E4R : ÉTUDE DE CAS

Durée : 5 heures **Coefficient : 5**

CAS CG96

Ce sujet comporte 16 pages dont 6 pages d'annexes.
Il est constitué de 5 dossiers qui peuvent être traités de façon indépendante.
Le candidat est invité à vérifier qu'il est en possession d'un sujet complet.

Matériels et documents autorisés :

- Lexique SQL sans commentaire ni exemple d'utilisation des instructions.
- Règle à dessiner les symboles informatiques.

Aucune calculatrice n'est autorisée

Liste des annexes

Barème

Dossier 1 : Évolution du réseau	35	points
Dossier 2 : Gestion du DNS et de l'accès à Internet	20	points
Dossier 3 : Protection des accès extérieurs	15	points
Dossier 4 : Gestion des incidents	15	points
Dossier 5 : Numérisation des documents	15	points
Total	100	points

Présentation du contexte

Le Conseil général de Seine-et-Orne (96)[1], rassemble 43 élus. Il siège dans l'Hôtel du Département, à Balbe. Les lois de décentralisation de 1982 lui ont octroyé de nombreuses compétences obligatoires (solidarité, collèges, transports...) qui ont été progressivement élargies et diversifiées.

Le Conseil emploie environ 1 500 personnes dont 19 au service informatique basé à la cité administrative.

L'infrastructure réseau se compose principalement d'une vingtaine de serveurs et environ d'un millier de postes de travail répartis sur plusieurs sites.

Le réseau dispose

- d'une zone démilitarisée (DMZ) publique comportant :
    - un serveur DNS maître pour la zone cg96.fr, le serveur secondaire (esclave) étant hébergé par le fournisseur d'accès ;
    - un serveur relais de messagerie/anti-virus de messagerie ;
    - un serveur *web* public (www.cg96.fr).
- d'un réseau privé où sont situés :
    - des serveurs d'infrastructure (DNS, DHCP, WWW, messagerie SMTP et POP3, annuaires d'authentification, serveurs de fichiers et d'impression, SGBD) ;
    - des serveurs applicatifs ;
    - les postes de travail.

L'organisation logique TCP/IP est basée sur le domaine internet **cg96.fr**. L'adressage est effectué par des serveurs DHCP.

[1] Ce conseil général est bien sûr fictif.

Dossier 1 : Évolution du réseau

Annexes à utiliser : 1 et 2

Suite à une réorganisation, le Conseil général disposera de nouveaux locaux situés à 600 m de la cité administrative. L'administratrice du réseau, Mme Simonet, hésite entre deux solutions pour relier le nouveau site au site principal. La première consiste à utiliser une liaison louée de 2 Mbit/s, la seconde consiste à utiliser un tunnel VPN sur Internet au moyen d'une liaison ADSL à 8 Mbit/s.

TRAVAIL À FAIRE

Question 1.1 **Donner à Mme Simonet des éléments de choix en évoquant la sécurité, le coût, le débit, la facilité de mise en œuvre pour chacune des deux solutions.**

Le CG96 utilise une librairie de bandes LTO *(Linear Tape Open)* pour les sauvegardes. La vitesse de sauvegarde est de 48 Mo/s. Cette librairie est reliée à un serveur qui la pilote par l'intermédiaire d'une interface Ultra160 SCSI3 à 160 Mo/s. Ce serveur récupère les données sur 6 serveurs par l'intermédiaire du réseau Fast Ethernet à 100 Mbit/s, soit 12.5 Mo/s.

Actuellement, le volume à sauvegarder est d'environ 110 Go dont 100 Go de bases de données, le reste étant constitué de fichiers utilisateurs. La sauvegarde a lieu la nuit. La durée disponible pour la sauvegarde est de 3 heures en raison des nombreux programmes qui fonctionnent la nuit. Cette durée est juste suffisante pour le moment. Mais, après la mise en place de nombreuses applications ainsi que l'archivage de documents papier sous forme numérique, la sauvegarde atteindra un volume d'environ 250 Go au total d'ici à un an. La sauvegarde des bases de données a lieu à froid (SGBD arrêté). La bande passante du réseau s'avère insuffisante.

