	Université Larbi Ben M'hidi **Institut des Sciences et des Techniques Appliquées ISTA** **Département des réseaux-télécommunications 2ème année**	
	Correction :Télécommunications réseaux2	

Exercice 1 : 0.5× 10 pt

1. **Quel est le terme utilisé pour décrire un danger potentiel pour les actifs, les données ou les fonctionnalités réseau d'une entreprise ?**
   a) Menace
   b) Exploit
   c) Vulnérabilité
   d) Algorithmes de chiffrement asymétrique
2. **Quel type de hacker agit pour des raisons politiques et sociales ?**
   a) cybercriminel
   b) **Hacktiviste**
   c) testeur de vulnérabilité
   d) scriptkiddie
3. **Par quel type d'attaque un cybercriminel tente-t-il d'empêcher les utilisateurs légitimes d'accéder à des services réseau ?**
   a) Attaque de l'homme au milieu
   b) **DoS**
   c) Piratage de session
   d) Usurpation d'adresse
4. **Quel énoncé est vrai à propos du pare-feu ?**
   a) **Les pare-feux permettent d'effectuer du cloisonnement de réseaux**.
   b) Les pare-feux assurent la sécurité des connexions entrantes par authentification forte des utilisateurs.
   c) Les pare-feux apportent sécurité et confidentialité des transmissions.
   d) Les pare-feux servent à protéger les postes clients contre les spams
5. **Quelle possibilité offre en plus un firewall par rapport à un simple routeur ?**
   a) La mise en place d'ACL
   b) Le filtrage sur des ports de communication
   c) Le filtrage sur des groupes d'adresses
   d) **La mise en place de règles de filtrage de manière dynamique**
6. **Quelle affirmation décrit une caractéristique des listes de contrôle d'accès standard ?**

a) Elles sont configurées en mode de configuration d'interface.
b) Elles peuvent être configurées de manière à filtrer le trafic en fonction des adresses IP source et des ports source.
c) **Elles filtrent le trafic en fonction des adresses IP source uniquement**.
d) Elles peuvent être créées avec un numéro, mais pas avec un nom.

7. **Quel ACL autorisera un paquet provenant de n'importe quel réseau et destiné à un serveur Web à 192.168.1.1?**
   a) access-list 101 permit tcp host 192.168.1.1 any eq 80
   b) access-list 101 permit tcp host 192.168.1.1 eq 80 any
   c) **access-list 101 permit tcp any host 192.168.1.1 eq 80**

d) access-list 101 permit tcp any eq 80 host 192.168.1.1

8. **En utilisant la terminologie NAT, quelle est l'adresse de l'hôte source sur un réseau privé telle qu'elle est vue depuis l'intérieur du réseau**?

   a) Inside local

   b) Inside global

   c) Outside global

   d) Outside local

9. **Quelle déclaration décrit avec précision NAT dynamique?**

   a) Il mappe toujours une adresse IP privée à une adresse IP publique.

   b) **Il fournit un mappage automatisé des adresses IP locales internes à des adresses globales internes**.

   c) Il fournit un mappage des noms d'hôte internes aux adresses IP.

   d) Il fournit dynamiquement l'adressage IP aux hôtes internes.

10. **Quelle version de NAT permet à de nombreux hôtes d'un réseau privé d'utiliser simultanément une seule adresse globale interne pour se connecter à l'internet ?**

