



Évaluation de Fin de Module Régionale
Année de Formation 2023/2024

Nom :

Prénom :

Groupe :

Etablissement :

Réserve à l'établissement Code :

Code module : M206

Intitulé du module : Sécurité d'une infrastructure digitale

Filière	:	Infrastructure Digitale option Systèmes et Réseaux	Durée	: 2h
Année	:	2A	Note finale	: / 40
Nom & Prénom du correcteur			Émargement	

Théorie : (20 Points)

- Qu'est-ce que la confidentialité des données dans le contexte de la sécurité informatique ? **(2 Pts)**
 - La garantie que les données sont accessibles uniquement par des personnes autorisées.
 - La vitesse à laquelle les données peuvent être traitées.
 - La mesure dans laquelle les données sont disponibles en cas de besoin.
 - La capacité à détecter et à réagir aux menaces de sécurité.
- Quel est l'objectif principal d'une ACL dans un réseau informatique ? **(2 Pts)**
 - Contrôler l'accès aux ressources réseau.
 - Accélérer le transfert de données sur le réseau.
 - Améliorer la qualité de service (QoS).
 - Identifier les menaces de sécurité.
- Quel est l'avantage principal d'utiliser un VPN ? **(2 Pts)**
 - Améliorer la vitesse de connexion.
 - Accéder à des ressources réseau de manière sécurisée via Internet.
 - Réduire la latence du réseau.
 - Fournir une meilleure qualité de service (QoS)

Réserve à l'établissement Code :

Surveillant1 :

Surveillant2 :

4. Quel est le principal objectif du chiffrement dans le contexte de la sécurité des données ? (2 Pts)
- A. Assurer l'intégrité des données.
 - B. Protéger les données contre les accès non autorisés.
 - C. Améliorer la vitesse de transfert des données.
 - D. Identifier les failles de sécurité dans un système.
5. Quelle est la différence entre le chiffrement symétrique et le chiffrement asymétrique ? (2 Pts)
- A. Le chiffrement symétrique utilise une seule clé pour le chiffrement et le déchiffrement, tandis que le chiffrement asymétrique utilise deux clés distinctes.
 - B. Le chiffrement symétrique est plus sécurisé que le chiffrement asymétrique.
 - C. Le chiffrement asymétrique est plus rapide que le chiffrement symétrique.
 - D. Le chiffrement symétrique est utilisé uniquement pour les communications en ligne, tandis que le chiffrement asymétrique est utilisé pour le stockage des données.

6. Qu'est-ce qu'une vulnérabilité en sécurité informatique ? (2 Pts)

.....

.....

.....

.....

.....

7. Quels sont les différents types de menaces informatiques ? (2 Pts)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

8. Citer les objectifs de la sécurité informatique (2 Pts)

.....

.....

.....

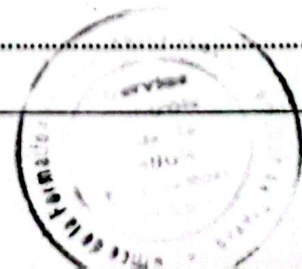
.....

.....

Réservé à l'établissement Code :

Surveillant1 :

Surveillant2 :



9. Qu'est-ce qu'une attaque de phishing et comment peut-on s'en protéger ?

(2 Pts)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

10. Qu'est-ce qu'un système de détection d'intrusion ? et quels sont les types des IDS ?

(2 Pts)

.....

.....

.....

.....

.....

.....

.....

.....

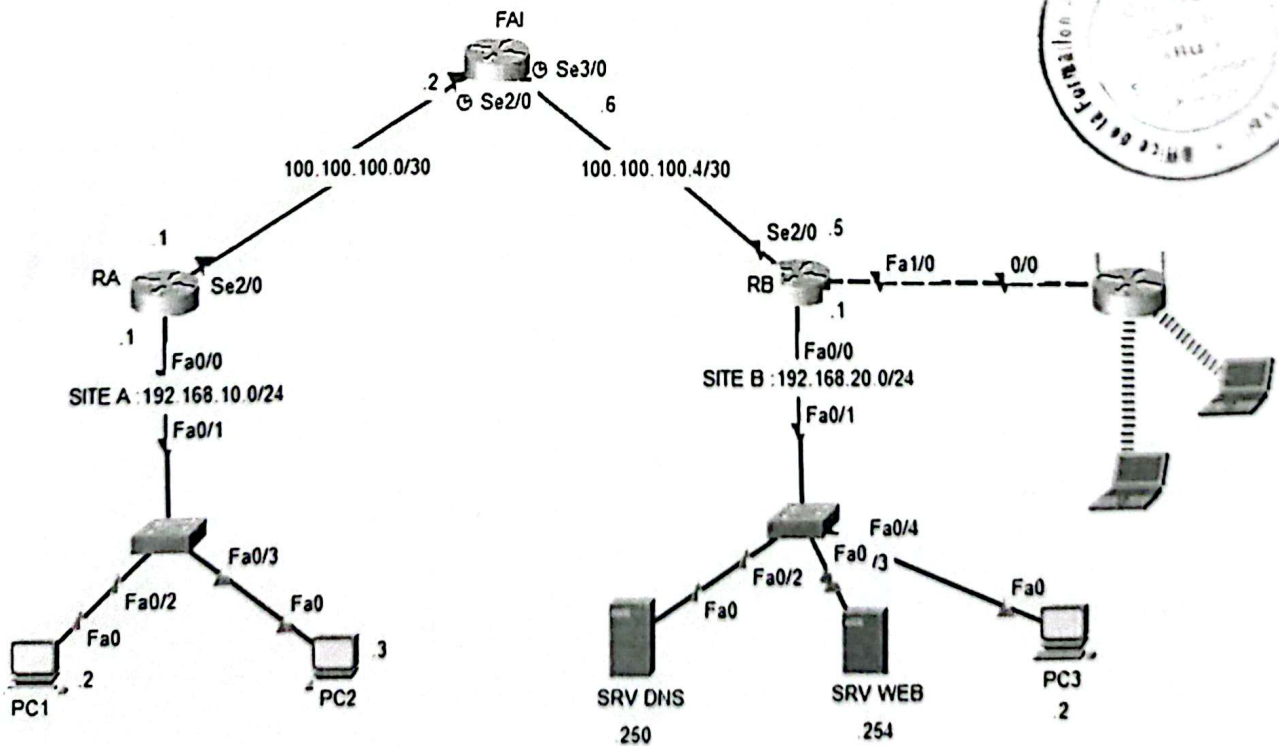
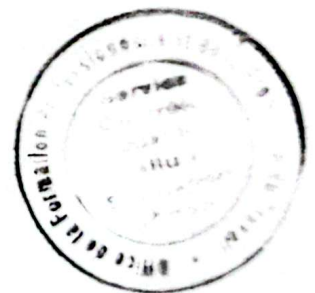
.....