TRAVAIL À FAIRE

Question 1.2 **Exprimer le calcul qui démontre, à partir de ces débits théoriques, l'insuffisance de la bande passante du réseau (prendre 1 Go = 1 000 Mo).**

Question 1.3 **Décrire les modifications de configuration matérielle permettant d'effectuer la sauvegarde de 250 Go en 3 heures au plus.**

Mme Simonet doit également mettre en place une infrastructure Wifi dans la salle du Conseil pour que les élus et les visiteurs, essentiellement des journalistes, puissent accéder à Internet depuis leur ordinateur portable lors des sessions du Conseil général.

Pour cela, elle dispose d'un point d'accès Wifi qui propose deux SSID (identifiant de réseau physique) associés chacun à un VLAN par le commutateur Wifi, ce qui permet la séparation complète des réseaux.

Le premier SSID n'est pas diffusé sur le réseau. Il est paramétré sur les portables des élus du CG96. Ce SSID a été configuré par le service informatique pour n'autoriser que certaines adresses MAC.

Le second SSID est diffusé sur le réseau. Il ne dispose d'aucune sécurité particulière et permet une connexion implicite pour un poste de travail configuré de manière standard. Les postes de travail utilisant ce SSID accèderont à Internet au moyen d'un accès ADSL classique. Les adresses MAC des portables des élus sont interdites sur ce SSID.

L'adressage sera effectué par deux serveurs DHCP (un pour chaque VLAN).

Le point d'accès est relié à un commutateur qui gère des VLAN. Selon la configuration d'un poste de travail portable, celui-ci se connectera sur le VLAN 1 (Élus) ou sur le VLAN 2 (Visiteurs).

TRAVAIL À FAIRE

Question 1.4 **Dire pourquoi les portables des visiteurs qui se connectent sur le second SSID obtiendront obligatoirement une adresse IP donnée par le serveur DHCP 192.168.1.33 et non par le serveur DHCP 172.16.108.2.** ***Justifier la réponse en vous appuyant sur le protocole DHCP et les VLAN.***

Pour le réseau VLAN2 (Visiteurs), Mme Simonet souhaite mettre en œuvre un plan d'adressage IP limitant à 13 le nombre d'adresses hôtes utilisables dans le réseau. Le serveur DHCP d'adresse 192.168.1.33 fera aussi office de routeur NAT.

TRAVAIL À FAIRE

Question 1.5 **Donner en la justifiant la valeur du masque de sous-réseau en notation classique et en notation CIDR.**

Question 1.6 **Donner la plage d'adresses utilisables par le serveur DHCP ainsi que les différents paramètres TCP/IP nécessaires au fonctionnement des postes de travail du réseau VLAN2 (Visiteurs).**

Après avoir paramétré le serveur DHCP du VLAN 1 (Élus), Mme Simonet teste la connexion avec la cité administrative au moyen de commandes *ping* depuis un portable d'élu disposant de l'adresse 172.16.108.10 et dont la passerelle par défaut est 172.16.108.1. Les liaisons sont opérationnelles et les postes et routeurs sont actifs. Elle exécute les deux commandes suivantes :

```
ping 172.16.4.10
      Réponse de 172.16.108.1 : impossible de joindre l'hôte de destination
      (le message sous Linux serait : Network Unreachable)

ping 192.168.8.1
      Délai d'attente de la demande dépassé (le message sous Linux serait :
      Destination Host Unreachable)
```

TRAVAIL À FAIRE

En analysant les tables de routage de l'annexe 2 :

Question 1.7 **Justifier les réponses obtenues aux deux commandes.**

Question 1.8 **Préciser quelles modifications sur les tables de routage Mme Simonet doit faire pour que la communication entre la salle du Conseil et la cité administrative fonctionne.**

Dossier 2 : Gestion du DNS et de l'accès à Internet

Annexes à utiliser : 1 et 3

Mme Simonet doit installer un nouveau serveur d'application à architecture 3-tiers (serveur *web*, couche applicative et base de données relationnelle). Elle a commandé un serveur performant nommé SRV-IM. Mais le fournisseur vient de la prévenir que la livraison sera retardée de trois semaines. Or, elle doit impérativement mettre ce serveur en production dès la semaine prochaine. En attendant, elle va donc installer le serveur sur une machine un peu ancienne nommé SRV-FIC.

L'application sera accessible sur SRV-FIC au moyen de l'URL suivante :
http://intra-marche.cg96.fr

Elle préparera ensuite SRV-IM, installera les outils et les applicatifs, réinstallera le contenu de la base de données, puis testera la nouvelle configuration. Les deux machines, SRV-FIC et SRV-IM, devront donc fonctionner simultanément sur le réseau. Lorsque les tests seront concluants, elle lancera le basculement sans que cela modifie l'URL en mettant à jour le fichier de la zone **cg96.fr**.

