OFPPT مكتب التكوين المهني وإنعاش الشغل
Office de la Formation Professionnelle et de la Promotion du Travail

COMPLEXE DE FORMATION PROFESSIONNELLE AL ADARISSA
Centre Mixte de Formation Professionnelle Fès

Examen de Fin de Module Régional
Année de Formation : 2022/2023
Module 206 : Sécurité d'une infrastructure digitale

Filière/Groupe : IDoSR | Epreuve : Synthèse | Durée : 2H
Niveau : 1S | Barème : /10
Variante : 1 | Date :05/06/23

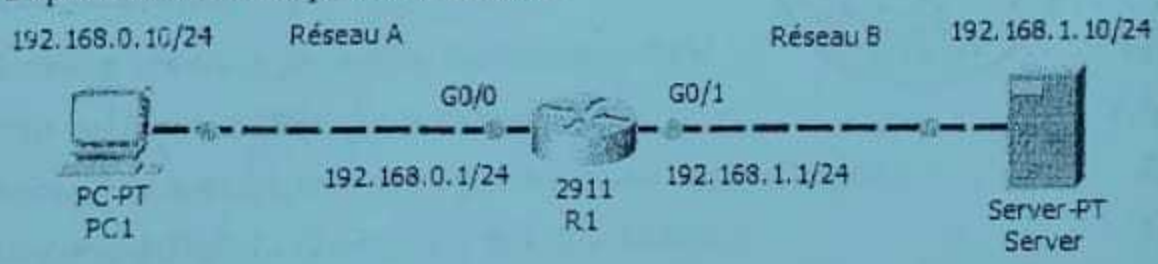
PARTIE THEORIQUE (10 PTS)

1) Expliquer le fonctionnement de la cryptographie à clé publique dans le cas de l'authentification. **2pts**
2) Quels sont les principaux services fournis par une infrastructure PKI ? **2pts**
3) Quelle est la différence entre SSL et TLS ? **2pts**
4) Définir les termes suivants : **2pts**
   a) Un système IDS/IPS
   b) Un pare-feu
5) Quels sont les différents types de VPN ? **2pts**

PARTIE PRATIQUE (30 PTS)

EXERCICE 1 : (6 PTS)

Reportez-vous à l'exposition suivante.



1) Quelle est la commande nécessaire pour autoriser les réponses au PING initié à partir du réseau A vers le réseau B. **1,5pts**
   a) #access-list 100 permit icmp 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255
   b) #access-list 100 permit icmp 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
   c) #access-list 100 permit icmp 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255 echo-reply
   d) #access-list 100 permit icmp 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255 echo-reply

Concepteur (Nom & Emargement) :	*Commission de validation :*	*Directrice Pédagogique :*
Hakima Ech-chad		

2) Quelle est la commande nécessaire pour appliquer la liste de contrôle d'accès précédente **1pt**

   (a) #interface G0/0
   #ip access-group 100 in
   b) #interface G0/1
   #ip access-group 100 in
   c) #interface G0/0
   #ip access-group 100 out
   d) #interface G0/1
   #ip access-group 100 out

3) Quelle est la meilleure façon de sécuriser un réseau sans fil ? **1pt**

   a) Utiliser un mot de passe fort
   b) Utiliser une clé WEP
   (c) Utiliser une clé WPA2-PSK

4) Qu'est-ce qu'un certificat SSL/TLS ? **1pt**

   a) Une clé de chiffrement utilisée pour protéger les communications
   (b) Une autorisation délivrée par une autorité de certification
   c) Une liste de vérification de sécurité pour un serveur web.

5) Un administrateur a défini un compte d'utilisateur local avec un mot de passe secret sur le routeur R1 pour une utilisation avec SSH. Quelles sont les trois étapes supplémentaires requises pour configurer R1 pour accepter uniquement les connexions SSH cryptées ? (Choisissez 3) **1,5pts**

   (a) Activer les sessions SSH VTY entrantes
   (b) Générez des clés pré-partagées bidirectionnelles
   c) Configurez le DNS sur le routeur
   d) Configurez le nom de domaine IP sur le routeur
   e) Activer les sessions Telnet VTY entrantes
   (f) Générez les clés SSH

EXERCICE 2 : (24 PTS)

1. **Mettre en oeuvre la prévention des intrusions IPS** **12pts**
2. Créer une signature **IPS** nommé «*IpTrafic1* ». **1,5pts**
3. Retirer, de la mémoire, toutes les signatures au sein de cette catégorie. **2pts**
4. Ajouter à «*IpTrafic1* » la catégorie « *IOS_IPS Basic* ». **2pts**
5. Expliquer l'effet des commandes suivantes : **3pts**

```
...
R1(config-sigdef-sig-engine)# event-action Produce verbose Alert
R1(config-sigdef-sig-engine)# event-action Deny connection inline
R1(config-sigdef-sig-engine)# exit
```

a) Appliquer «*IpTrafic1* » à l'interface *S3/0* de *R1*. **1,5pts**

b) Activer la journalisation. **2pts**

2. **La configuration du VPN sur les routeurs R1 et R3.** **12pts**

a) Expliquer l'effet de la commande suivante : **1.5 pts**

R1(config)# ***access-list 111 permit ip 192.168.200.240 0.0.0.15 any eq 80***

b) Configurez un type d'authentification avec clés pré-partagées. Utilisez AES-256 pour le cryptage, SHA pour l'algorithme de hachage et Diffie-Hellman groupe 5 pour l'échange de clés pour cette stratégie IKE. **2pts**

