BTS SIO – Spécialité SISR

BTS BLANC 01/2012

E5R : ÉTUDE DE CAS

Durée : 4 heures **Coefficient : 5**

CAS XONI
Éléments de corrigé

Q-1.1. En quoi le découpage en VLAN correspond-il aux objectifs d'amélioration de performance et de sécurité définis dans les préconisation du rapport d'audit ?

Les Vlan étant, par principe, étanches, aucune trame d'un vlan ne peut circuler sur un autre vlan.

- Amélioration de la sécurité : Aucune communication n'est donc possible entre les différents ateliers.
- Amélioration des performances : chaque Vlan forme un réseau indépendant dans lequel la capacité de transport est entièrement dédiée à ce vlan. Les trames de diffusion, notamment, émises par les machines des différents ateliers resteront cantonnées à leur vlan, améliorant ainsi la performance globale du réseau en réduisant le trafic au sein de chaque vlan.

Q-1.2. Pourquoi chaque VLAN doit-il correspondre à un sous-réseaux différent ?

Les vlan étant étanches, toute communication d'un vlan vers un autre doit obligatoirement passer par un routeur ; or un routeur ne peut router des paquets que d'un réseau IP vers un autre réseau IP. Cela implique donc que chaque vlan forme un réseau IP différent sinon, aucune communication ne serait possible entre eux.

Q-1.3. Chaque VLAN pourra-t-il accueillir le nombre de postes nécessaire ?

D'après les masques :

Vlan	Masque	Possibilité	Besoin
2	20 bits	2^{12} -2 = 4094 interfaces	50 + serveurs
3	27 bits	2^5 -2 = 30 interfaces	15 à 20
4	27 bits	2^5 -2 = 30 interfaces	15 à 20
5	26 bits	2^6 -2 = 62 interfaces	30 à 40
6	27 bits	2^5 -2 = 30 interfaces	15 à 20
7	27 bits	2^5 -2 = 30 interfaces	15 à 20

Q-1.4. Pourquoi est-il intéressant que le commutateur SW1 puisse faire du routage inter-vlan ?

Même si les ateliers n'ont pas besoin de communiquer entre eux, ils ont tous besoin de communiquer avec le vlan administratif (vlan2) dans lequel se trouvent les serveurs. Le routage inter-vlan permettra d'assurer ces communications en évitant d'avoir besoin d'un routeur externe pour cela.

Q-1.5. Pouvait-on obtenir la même architecture avec un commutateur ne supportant pas le routage inter-vlan ? Si oui, comment ?

Oui, il suffirait de placer sur un (ou plusieurs) des ports de sw1 un routeur qui assurera les communication IP entre les différents vlan.

Q-1.6. Pourquoi n'est-il pas gênant que les commutateurs du réseau administratif ne supportent pas les VLAN ?

Tous les postes et serveurs du réseau administratif appartiennent au même vlan (2). Il n'est donc pas utile que les commutateurs internes au réseau administratif supportent les vlan. Le fait qu'ils soient raccordés à sw1 sur un port appartenant au vlan 2 place de fait toutes les machines dans ce vlan.

Q-1.7. Le protocole Spanning Tree doit-il être activé sur tous les commutateurs, seulement sur certains ou sur aucun ?

Sur le schéma on n'observe aucune boucle entre les commutateurs ; on est donc dans une architecture arborescente dans laquelle le STP n'est absolument pas indispensable. Il serait toutefois préférable de l'activer sur tous les switchs afin qu'une boucle « accidentelle » ne vienne pas perturber le réseau par une tempête de diffusion.

Q-1.8. Évaluer chaque solution en indiquant si elle est envisageable avec le matériel dont on dispose et si elle répond ou pas au besoins de sécurité exprimé. Chaque réponse devra être argumentée.

Le but est d'empêcher les machines des employés des ateliers de se connecter au réseau de l'entreprise.