TRAVAIL À FAIRE

Question 2.1 Dire quelle modification doit être effectuée sur le fichier de zone cg96.fr du serveur Richelieu pour faire le basculement.

Mme Simonet décide d'installer un serveur DNS secondaire (**Milady**) pour le domaine **cg96.fr**.

TRAVAIL À FAIRE

Question 2.2 Dire quel intérêt présente la mise en place d'un serveur DNS secondaire (esclave).

À l'issue des tests, le serveur secondaire est opérationnel pour la résolution de noms sur la zone **cg96.fr**. Les postes de travail de la cité administrative sont configurés pour utiliser le serveur DNS **Milady** en premier et le serveur DNS **Richelieu** en deuxième. Après l'installation d'un nouveau serveur applicatif (**g-equip**), Mme Simonet ajoute manuellement un enregistrement Adresse (ou Hôte) dans le fichier de zone **cg96.fr** du serveur maître (**Richelieu**), mais oublie d'incrémenter le numéro de version.

Pour tester le nouvel hôte, elle lance à partir d'un poste de travail de la cité administrative la commande suivante :

```
ping g-equip.cg96.fr
```

TRAVAIL À FAIRE

Question 2.3 Donner et justifier la réponse à cette commande en vous appuyant sur les fichiers de zone de l'annexe 3.

Le pare-feu externe est paramétré pour filtrer les flux en provenance d'Internet :

Extrait de la table de filtrage du pare-feu externe coté Internet :

Règle	IP source	Port source	IP destinataire	Port destinataire	Etat TCP	Décision
9	*	*	*	> 1024	établi	Accepte
10	*	*	*	DNS (port 53)	SO	Accepte
11	*	*	*	WWW (port 80)	*	Accepte
12	*	*	*	SMTP (port 25)	*	Accepte
13	*	*	*	SSH (port 22)	*	Accepte
14	*	*	*	HTTPS (443)	*	Accepte
Défaut	*	*	*	*	*	Bloque

Remarques : Les règles sont appliquées dans l'ordre. "> 1024" signifie tous les ports supérieurs à 1024. Une étoile (*) signifie "tout". "SO" signifie sans objet, c'est-à-dire que le paramètre n'a pas d'intérêt dans ce cas. L'état TCP établi correspond à une connexion TCP en cours.

Le serveur DNS Athos ayant été victime d'attaques sur le port SSH, Mme Simonet a trois objectifs :

- éviter momentanément toute connexion SSH ;
- continuer à autoriser l'accès au DNS, au relais de messagerie et au serveur WWW de la DMZ ;
- continuer à permettre la navigation sur Internet des postes du réseau interne.

Pour cela elle envisage la solution suivante :

Supprimer les règles 9, 10, 11, 12, 13 et 14, puis n'autoriser dans un premier temps en entrée du pare-feu externe (à partir d'Internet) que les requêtes TCP établies (c'est-à-dire postérieure à une requête de connexion TCP préalable). Pour cela elle modifie la table de filtrage ainsi :

Extrait de la nouvelle table de filtrage du pare-feu externe côté Internet :

Règle	IP source	Port source	IP destinataire	Port destinataire	État TCP	Décision
9	*	*	*	*	établi	Accepte
Défaut	*	*	*	*	*	Bloque

TRAVAIL À FAIRE

Question 2.4 **Dire si cette table de filtrage répond aux trois objectifs.** ***Justifier la réponse pour chaque objectif.***

Non satisfaite par cette solution, Mme Simonet revient à la table de filtrage initiale.

TRAVAIL À FAIRE

Question 2.5 Proposer une deuxième solution respectant les trois objectifs. *Justifier la réponse.*

La politique de sécurité interne implique l'utilisation d'un serveur mandataire (*proxy*) pour accéder à Internet. Les postes de travail de la cité administrative auront comme passerelle par défaut le routeur **R-CA8** d'adresse 172.16.4.2. La solution de paramétrer les navigateurs sur les postes n'a pas été retenue car elle n'offre pas une garantie suffisante. Mme Simonet a paramétré **PROXY1** en *proxy* transparent. Un *proxy* transparent est un *proxy* dont l'existence n'est pas connue par les navigateurs. **PROXY1** écoute les requêtes HTTP sur le port 8080, les navigateurs envoient leurs requêtes sur le port 80.