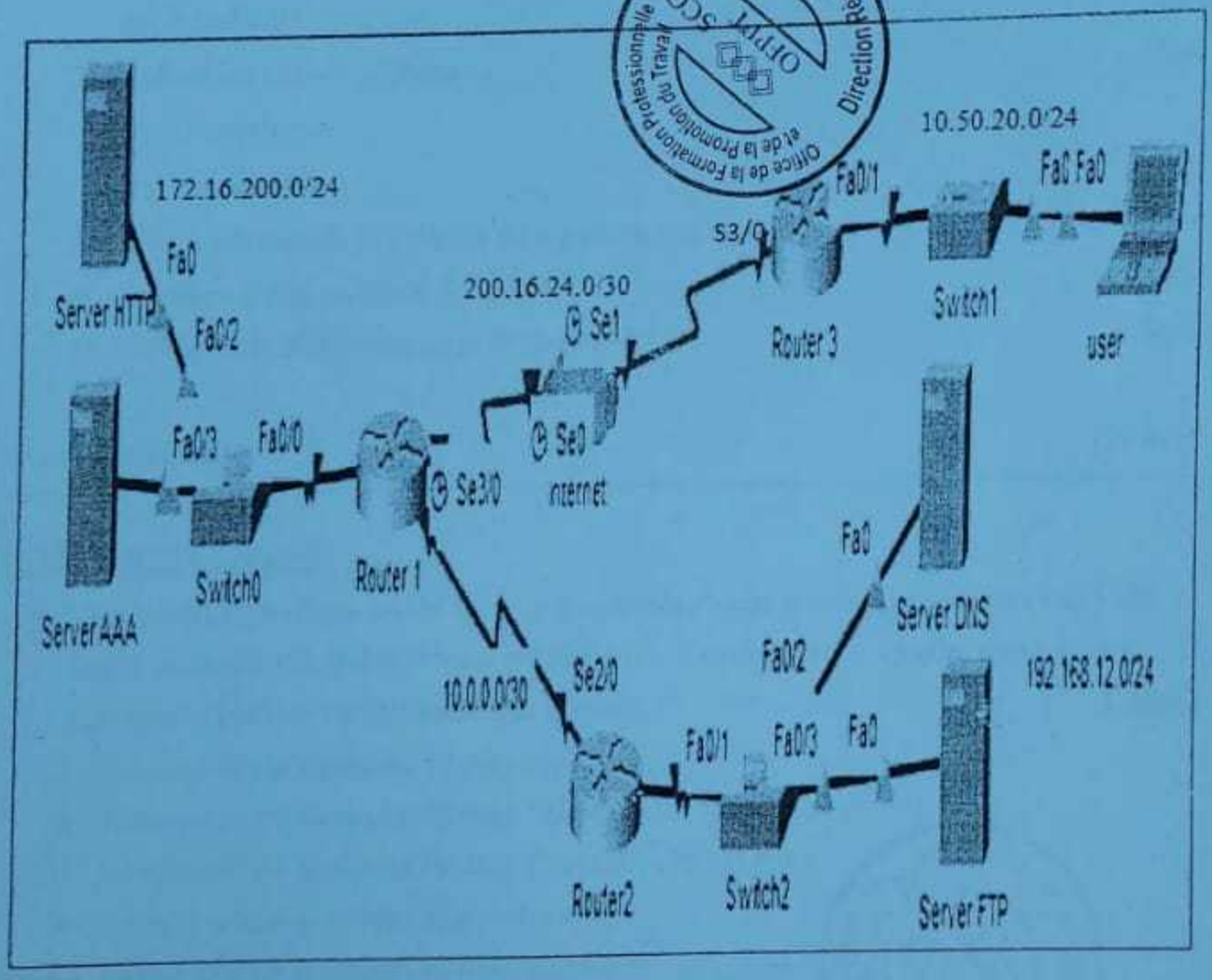
c) Configurez la clé pré-partagée CiscoR@123 en utilisant l'adresse de l'extrémité VPN distante. **2pts**

d) Créer un transform set avec le nom **VPN-SET1** et utilisez ESP avec cryptage AES-256 et SHA HMAC. **1.5 pts**

e) Créer une liste de contrôle d'accès, servant à identifier le trafic à traiter par le tunnel VPN. **2pts**

f) Créer une carte de cryptage "**CARTE1-VPN**", servant à spécifier le pair distant, le 'transform set' et l'Access list. **2pts**

g) Appliquer le cryptage VPN sur S3/0. **1pt**



OFPPT

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle
et de la Promotion du Travail