1. Filtrer les adresses MAC sur les ports d'interconnexion et sur les ports des serveurs.
    - SW2/3/4 supportent cette fonctionnalité (acl mac par port)
    - SW1 ne supporte pas cette fonctionnalité
    - Cela ne répond pas au besoin car cela empêcherait la communication entre le matériel « perso » et les serveurs, mais n'empêcherait pas le matériel « perso » de se connecter dans le vlan de l'atelier. Il ne recevrait pas d'adresse IP du DHCP mais on pourrait très bien la fixer manuellement.
2. Filtrage IP sur SW1
    - SW1 supporte cette fonctionnalité (LCA/IP3)
    - Cela ne répond pas au besoin car cela empêcherait, comme dans le cas précédent, la communication entre le matériel « perso » et les serveurs, mais n'empêcherait pas le matériel « perso » de se connecter dans le vlan de l'atelier. De plus s'il se fixe manuellement une adresse IP valide (en ayant soin de débrancher le matériel « officiel » correspondant) il aurait les même accès que s'il était autorisé. Même en restant en dhcp, le serveur dhcp lui donnera de toute façon une adresse valide.
3. Contrôle MAC par port fixé manuellement
    - SW2/3/4 supportent cette fonctionnalité (acl mac par port)
    - Cela répond au besoin puisque le matériel « perso » n'aura pas accès au port sur lequel il sera branché, lui interdisant ainsi toute communication.
4. Limitation du nombre d'hôtes
    - Ni SW1, ni SW2/3/4 ne supporte cette fonctionnalité.
    - Cela ne répond pas au besoin car si on débranche le matériel « officiel » pour mettre à la place le matériel « perso », le nombre d'hôtes sera le même.
5. Interdiction de communication entre les ports d'un même vlan
    - SW1 supporte cette fonctionnalité (filtrage du port source) mais cela n'est pas exploitable puisqu'il n'y a toujours qu'un port de SW1 dans un vlan donné, sauf pour le vlan2 qui lui n'est pas concerné
    - SW2 ne supporte pas cette fonctionnalité.
    - Cela ne répondrait pas au besoin puisqu'il suffirait de brancher le matériel non autorisé à la place d'un matériel autorisé pour que l'accès soit possible.

Q-1.9. Proposer la solution qui vous semble la plus appropriée en justifiant ce choix.

Une seule solution est matériellement faisable et répond au besoin exprimé, il s'agit de la solution consistant à lister les adresses MAC autorisées à se connecter sur chaque port du commutateur.
Toutefois, cela risque d'être long et fastidieux de saisir toutes les adresses MAC et de les affecter à chaque port et il faudra modifier ce paramétrage à chaque ajout ou déplacement de matériel.. De plus, cela ne met pas à l'abri d'une usurpation d'adresse MAC si facile avec des machines virtuelles ou des systèmes d'exploitation un peu évolués.

Q-1.10. Quel est le volume à sauvegarder à partir duquel l'offre BeNeo sera, d'un point de vue tarifaire, plus intéressante ?

Le coût annuel de Beneo est de 60*12 = 720€/an pour 50 Go
Le coût annuel de Tecarch est de 500 € pour 20 Go + 10€/an par Go supplémentaire.
L'inéquation est donc la suivante :
$720 < 500 + 10 (x-20)$
soit $x > 42$ Go

Q-1.11. Les deux prestataires n'autorisent pas le même type de sauvegarde. Quelle est l'incidence des « types de sauvegardes autorisés » sur une restauration complète en fin de période de sauvegarde ?

Sauvegarde Différentielle
Il faut restaurer la dernière sauvegarde totale et la dernière sauvegarde différentielle. En fin de période, il n'y a toujours que 2 sauvegardes à restaurer.
Sauvegarde Incrémentielle
Il faudra restaurer la dernière sauvegarde totale et toutes les sauvegarde incrémentielles depuis la sauvegarde totale ; En fin de période cela peut faire beaucoup de sauvegardes à restaurer ; Cela risque donc d'être plus long.

Q-1.12. Quels sont les autres critères qui diffèrent entre les deux prestataires et qui ont une importance dans le choix de l'offre ?

