques RAID, typiquement, fonctionnent selon un principe de secours actif.*
- ***Avantage :*** *interruption de service quasi inexistante en cas de panne et permet detirer parti du surplus de matériel pour disposer d'une meilleure qualité de service même en l'absence de secours.*
- ***Inconvénient*** *: risque de dégradation des performances si l'estimation des besoins est mal estimée.*

Dans un groupe HSRP/VRRP, il n'y a pas de notion de partage de la charge, c'est le routeur maître qui assure exclusivement la transmission des paquets pour le routeur virtuel.

- *S'il y a un nombre d'hôtes suffisant, il est toutefois possible de définir plusieurs groupes HSRP/VRRP sur chacun des routeurs, et de configurer autant de groupes d'hôtes qui auront chacun une passerelle par défaut différente.*

GLBP *est un protocole propriétaire Cisco qui permet de faire de la redondance ainsi* que de la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle, *mais plusieurs adresses MAC virtuelles*.

- *Le protocole GLBP élit un Active Virtual Gateway (AVG) qui va répondre aux requêtes ARP pour l'adresse IP virtuelle. GLBP permet de donner un poids variable à chacun des routeurs participants pour la répartition de la charge entre ces routeurs. La charge est donc répartie par hôte dans le sous-réseau.*

c) Justifier le choix des mécanismes de tolérance aux pannes :

Accès MPLS :

- En mode de fontionnement normal, tous les paquets doivent passer par le routeur principal et n'emprunter la liaison vers le routeur de secours qu'en cas d'interruption de service de l'accès vers le routeur nominal car le routeur de secours a un débit 4 fois moins important que le principal ; les deux ne peuvent jouer un rôle équivalent.
- Sur certains sites distants, le routeur de secours est un routeur 3G qu'on ne souhaite pas utiliser en permanence (coût).
- Le protocole HSRP est par conséquent le mieux adapté pour cette passerelle.

Accès Internet :

- L'accès Internet est constitué de deux liaisions SDSL de caractéristiques identiques à 2Mbps que l'on peut utiliser simultanément. La répartition de charge permettra de ne pas créer un goulet d'étranglement en n'utilisant qu'une des deux sorties, de ne pas dépenser pour une liaison non utilisée, et permettra de délivrer le même débit sur le lien internet et le lien MPLS.
- Tout cela justifie l'emploi du protocole GLBP.

Question B.1.2

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

a) Relever les indications vous permettant d'affirmer que le système est correctement paramétré pour le VLAN « bureaux ».

b) Indiquer les paramétrages nécessaires pour rendre la solution opérationnelle sur l'autre VLAN.

a) Relevé des indications

On doit s'assurer que le routeur qui possède l'adresse virtuelle est bien le routeur principal :

- on voit que le routeur principal est passé en mode actif et l'autre en *standby* (document B.1.2/5) ;
- les *logs* indiquent bien que c'est le routeur RPr-SDSL-4M qui a répondu à la requête *ping* (document B.1.2/4) ;
- les informations HSRP relevées signalent que le routeur RPr-SDSL-4M a bien la priorité la plus importante, document B.1.2/5.

b) Modifications pour l'autre VLAN

Il faut procéder aux paramétrages équivalents sur l'interface virtuelle Fa0/201 de manière à activer le protocole pour le VLAN « Infra et serveurs » :

- créer un groupe HSRP pour le VLAN 201 ;
- activer l'adresse virtuelle 172.16.201.211 sur les deux équipements ;
- définir la priorité la plus importante sur le routeur RPr-SDSL-4M ;
- pour optimiser le fonctionnement, on pensera à définir le routeur RPr-SDSL-4M en mode préemptif.

Configurer HSRP sur les 2 routeurs : (ne pas pénaliser le numéro de groupe [ici 2])

RPr-SDSL-4M

```
(config)#interface Fa0/1.201                 #sous-interface 201 sur l'interface Fa0/1
(config-if)#standby 2 ip 172.16.201.211      #crée l'adresse virtuelle HSRP
(config-if)#standby 2 priority 150           #définit la priorité de l'interface
(config-if)#standby 2 preempt                #le routeur agit en préemptif
```

RSec-SDSL-1M

```
(config)#Interface Fa0/1.201
(config-if)#standby 2 ip 172.16.201.211
(config-if)#standby 2 priority 100
```

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

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

a) Installations sur le poste de test

On installera (ou on copiera) sur le poste de test (puis ensuite sur chaque poste) le client compatible avec OpenVPN, son certificat client et le certificat de l'autorité de certification (AC) ou une référence à un fichier de configuration.
Le client permet d'établir la connexion. Le certificat de l'AC est nécessaire à l'établissement de la connexion pour valider le certificat serveur sans intervention. Le certificat du client permet de s'authentifier.