COMPLEXE DE FORMATION PROFESSIONNELLE AL ADARISSA
Centre Mixte de Formation Professionnelle Fès

Examen de Fin de Module Régional

Année de Formation : 2022/2023

Module 206 : Sécurité d'une infrastructure digitale

Filière/Groupe : IDoSR **Epreuve : Synthèse** **Durée : 2H**

Niveau : TS **Barème : /40**

Variante : 2 **Date :05/06/23**

PARTIE THEORIQUE (10 PTS)

1) Expliquer le fonctionnement de la cryptographie à clé publique dans le cas de la confidentialité. **2pts**
2) Définir les termes suivants : **2pts**
   a) Un antivirus
   b) Un pare-feu
3) Citer les étapes de la création de signature numérique ? **2pts**
4) Qu'est-ce qu'un certificat SSL/TLS ? **2pts**
5) Quelle est la différence entre IP Sec et SSL ? **2pts**

PARTIE PRATIQUE (30 PTS)

EXERCICE 1 : (6 PTS)

1) Un administrateur réseau établit une liste de contrôle d'accès standard qui interdira tout trafic venant du réseau 172.16.0.0/16 mais autorisera tous les autres trafics. Quelles sont les deux commandes à utiliser ? (Choisissez deux réponses.) **1,5pts**
   a. Router(config)# access-list 95 deny any
   b. Router(config)# access-list 95 deny 172.16.0.0 0.0.255.255
   c. Router(config)# access-list 95 deny 172.16.0.0 255.255.0.0
   d. Router(config)# access-list 95 permit any
   e. Router(config)# access-list 95 host 172.16.0.0
   f. Router(config)# access-list 95 172.16.0.0 255.255.255.255

Concepteur (Nom & Emargement) :	*Commission de validation :*	*Directrice Pédagogique :*
Hakima Ech-chad		

2) Un administrateur a configuré une liste de contrôle d'accès sur un routeur R1 pour permettre l'accès administratif SSH au host 172.16.1.100. Quelle commande applique correctement la liste de control d'accès ? **1pt**

a. R1(config-if)# ip access-group 1 out
b. R1(config-line)# ip access-class 1 out
c. R1(config-if)# ip access-group 1 in
d. R1(config-line)# ip access-class 1 in

3) Quelle est la meilleure façon de sécuriser un réseau sans fil ? **1pt**

a) Utiliser un mot de passe fort
b) Utiliser une clé WEP
c) Utiliser une clé WPA2-PSK

4) Quelle est la différence entre SSL et TLS ? **1pt**

a) SSL est une version plus ancienne de TLS
b) TLS est une version plus ancienne de SSL
c) SSL et TLS sont identiques

5) Un administrateur a défini un compte d'utilisateur local avec un mot de passe secret sur le routeur R1 pour une utilisation avec SSH. Quelles sont les trois étapes supplémentaires requises pour configurer R1 pour accepter uniquement les connexions SSH cryptées? (Choisissez 3) **1,5pts**

a) Activer les sessions SSH VTY entrantes
b) Générez des clés pré-partagées bidirectionnelles
c) Configurez le DNS sur le routeur
d) Configurez le nom de domaine IP sur le routeur
e) Activer les sessions Telnet VTY entrantes
f) Générez les clés SSH

EXERCICE 2 : (24 PTS)

1. Mettre en oeuvre la prévention des intrusions IPS **12pts**

a) Créer une signature IPS nommé «*IpTrafic2* ». **1,5pts**

b) Retirer, de la mémoire, toutes les signatures au sein de cette catégorie. **2pts**

c) Ajouter à «*IpTrafic2* » la catégorie « *IOS_IPS Basic* ». **2pts**

d) Expliquer l'effet des commandes suivantes : **3pts**

```
...
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny attacker inline
R1(config-sigdef-sig-engine)# exit
```

e) Appliquer «*IpTrafic2* » à l'interface *S3/0* de *R1*. **2pts**

f) Activer la notification d'événement *SDEE.* **1,5pts**

2. La configuration du VPN sur les routeurs R1 et R3. **12pts**

a) Expliquer l'effet de la commande suivante : **1,5pts**

R1(config)# ***access-list 120 permit ip 209.165.200.240 0.0.0.15 198.133.219.32 0.0.0.31***

b) Configurez un type d'authentification avec clés pré-partagées. Utilisez AES-256 pour le cryptage, SHA pour l'algorithme de hachage et Diffie-Hellman groupe 5 pour l'échange de clés pour cette stratégie IKE. **2pts**

c) Configurez la clé pré-partagée EfmR@123 en utilisant l'adresse de l'extrémité VPN distante. **2pts**

d) Créer un transform set avec le nom **VPN-SET2** et utilisez ESP avec cryptage AES-256 et SHA HMAC. **1.5 pts**

e) Créer une liste de contrôle d'accès, servant à identifier le trafic à traiter par le tunnel VPN. **2pts**

f) Créer une carte de cryptage "**CARTE2-VPN**", servant à spécifier le pair distant, le 'transform set' et l'Access list. **2pts**

g) Appliquer le cryptage VPN sur S3/0. **1pt**