

Examen de FIN DE MODULE -Régional : N° : 206 : MH : 60H Sécurité d'une infrastructure digitale Année 2022-2023		
Filière : IDOSR	Durée :	2H30
Niveau : TS	Variante 2	Barème : /40

Partie 1 : Les concepts de base de la sécurité : (4 pts)

1. Vous devez mettre à la disposition de votre responsable supérieur une étude technique lui expliquant les différentes contremesures à entreprendre. Pour cela, vous devez utiliser certains termes.

1.1 Définir les termes suivants : (2 pts)

- a) Une Menace
- b) Un risque.

1.2. Donner les différents types de trafic réseau : 2pts

Partie 2 : La sécurisation des périphériques : (10pts)

2. Pour la sécurisation du *plan gestion*, on vous a confié un cahier de charge que vous devrez l'appliquer sur **R1**.

2.1 Configurer les connexions SSH :

- a) Créez un nouveau compte utilisateur avec les options suivantes : (5 pts)
 - Nom de compte : « *Sshroot* »,
 - Mot de passe « *idosrSshPs*»,
 - L'algorithme de cryptage du mot de passe **MD5**.
- b) Configurer les connexions *ssh* avec les options suivantes : (5 pts)
 - Nom de domaine : **IDOSR.local**,
 - La clé de cryptage RSA est de **2048 bit**,
 - La version SSH est la **version 2**,
 - Le délai d'attente **300s**,
 - le nombre de tentatives de connexion **5**,
 - Bloquer uniquement les sessions **SSH**.

Partie 3 : La Sécurisation de l'accès aux réseaux à l'aide d'un pare-feu et d'un IPS : (10 pts)

3. Pour contrôler le flux de données venant de l'extérieur et traversant le routeur **R1**, le cahier de charge contient l'obligation d'utiliser un pare-feu à base d'**ACL** et l'implantation d'un **IPS Cisco IOS**. Vous allez appliquer la configuration sur le routeur **R1**.

3.1 Expliquer le fonctionnement des éléments suivant : (2 pts)

- a) **IPS** :
- b) Signature

3.2 Implémenter un pare-feu à base d'ACL : (8 pts)

- a) Créer une **ACL IPv4** nommée « *TraficbloqueIPv4* » qui permet d'assurer les besoins suivants : (3pts)
- Bloquer le trafic **HTTPS** vers le « *ServeurWeb-FTP* »,
 - Bloquer le trafic **DNS** vers le le « *ServeurDNS* »,
 - Bloquer le trafic **FTP** vers le « *ServeurWeb-FTP* »,
 - Bloquer le trafic **IP** depuis le « *Réseau 1* » vers le « *Siège* ».
- b) Activer cette **ACL** sur **S0/0** (2pts)
- c) Créer une **ACL IPv6** nommée « *TraficAutoriséIPv6* » qui permet d'assurer les mêmes besoins en prenant en compte les éléments suivants : (3 pts)

Périphérique	Adresse IPV6
<i>ServeurWeb-FTP</i>	<i>FD01 :11/64</i>
<i>ServeurDNS</i>	<i>FD01 :12/64</i>
<i>Poste administrateur</i>	<i>FD00 :10/64</i>

Partie 4 : La Sécurisation des données sur Internet : (8 pts)

4. Le réseau de la société doit échanger plusieurs données sensibles à travers le réseau Internet. En effet, le serveur « *Serveur DB* », situé dans la zone **DMZ**, est accédé par des télétravailleurs à partir du réseau « *Réseau-Ext* ».

Pour sécuriser ce trafic de données vous devez créer un tunnel **VPN** entre le routeur **R1** et **R3**. Cette technique utilise plusieurs concepts que vous devez maîtriser avant de configurer les routeurs.

4.1 Définir les termes suivants : (2 pts)

- a) Un chiffrement *asymétrique* et donner deux exemples d'algorithmes.
- b) Une fonction de *Hachage*.