On note surtout une grosse différence au niveau des conditions techniques de l'hébergement. Alors que Beneo offre toutes les garanties en terme de sécurité et de sérieux de l'hébergement, on a aucune indication sur les conditions techniques de Tecarch.
Beneo propose des serveur virtuels privés, dont on est maître et où ne crains pas les interférences avec l'usage fait du serveur par les autres clients de Beneo ; par contre Tecarch ne propose que des serveurs mutualisés, c'est à dire où tous les clients utilisent le même serveur ce qui, en cas de compromission du serveur, présente un risque non négligeable pour nos données..
La période de sauvegarde est modulable chez Beneo et imposée chez Tecarch, ce qui laisse moins de souplesse à l'entreprise pour organiser ses sauvegardes selon ses besoins.

Q-1.13. Quelle est, de votre point de vue, l'offre à retenir ?

De toute évidence, Beneo est l'offre à retenir car elle offre une bien meilleure sécurité et plus de souplesse ; Tecarch ne présente aucun avantage sur Beneo, seul sont coût à court terme est légèrement plus intéressant. D'ici quelques années, cet avantage ne sera même plus d'actualité puisque le volume à sauvegarder s'accroît de 5% an.

Q-1.14. Énumérer la liste des VLAN à définir sur chaque commutateur (SW1, SW2, SW3 et SW4). Cette liste sera limitée au strict nécessaire.

SW1 : Vlan 2, 3, 4, 5, 6, 7
SW2 : Vlan 3 et 4
SW3 : Vlan 5 (ou aucun)
SW4 : Vlan 6 et 7

Q-1.15. Expliquer le problème posé pour la distribution des adresses par le serveur DHCP actuel sur les différents VLAN et proposer une solution.

Les vlan étant étanches, les communications DHCP entre les postes des ateliers et le serveur DHCP ne sont pas possibles même si le routage inter-vlan est activé puisque les trames de diffusion ne sont pas routées.
1 solution parmi 2

- Installer un agent relais DHCP sur le routeur entre le vlan2 et les vlan d'atelier. Si le routage est assuré par la fonction de routage inter-vlan de SW1, il faut que SW1 supporte la fonction DHCP-relay
- Implémenter le protocole 802.1q sur le serveur DHCP et lui créer une interface virtuelle dans chacun des vlan 2 à 7. Taguer le port 2 de SW1 dans les vlan 2 à 7.

Q-1.16. Établir un tableau reprenant l'affectation des ports de SW1, en lui rajoutant deux colonnes :

- ***Le ou les VLAN à associer à ce port ;***
- ***L'usage du protocole 802.1q sur ce port (oui ou non).***

Port	Périphérique connecté	Vlan	802.1q
1	R2	2	Non
2	DHCP	2 (ou 2,3,4,5,6,7 suivant la réponse à Q1.15)	Non (ou Oui suivant la réponse à Q1.15)
3	SW2	3,4	Oui
4	SW3	5	Non
5	SW4	6,7	Oui
6	Ancien switch1	2	Non
7	Ancien switch2	2	Non
8	Non connecté	1	Non
SUP 1	Non équipé	1	Non
SUP 2	Non équipé	1	Non

Q-1.17. Donner la suite de commandes à réaliser pour obtenir la configuration que vous avez prévu à la question Q-1.16.

configure reset factory-default
configure host-name **SW1**
configure max-vlans **7**
configure vlan **2** name **Administration**
configure vlan **3** name **Production-1**
configure vlan **4** name **Gestion-1**
configure vlan **5** name **Production-2**
configure vlan **6** name **Production-3**
configure vlan **7** name **Gestion-3**
configure vlan **3** tagged **3**
configure vlan **4** tagged **3**
configure vlan **6** tagged **5**
configure vlan **7** tagged **5**
configure vlan **2** untagged **1,2,6,7**
configure vlan **5** untagged **4**