TRAVAIL À FAIRE

Question 2.6 Dire quel mécanisme doit mettre en œuvre l'administratrice pour que les requêtes HTTP des postes de travail soient envoyées à PROXY1.

Dossier 3 : Protection des accès extérieurs

Depuis quelque temps, le serveur DNS externe (**Athos**) subit des attaques SSH. Les fichiers journaux font apparaître les essais infructueux de machines tentant de se connecter à l'aide d'outils fonctionnant en « force brute » c'est-à-dire par tentative d'ouverture de sessions sous le compte administrateur *(root)* ou sous d'autres comptes utilisateurs.

Extrait de fichier journal "message.log" du serveur DNS Athos

```
Jun  4 09:23:28 athos sshd[29792]: Failed password for root from 206.48.59.199 port 43540 ssh2
Jun  4 09:23:29 athos sshd[29794]: Failed password for root from 206.48.59.199 port 43622 ssh2
Jun  4 09:23:31 athos sshd[29796]: Illegal user network from 206.48.59.199
Jun  4 09:23:31 athos sshd[29796]: error: Could not get shadow information for NOUSER
Jun  4 09:23:33 athos sshd[29798]: Illegal user word from 206.48.59.199
Jun  4 09:23:33 athos sshd[29798]: error: Could not get shadow information for NOUSER
Jun  4 09:23:35 athos sshd[29800]: Failed password for root from 206.48.59.199 port 43829 ssh2
Jun  4 09:23:36 athos sshd[29802]: Failed password for root from 206.48.59.199 port 43911 ssh2
...
```

Le service informatique souhaite écrire un script qui identifiera et bloquera les adresses IP incriminées. Le script devra parcourir séquentiellement le fichier journal "message.log" et mémoriser le nombre d'attaques par adresse IP dans un tableau récapitulatif des attaques (tab_TRA). Le script identifiera une attaque par la présence du message « *Failed password for* ». Il déterminera l'adresse IP source de cette attaque et calculera le nombre d'attaques en provenance de cette adresse IP.

tab_TRA est un tableau associatif qui permet de mettre en relation une adresse IP et un nombre d'attaques. L'adresse IP est utilisée comme index du tableau.

tab_TRA['206.46.59.199'] contient le nombre d'attaques en provenance de l'adresse IP 206.46.59.199

tab_TRA['206.46.59.199'] ← *tab_TRA['206.46.59.199']* + *1* ajoute une attaque à l'adresse IP 206.46.59.199. Si l'adresse n'existe pas, elle est ajoutée automatiquement à l'index du tableau associatif et l'élément correspondant est initialisé à 0.

Une adresse IP à l'origine de plus de cinq attaques sera définitivement bloquée. Pour cela, elle sera ajoutée au fichier *interdit.txt*.

Pour écrire votre script, vous disposez des informations et ressources suivantes :

Fonction f_Présence_Chaîne(ch, ssCh) : booléen

Elle renvoie la présence (valeur vrai) ou l'absence (valeur faux) de la sous-chaîne ssCh dans la chaîne ch.

Fonction f_Extraire_IP(ch) : chaîne

Elle renvoie, sous forme de chaîne, l'adresse IP contenue dans la chaîne ch.

Procédure p_Bloque_IP(iP)

Elle ajoute la chaîne iP dans le fichier *interdit.txt*. Le fichier doit être ouvert au préalable.

Exemple de parcours d'un tableau associatif : cette suite d'instructions permet d'afficher la valeur d'index (ou clé) et la valeur correspondante pour chaque élément du tableau.

Exemple : *Pour chaque clé de tab_TRA*

Afficher("Adresse IP : ", clé, " Nombre d'attaques : ", tab_TRA[clé])

Fin pour

TRAVAIL À FAIRE

Question 3.1 **Écrire la partie du script qui permet de compter le nombre d'attaques SSH par adresse IP.** ***La déclaration des variables n'est pas exigée. Vous pouvez écrire ce script en langage algorithmique en utilisant les fonctions ci-dessus ou bien dans le langage de script de votre choix, en précisant lequel.***

Question 3.2 **Écrire la partie du script qui permet de bloquer les adresses IP sources de plus de 5 attaques SSH, le tableau tab_TRA étant déjà valorisé.**

Dossier 4 : Gestion des incidents

Annexe à utiliser : Annexe 4

Le CG96 assure en interne la maintenance de son parc informatique, notamment la gestion des incidents. Chaque utilisateur rencontrant un problème avec son poste en informe le service informatique par téléphone. Une analyse rapide de cette gestion a conduit à la création d'une base de données BDINCIDENTS dont un extrait du schéma relationnel est fourni en **annexe 4**.

