	Université Larbi Ben M'hidi **Institut des Sciences et des Techniques Appliquées ISTA** **Département des réseaux-télécommunications** **2ème année**
• **Durée : 1h 30** • **Documents non autorisés**	***Correction : Télécommunications réseaux2***

Exercice 1 : 4.5 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. **Quelle attaque implique des acteurs de menace se positionnant entre une source et une destination dans le but de surveiller, capturer et contrôler la communication de manière transparente ?**
   a) attaque par déni de service (DoS)
   b) Attaque par inondation SYN
   c) attaque d'homme-au-milieu
   d) Attaque ICMP
3. **Quel type de hacker agit pour des raisons politiques et sociales ?**
   a) cybercriminel
   b) Hacktiviste
   c) testeur de vulnérabilité
   d) script kiddie
4. **Par quel type d'attaque un cybercriminel tente-t-il d'empêcher les utilisateurs légitimes d'accéder à des services réseau ?**
   a) MITM
   b) DoS
   c) Piratage de session
   d) usurpation d'adresse
5. **Quelle affirmation décrit une caractéristique des listes de contrôle d'accès IPv4 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.

6. **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
7. **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**?

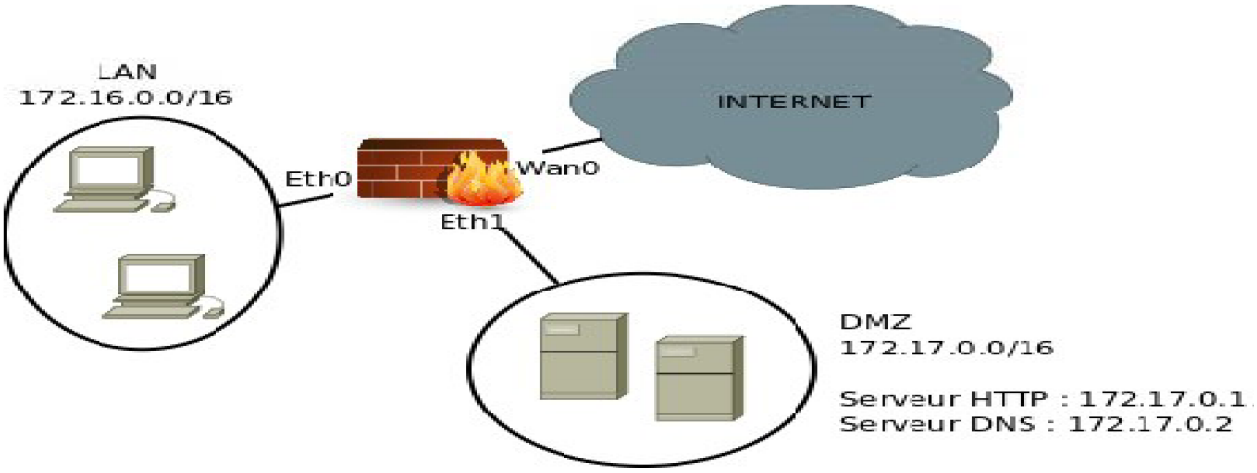
a) Inside local
b) Inside global
c) Outside global
d) Outside local

8. **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.

9. **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 :



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

1. Quelles sont les tâches principales d'un gestionnaire de réseau ? **1.5pt**
   - ✓ **Concevoir et planifier le réseau.**
   - ✓ **Installer et configurer les équipements réseau.**
   - ✓ **Contrôler et maintenir la performance du réseau et résoudre les problèmes.**
   - ✓ **Sécuriser le réseau et protéger les données.**
   - ✓ **Gérer les comptes utilisateurs et les accès**.
2. Quels sont les principaux objectifs visés par cette politique de sécurité ? **1.5 pt**
   - ✓ **Confidentialité des informations.**
   - ✓ **Intégrité des données.**
   - ✓ **Disponibilité des services et des informations**.
3. Quels outils ou technologies ont été utilisés pour mettre en œuvre cette politique**?** en indiquant les avantages de chaque outil ou technologies?

   Pare-feu (Firewall) : matériel dédié. 1.5 pt

   Avantages : pour le contrôle d'accès, la protection du périmètre et la journalisation.

   DMZ (Demilitarized Zone) **1.5 pt**

   avantages :.
   - ✓ **Contrôle d'accès : Filtrage strict du trafic.**
   - ✓ **Meilleure organisation : Séparation logique des services.**
   - ✓ **Surveillance améliorée : Détection facilitée des intrusions.**
   - ✓ **Réduction des risques : Protection accrue du réseau interne.**

4. Classer les différentes zones de cette architecture de la zone la plus sécurisée à la zone la moins sécurisée ?

LAN DMZ internet **1.5 pt**

5. Quel est l'avantage principal de placer un IDS dans cette architecture et où doit-il être placé ? **2pt**
   - ✓ **Systèmes de détection d'intrusion (IDS) : pour la détection proactive, le blocage automatique et l'analyse comportementale. Il doit être place entre le routeur et le firewall**
   - ✓ **Il doit être place entre le firewall et le DMZ**

La politique de sécurité appliquée est décrite par ce tableau. **2p**t

1. Compléter le tableau suivant permettant aux utilisateurs externes d'accéder au serveur http et ne permettant pas aux utilisateurs du LAN d'accéder aux serveurs DNS.

@IP source	@IP dest	Port source	Port destination	Protocole	ACK=1	Action
toutes	**172.17.0.1**	**>1023**	**80**	**TCP**		**Accepter**
toutes	**172.17.0.1**	**>1023**	**25**	**TCP**		**Refuser**

1) Traduire les règles suivantes implémenté au niveau du routeur en utilisant des ACL et les affecter aux interfaces adéquates **4pt**

N° de la règle	@IP source	@IP dest	port source	Port destination	protocole	Action
1	Toutes	172.17.0.1	>1023	80	TCP	Accepter
2	Toutes	172.17.0.2	>1023	25	TCP	Refuser
3	172.17.0.2	172.16.0.2	25	>1023	TCP	Accepter
4	Toutes	172.16. 0.1	>1023	21	TCP	Refuser

Rconfig access-list 101 permit tcp any host 172.17.0.1 eq 80

Rconfig access-list 101 deny tcp any host 172.17.0.2 eq 25

Rconfig access-list 101 permit tcp host 172.17.0.2 host 172.16.0.2 gt 1023

Rconfig access-list 101 deny tcp any host 172.16.0.1 eq 21