4.2 Crypter le message suivant « *bonne chance* » en utilisant la clé symétrique « *EFM* » et en utilisant :

Un chiffrement par Vigenère : (4 pts)

4.3 Expliquer le fonctionnement de la cryptographie à clé publique dans le cas suivant:

L'authentification. : (2pts)

Partie5 : La configuration du **VPN** a été introduite sur le routeur **R1** par un spécialiste. Cependant, vous êtes invités à expliquer certains paramètres. : (8 pts)

5.1 : Quels logiciels pour mettre en place un proxy : (2 pts)

5.2 En se basant sur les commandes suivantes, remplir le tableau 1. (4 pts)

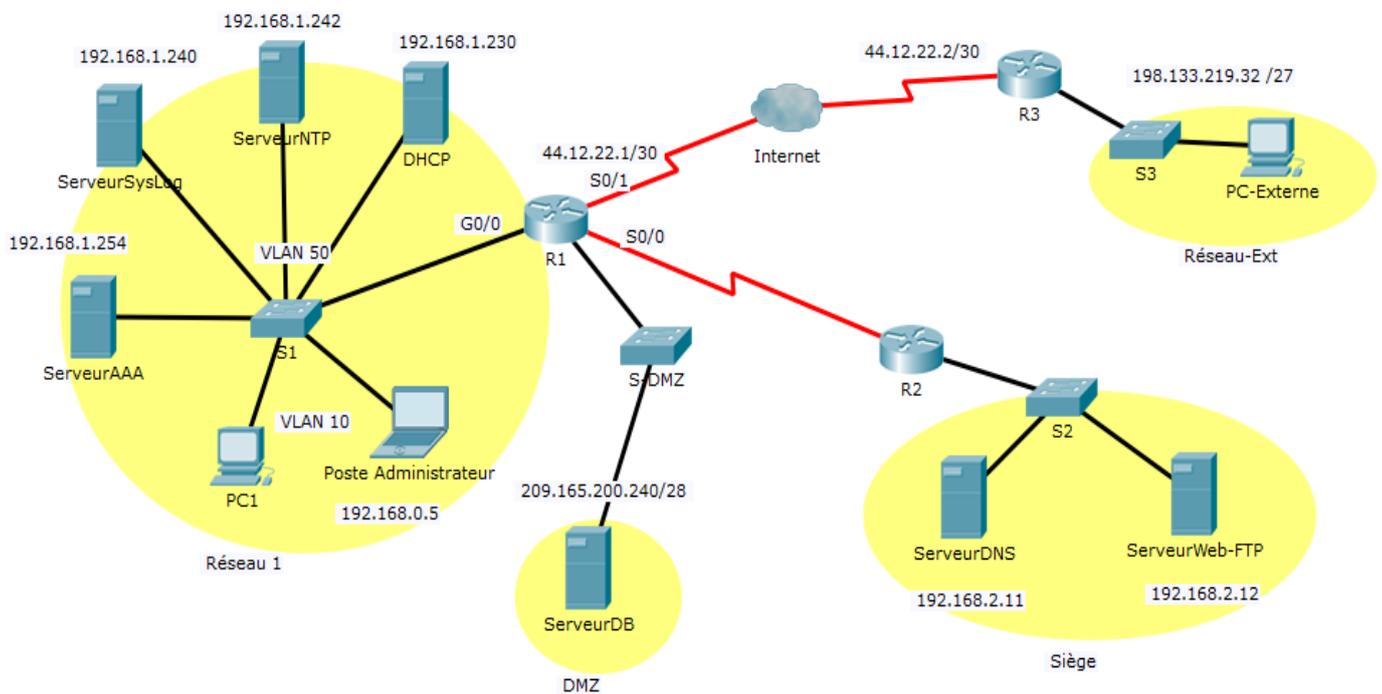
```
R1 (config)# crypto isakmp policy 1
R1 (config-isakmp)# encryption aes 192
R1 (config-isakmp)# authentication pre-share
R1 (config-isakmp)#group 2
R1 (config-isakmp)# lifetime 86400
R1 (config-isakmp)# hash sha 256
R1 (config-isakmp)# exit
R1 (config)# crypto isakmp key CiscoVpnPs address 44.12.22.2
```

Les paramètres ISAKMP Phase 1	
L'algorithme de <i>cryptage</i>	
Le nombre <i>de bit</i> utilisé pour la clé de cryptage	
L'algorithme de <i>hachage</i>	
La méthode d' <i>authentification</i>	
La clé ISAKMP	

Tableau 1

5.3 Appliquer le cryptage VPN sur S0/1. (2pts)

Annexe :



FORMATEUR : Concepteur

Oubekkar :