TRAVAIL À FAIRE

Question 4.1 **Rédiger la requête SQL qui permet de créer la table PERSONNEL en précisant les contraintes de clé primaire et de clé étrangère.**

Un des programmes de l'application de gestion des incidents comporte la requête suivante :

```
Select LibelleService, month(DateIncident), count(*)
From INCIDENT I, PERSONNEL P, SERVICE S
Where I.NoUtilisateur = P.NoPersonnel
And P.NoService = S.NoService
And year(DateIncident) = 2006
Group by LibelleService, month(DateIncident)
Order by LibelleService
```

Remarque : La fonction year() *retourne l'année d'une date ; de même, la fonction* month() *retourne le mois.*

TRAVAIL À FAIRE

Question 4.2 **Décrire le résultat produit par l'exécution de la requête SQL précédente.**

La dernière intervention sur l'incident n° 2006086 a été enregistrée, mais il reste à mettre à jour la table INCIDENT, où l'état de cet incident doit passer à la valeur "fermé".

TRAVAIL À FAIRE

Question 4.3 **Rédiger la requête SQL de mise à jour de la table INCIDENT.**

Pour aider au suivi des incidents restant à traiter, on veut éditer la liste de tous les incidents qui n'ont pas encore fait l'objet d'une intervention avec, pour chaque incident, son numéro, sa date, le numéro de poste et le nom de la personne ayant déclaré l'incident.

TRAVAIL À FAIRE

Question 4.4 **Rédiger la requête SQL permettant d'établir cette liste.**

Mme Simonet, administratrice de la base, désire dans un premier temps, que cette application soit gérée uniquement par M. Charlus. Celui-ci aura tous les droits sur les tables INCIDENT et INTERVENTION.

TRAVAIL À FAIRE

Question 4.5 **Formuler la requête SQL permettant d'attribuer ces droits à l'utilisateur « Charlus ».**

Dossier 5 : Numérisation des documents

Annexe à utiliser : Annexe 5

Le Conseil général a décidé de numériser tous les documents de travail nécessaires aux différents collaborateurs. La procédure suivante est envisagée :

- Une fois par semaine, les documents papier à numériser sont transmis à une société spécialisée qui retourne un DVD sur lequel chaque document est mémorisé sous la forme d'un fichier au format JPEG.
- Les différents fichiers font alors l'objet d'une indexation dans un fichier XML fourni en **annexe 5**. Ce fichier contient la description de chaque document : titre, thème principal, mots clés, source (auteur et date de publication) et emplacement de stockage.
- Un dispositif de conversion XML-HTML basé sur une feuille de style XSL (voir **annexe 5**) permet à chaque collaborateur d'accéder à la liste des documents disponibles, depuis son navigateur via l'intranet.

Le tableau ci-dessous indique toutes les tâches à effectuer pour la mise en place de ce projet.

Référence de la tâche	Désignation de la tâche	Durée en jours	Tâches antérieures
A	Définition et analyse du projet.	5	Aucune
B	Recherche et choix de la société qui numérisera les documents.	4	A
C	Définition de la structure des documents XML.	2	A
D	Écriture d'un logiciel permettant l'indexation des documents.	4	B - C - F
E	Écriture de la feuille de style XSL.	2	A - C
F	Définition des droits d'accès.	3	A
G	Intégration de l'accès aux documents dans l'intranet.	3	E
H	Tests et mise au point de la solution.	3	D - G
I	Mise en place et formation des utilisateurs.	2	H

TRAVAIL À FAIRE

Question 5.1 **Construire le graphe MPM ou PERT du projet, en indiquant la date au plus tôt, la date au plus tard et la marge totale de chaque tâche. Indiquer le chemin critique.** ***Présenter la légende utilisée pour la représentation du graphe.***

La liste actuelle présente le titre, le thème principal et l'auteur de chaque document. Les collaborateurs jugent indispensable d'ajouter la date de publication à ces informations.

TRAVAIL À FAIRE

Question 5.2 **Indiquer les modifications à faire dans la feuille de style XSL de l'annexe 5 pour ajouter la date de publication dans le descriptif d'un document.**