Mission 2
Problème du site de Rouen.
Commentaire *:*
Méthodologie*. Cette question implique que l'étudiant utilise une méthodologie pour situer la panne qui sinon est très difficile à localiser dans l'ensemble des règles filtrage. La présence des fichiers d'iptables n'est utile que pour pouvoir indiquer « précisément » les manipulations à réaliser.*
Méthode résolution. *Il s'agit d'un problème de réplication des données LDAP sur le site de Rouen, le site de Dijon n'est pas touché. On s'intéressera donc à la communication entre le siège et Rouen. La réplication DNS n'est pas touchée, on ne s'intéressera donc qu'aux ports LDAP (88, 389, 636 et 3268).*
On vérifiera donc sur le routeur R1 les 4 règles de filtrage et de nat concernées. Tout est conforme
On vérifiera ensuite les 4 règles de nat de R3, tout est correct et les 4 règles de filtrage de R3. On découvre alors facilement l'erreur sur la règle 4 :172.16.48.20 (serveur dhcp) au lieu de 172.16.48.10 (serveur ldap).

Q-2.1. Rédiger un mail à destination du directeur de l'usine de Rouen en lui expliquant la raison de l'incident qu'il mentionne.

Expéditeur : DSI
Destinataire : Directeur Usine Rouen
Objet : Incident sur la création des comptes des nouveaux employés

Monsieur le Directeur,

L'incident que vous nous avez signalé concernant la création des comptes des nouveaux employés a été pris en charge et sa cause a été trouvé.
La panne provenait d'une erreur de configuration du routeur de votre usine qui relie votre site au siège social et qui permet, entre autre, de mettre à jour la base de comptes de votre usine.
Cet incident est en cours de résolution par le correspondant informatique de votre site, tout devrait rentrer en ordre dans les prochaines heures.

Respectueuses salutations

Prénom nom
Technicien Réseau « junior »

Q-2.2. Rédiger une courte note rappelant les symptômes de l'incident et sa cause technique.

Symptômes : Les comptes des nouveaux employés, créés au siège, ne sont pas opérationnels dans le site sur lequel ils travaillent.
Causes : La réplication de la base Ldap du site de Paris n'est pas réalisée sur le site où travaille l'employé. La réplication utilise les ports tcp 88, 389, 636 et 3268. Une erreur dans le filtrage de ces ports sur les routeurs empêche la réplication.

Q-2.3. Rédiger un courriel au correspondant informatique de Rouen pour lui indiquer précisément comment solutionner le problème.

Expéditeur : DSI
Destinataire : Correspondant Informatique Usine Rouen
Objet : Incident sur la création des comptes des nouveaux employés

Bonjour,

Le directeur de l'usine de Rouen nous a signalé un incident lors de la réplication des comptes de la base ldap sur les serveurs de votre site.
La cause de cet incident à été localisée dans le fichier de filtrage du routeur R3 dont vous avez la charge.
Voici la procédure à suivre pour retourner à un fonctionnement normal.
1/Prendre le contrôle du routeur R3
2/Éditer le fichier /etc/rules/firewall
3/Modifier la ligne 18

iptables -A FORWARD -i eth0 -s 91.10.10.10/32 ***-d 192.16.48.20/32*** *-p tcp --dport 3268 -j ACCEPT*

en la remplaçant par

iptables -A FORWARD -i eth0 -s 91.10.10.10/32 ***-d 192.16.48.10/32*** *-p tcp --dport 3268 -j ACCEPT*

4/Enregistre le fichier
5/Exécuter le programme /etc/rules/firewall

D'ici une heure les annuaires LDAP devrait être à nouveau synchronisés

Cordialement
Prénom nom
Technicien Réseau « junior »

Problème du service commercial

Commentaire *: Ici également, il faut faire preuve d'un peu de réflexion. La connexion VPN se fait correctement vers les serveurs BDD et LDAP/DNS. La connexion VPN n'est donc pas en cause, pas plus que le filtrage puisqu'il est précisé qu'il n'y en a pas sur le routeur VPN. Il faut donc chercher sur la configuration des serveurs incriminés (http et messagerie). Toutes les connexions sont autorisés, ce n'est donc pas un problème de filtrage ; il ne peut donc s'agir que d'un problème de routage. En regardant les tables de routage des différents serveurs on voit que ceux qui marchent ont une route vers le VPN que ne possèdent pas ceux qui ne marchent pas. Ils utilisent donc la passerelle par défaut ce qui empêche les réponses du serveur de revenir par le tunnel VPN.*

Q-2.4. Rédiger un mail à destination du directeur du service commercial en lui expliquant la raison de l'incident VPN qu'il mentionne.