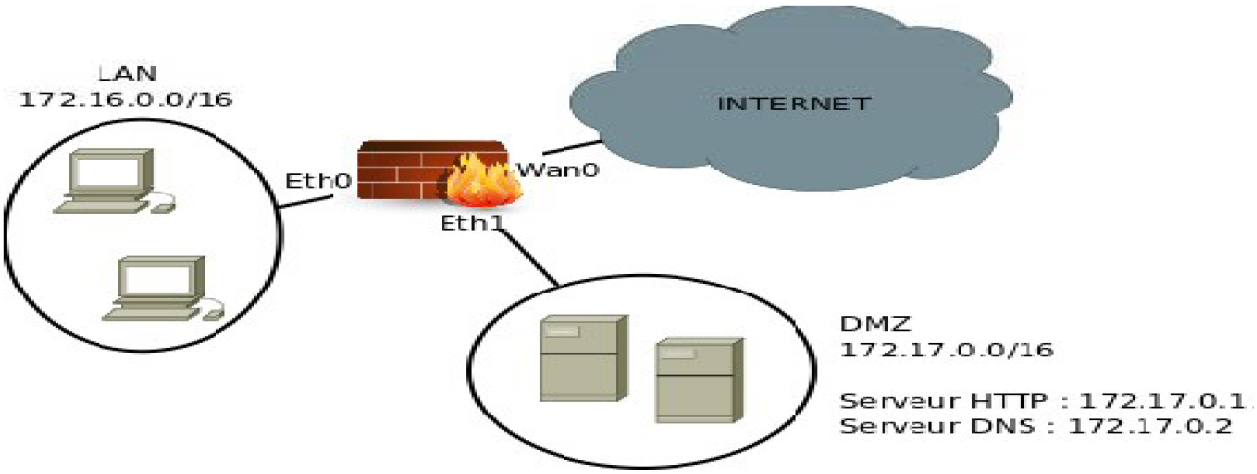
    a) **PAT**

    b) NAT statique

    c) NAT dynamique

    d) Transfert de port

Exercice 2 : 7pt



Un gestionnaire de réseau d'une entreprise a appliqué une politique de sécurité"selon la figure ".

1. Quels sont les principaux objectifs visés par cette politique de sécurité ? **1.5**pt
2. Quels outils ou technologies ont été utilisés pour mettre en œuvre cette politique **?** en indiquant les avantages de chaque outil ou technologies ? **2pt**

   Le Pare-feu (Firewall) : Avantage : Bloque les connexions non autorisées, inspecte l'état des sessions et applique la politique de sécurité.

   La DMZ (Zone Démilitarisée) : Avantage : Zone tampon isolée. Si un serveur Web y est piraté, l'attaquant reste bloqué dans la DMZ et n'accède pas directement au réseau privé interne de l'entreprise.

3. Classer les différentes zones de cette architecture de la zone la plus sécurisée à la zone la moins sécurisée **1.5**p

   ✓ Zone Interne / LAN (Le réseau local privé des utilisateurs, sécurité maximale).

   ✓ DMZ (Zone Démilitarisée) (Sécurité intermédiaire : contient les serveurs accessibles depuis Internet).

- ✓ Zone Externe / Internet (Sécurité nulle, zone totalement publique et non fiable).

4. Quelle technologie NAT permet de rendre un serveur interne accessible depuis Internet via une adresse IP publique et un port spécifique ? **1pt**

Il s'agit du Transfert de port (Port Forwarding) ou NAT Statique avec redirection de port. Cela permet d'associer l'IP publique de l'entreprise sur un port donné à l'IP privée du serveur interne.

5:Si le serveur de fichiers devait devenir public (accessible par tous les clients), dans quelle zone de l'architecture réseau vue en cours devrait-il être déplacé ? **1pt**