b) Paramétrages du pare-feu

Il faudra

- mettre en place une redirection des paquets à destination de ce port sur l'interface 109.3.130.36 vers le serveur (ce qui implique d'ouvrir le port 1194, mais qui est généralement fait automatiquement) ;
- *ajouter la route 10.8.0.0 vers le serveur OpenVPN ;*
- *prévoir des règles de filtrage autorisant les communications entre le réseau 10.8.0.0 et le réseau 172.16.201.0.*

c) Informations contenue dans un paquet

Les adresses IP visibles sont celles des extrémités publiques du tunnel VPN (pour le poste : 88.88.88.10 et pour le Pare-feu : 109.3.130.36).
Le port serveur (ou port destination) sera celui par défaut (1194), le port client (ou port source) étant une valeur dynamique.

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 un TCO et comment ce dernier va évoluer dans le temps.

b) Justifier de l'intérêt de Savéol à 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 au 31/12/2014 en détaillant les calculs pour l'obtenir.

d) Dire si cette dernière valeur correspond à la réalité.

e) Indiquer l'intérêt ou les risques à continuer à utiliser le serveur au-delà de son cycle de vie estimé

a) Le TCO

Le TCO est un indicateur qui permet de calculer le coût global d'un bien (solution informatique par exemple) dans le temps c'est à dire son coût cumulé tout au long de son cycle de vie.

- Il est supérieur au coût d'acquisition car il est nécessaire d'ajouter à ce dernier des coûts indirects (maintenance, formation, évolution...), des coûts différés c'est-à-dire des coûts liés à l'utilisation, des coûts récurrents et des coûts cachés, comme par exemple, le coût des arrêts et des défaillances : le serveur « a nécessité 2 interventions en 2012 occasionnant 2 légères interruptions de services, une formation interne de 2 jours pour Mme Farez ainsi qu'une mise à niveau de la mémoire vive et de la capacité de stockage en 2013 ».
- Il augmentera encore jusqu'à la fin de son cycle de vie. Les frais de gestion sont même en règle générale plus importants en fin de vie (serveur vieillissant) qu'au début du cycle.

b) Intérêt du renouvellement sur 2 ans de la garantie

Savéol a intérêt à opter pour le renouvellement de la garantie car les coûts indirects et cachés sont moindres si le matériel est garanti. Savéol a des risques réels d'avoir plus de 1 200 € de remplacement de pièces et de main d'œuvre ; l'entreprise réduira ainsi le TCO sur ce serveur.

c) Le montant de la valeur nette comptable au 31/12/2014

La valeur nette comptable en fin d'exercice est égale à la valeur d'origine de l'actif (augmentée de la valeur résiduelle égale à zéro dans notre cas car l'entreprise ne revend pas ses actifs informatiques) diminuée par le cumul des amortissements. Les amortissements sont calculés ici de manière linéaire en fonction du cycle de vie du serveur (5 ans - taux d'amortissement annuel = 1/5 = 0,2) à compter de sa date de mise en service.

L'amortissement pour une année complète est donc de 4 200 * 0,2 = 840

Amortissement en 2012 (sur 2 mois) : 840 * 2/12 = 840 / 6 = 140
Amortissement en 2013 : 840
Amortissement en 2014 : 840
Soit un amortissement cumulé de 1 820.

Valeur actuelle nette = 4 200 + 0 - *1 820* = *2 380* €.

d) Valeur actuelle nette et réalité

La valeur actuelle nette d'un actif à une date donnée ***est une valeur théorique qui tente de refléter le mieux possible la réalité compte tenu du mode d'amortissement choisi****. En effet, l'amortissement valorise l'utilisation qui est faite d'un bien (« 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 »). Il est programmé d'utiliser cet actif de manière continue pendant 5 ans, le mode d'amortissement sur la durée d'utilisation est donc dans le cas d'un serveur le plus approprié.*

Mais en ce qui concerne le matériel informatique, l'effet des évolutions technologiques et économiques est très fort les premières années.

Ainsi, au cours du cycle de vie, il se peut donc que cette valeur soit supérieure à la valeur vénale ou valeur d'usage du serveur. C'est bien le cas ici.

e) Intérêt ou risques à continuer à utiliser son serveur au-delà du cycle de vie estimé

Utiliser son serveur au-delà du cycle de vie augmente le risque de panne, d'interruption de service et de baisse de performance. L'économie attendue risque finalement de coûter cher.

Mais selon le cas, il est toujours possible d'utiliser les anciens serveurs sur des services moins exigeants.