.....

.....

Pratique : (20 Points)

Soit le réseau suivant représentant l'interconnexion entre deux sites d'une société



1. Créer une ACL IPv4 nommé « *FilterAtoB* » qui permet d'assurer les besoins suivants : (2 Pts)

- ✓ Autoriser le trafic *HTTP du site A* vers le serveur « *SRVWEB*»,
- ✓ Autoriser le trafic *DNS du site A* vers le serveur « *SRVDNS*»,
- ✓ Refuser tout le trafic *IP* depuis le réseau 192.168.10.0 vers le RESEAU 192.168.20.0

AUTORISER TOUT AUTRE TRAFIC

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

2. Activer cette ACL sur *L'interface convenable* (1 Pt)



.....
.....
.....
.....
.....

3. L'administrateur veut séparer le réseau des serveurs et le réseau des machines sur le site B sans introduire de nouveau matériel, quelle est la solution que vous proposez ? (1 Pt)

.....
.....
.....
.....

4. Donner des exemples d'attaques ciblant le réseau sans fil (2 Pts)

.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

5. L'administrateur réseau veut assurer une meilleure protection de son réseau sans fil, quelles sont les directives qu'il doit suivre et les paramètres qu'il doit configurer sur le routeur sans fil (2 Pts)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

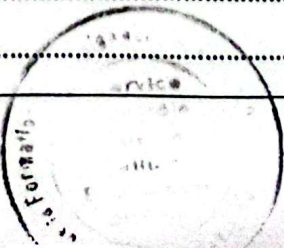
6. Dans cette partie, l'administrateur a décidé d'adopter une solution VPN pour sécuriser la communication entre les deux sites, Comment fonctionne un VPN ? (1 Pt)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Réservé à l'établissement Code :

Surveillant1 :

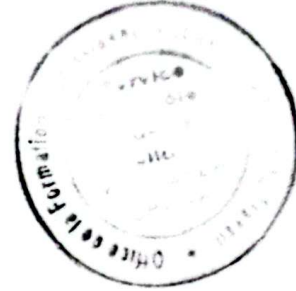
Surveillant2 :



7. L'administrateur a choisi de configurer tunnel VPN IPsec entre les sites A et B, Donner la configuration de VPN IPSEC sur le routeur RA en suivant les instructions suivantes :

7.1. Configurer le protocole 'ISAKMP' qui gère l'échange des clés en respectant les paramètres suivants : (3 Pts)

- ✓ L'algorithme de cryptage AES
- ✓ Authentification par clé pré-partagées
- ✓ Algorithme de hachage SHA (valeur par défaut)
- ✓ Groupe Diffie-Hellman 2
- ✓ Durée de vie 86400 secondes (valeur par défaut)



.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

7.2. Créer la méthode de cryptage (transform-set) nommé VPNSETV1, avec "esp-aes" comme méthode de cryptage et "esp-sha-hmac" comme méthode d'authentification. (2 Pts)

.....

.....

.....

.....

.....

7.3. Créer une liste de contrôle d'accès nommée VPNLIST, servant à identifier le trafic à traiter par le tunnel VPN. Pour RA, ce sera le trafic d'origine 192.168.10.0 à destination de 192.168.20.0 (2 Pts)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

7.4. Configurer une carte de cryptage (crypto-map) nommée VPNMAP1, servant à spécifier le pair distant, le 'transform set' et l'access list. (2 Pts)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

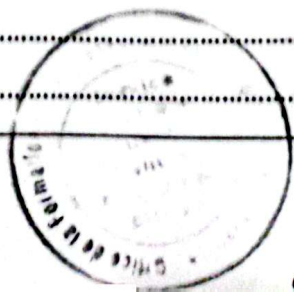
7.5. Appliquer la crypto-map à l'interface WAN de Routeur RA (2 Pts)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Réservé à l'établissement Code :

Surveillant1 :

Surveillant2 :



Scanné avec CamScanner