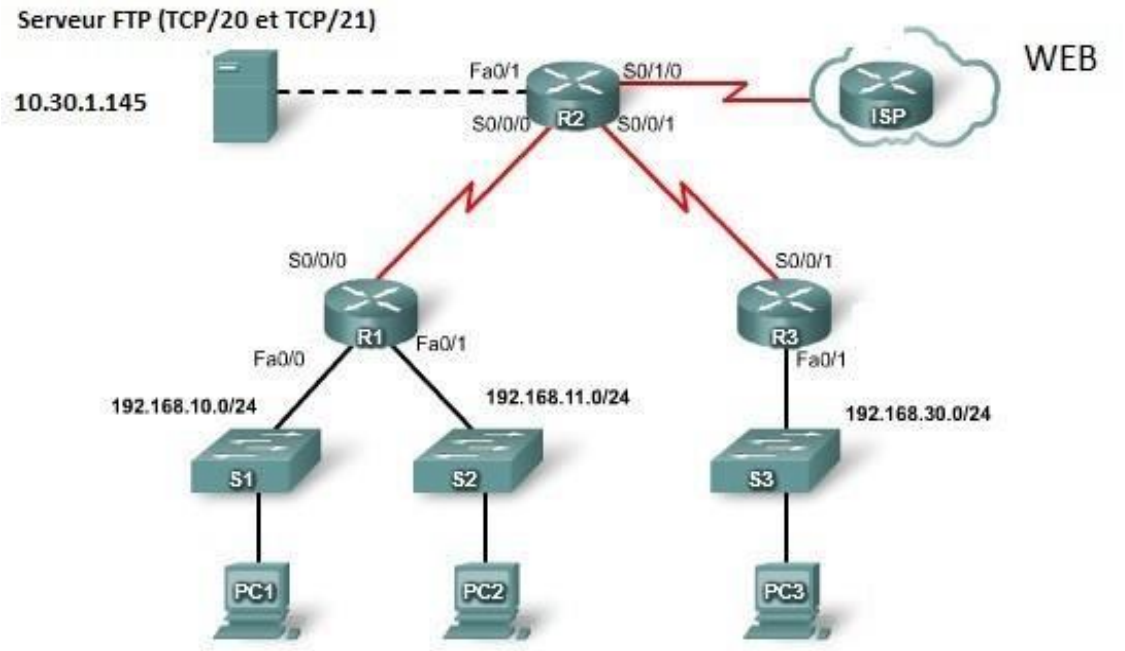
Il doit être déplacé dans la DMZ (Zone Démilitarisée). C'est la zone dédiée aux serveurs devant être consultés à la fois par le réseau interne et par les clients externes sur Internet.

Exercice 3 08pt

Soit le réseau ci-dessous, il comporte trois sous réseaux (192.168.10.0/24 et 192.168.11.0/24 et 192.168.30.0/24), 3 routeurs (R1, R2 et R3). Il y a un serveur FTP externe et une connexion série à l'internet via routeur R3.

La notation de l'interface Fa0/1 : lien Fast ethernet n°1

La notation du port S/0/0/1 : connexion série n°0



- On souhaite restreindre l'accès au service FTP pour les utilisateurs du réseau 192.168.30.0/24. Une liste d'accès (ACL) étendue doit être configurée pour répondre à cet impératif de sécurité.

1) **Comment peut-on reconnaître qu'il s'agit d'une ACL étendue ? 2pt**

On la reconnaît par son numéro (compris entre 100 et 199 dans la configuration classique Cisco) et par le fait qu'elle spécifie obligatoirement un protocole (ici TCP), une adresse source, une adresse de destination, ainsi qu'un numéro de port applicatif.

2) **Sur quel routeur de l'architecture (R1, R2 ou R3) est-il préconisé d'implanter cette ACL étendue ? Justifiez votre choix .** Il est préconisé d'implanter une ACL étendue au plus près de la source du trafic, c'est-à-dire sur le routeur relié au réseau qu'on veut bloquer : le routeur R3 (qui gère le réseau source 192.168.30.0/24). 2pt

3) Précise l'interface exacte du routeur choisi sur laquelle l'ACL doit être appliquée. ? L'interface de R3 connectée au réseau local des utilisateurs à restreindre, soit l'interface Fa0/0 (ou Fa0/1 selon le schéma typique, désignant la passerelle du sous-réseau 192.168.30.0/24). 1pt

4) **Déterminez le sens de filtrage du flux par rapport à l'interface (direction IN OUT ? IN. Le trafic doit être analysé dès qu'il entre dans l'interface du routeur en provenance du switch local. 1pt**

5) Rédigez les commandes de configuration permettant de définir cette liste d'accès et de l'activer sur l'interface appropriée, tout en garantissant que les autres types de trafic ne seront pas impactés 2pt

```
Router_R3 (config)# access-list 105 deny tcp 192.168.30.0 0.0.0.255 host  10. 30.1.145 eq 21
Router_R3 (config)# access-list 105 deny tcp 192.168.30.0 0.0.0.255 host  10. 30.1.145 eq 20
Router_R3(config)# access-list 105 permit ip any any Router_R3(config)# interface fastEthernet 0/0
Router_R3(config-if)# ip access-group 105 in
```