Expéditeur : DSI
Destinataire : Direction commerciale
Objet : serveurs web et messagerie inaccessibles depuis une connexion VPN

Monsieur le Directeur,

L'incident que vous nous avez signalé concernant les difficultés que rencontrent vos commerciaux pour accéder depuis une connexion VPN aux serveurs web et de messagerie a été pris en charge et la cause a été trouvé.
La panne provient d'une erreur de configuration de ces deux serveurs.
Cette erreur est en cours de résolution par nos services et, tout devrait rentrer en ordre dans les prochaines heures.

Concernant le vol de portable, nous nous occupons de répondre à votre demande dans les plus brefs délais.

Je reste à votre disposition

Respectueuses salutations

Prénom nom
Technicien Réseau « junior »

Q-2.5. Rédiger une courte note rappelant les symptômes de cet incidents VPN et précisant la cause technique.

Symptômes : Certains serveurs, bien que fonctionnant normalement, sont inaccessibles à partir d'une connexion VPN
Cause : les connexions VPN utilisent un chemin particulier pour communiquer avec les serveurs du siège passant par le routeur RVPN et non par le routeur R1 comme le reste des communications. Il faut donc que les serveurs disponibles pour une connexion VPN possèdent une route particulière pour cet usage ; toutes les connexion destinées au VPN (10.0.0.0/24) doivent passer par RVPN (172.16.0.2).

Q-2.6. *Rédiger un e-mail à votre responsable pour proposer une solution afin de solutionner ce problème.*

Expéditeur : DSI
Destinataire : Directeur du Service Informatique
Objet : Serveurs Messagerie et http inaccessibles à partir des connexions VPN

Bonjour,

Le directeur du service commercial nous a signalé que les commerciaux n'arrivaient pas à accéder au serveur de messagerie et au serveur http.
La cause de cet incident à été localisée dans les tables de routage de ces deux serveurs. Ils n'ont, en effet, pas de route pour aller vers les tunnels VPN en passant par RVPN.

Il conviendrait de demander à un technicien « senior » d'ajouter la route :

Réseau	Masque	Passerelle	Interface
10.0.0.0	255.255.255.0	172.16.0.2	172.16.0.20

Sur les deux serveurs concernés (http et messagerie)

Cordialement

Prénom nom
Technicien Réseau « junior »

Q-2.7. *Expliquer, en le justifiant, quelle action il va falloir faire sur le routeur VPN afin que le vol du portable ne mette pas en danger la sécurité de l'entreprise.*

Afin que le voleur du portable ne puisse pas l'utiliser pour accéder au réseau de l'entreprise il convient d'invalider le certificat du portable P-COM-027 sur le routeur RVPN. Lorsqu'un ordinateur ce connecte à un serveur VPN, il présente son certificat authentifié au serveur. Le serveur vérifie ce certificat par rapport à sa base de certificats afin de vérifier l'identité de la machine demandant la connexion. Si ce certificat est invalidé sur le serveur, la connexion sera refusée.

Q-2.8. *Expliquer ce qu'il va falloir faire, avant d'envoyer le nouveau portable, pour que le commercial puisse accéder au VPN. Vous expliquerez les raisons de ces actions.*

Avant d'envoyer le portable, il va falloir, sur le serveur VPN, créer une paire de clés spécifique à cette machine et lui générer un certificat, puis enregistrer ce certificat dans la base de certificats. C'est grâce à ces éléments signés, validés et enregistrés par le serveur que le portable va pouvoir prouver son identité et que le serveur va ouvrir ou pas la connexion (le tunnel VPN).
Il faudra ensuite copier du serveur vers le portable (de façon sécurisée) la paire de clés spécifiques au portable, le certificat généré pour le portable et le certificat du serveur (certificat racine). C'est grâce à ce dernier que le portable pourra lors de la connexion s'assurer de l'identité du serveur.