EXAM SENE LMADYE :

1- Ce parefeu permet (0.5 pt)

✅ **Réponses correctes :**

- **b. La prévention des attaques**
- **c. La détection des attaques**
- **d. Le routage sécurisé des paquets vers le serveur web**

a est incorrecte car le pare-feu ne protège pas seulement le LAN.

2- Le serveur web sécurisé (0.5 pt)

✅ **Réponses correctes :**

- **b. Doit exister dans une zone séparée**
- **c. Doit être sur l'interface DMZ**
- **d. A une adresse routable publique**

3- L'interface DMZ est une interface (0.5 pt)

✅ **Réponse correcte :**

- **c. Contrôlée**

Elle est ni totalement publique ni privée, mais contrôlée pour limiter les accès.

4-1 Corriger la table de filtrage (1.5 pt)

Adresse IP source	Adresse IP destination	Port source	Port destination	Protocole	Action
Adresse IP LAN	*	>1024	80,443	TCP	Accept

Adresse IP serveur	*****	**>1024**	**80,443,53**	**TCP**	**Accept**
*****	*****	*****	*****	*****	**Deny**

4-2 Stateful ou Stateless ? (1 pt)

Ce pare-feu est stateless car :

- **Il applique des règles basées sur les en-têtes de paquets uniquement, sans tenir compte de l'état de la connexion (pas d'inspection de session TCP).**
- **On observe dans la table que seuls IP, ports et protocoles sont définis.**

4-3 Protocoles VPN/IPSec (2 pts)

Couche	Protocoles (client)	Protocoles (serveur)
Application	**HTTPS**	**HTTPS**
Transport	**TCP**	**TCP**
Réseau	**IPSec (ESP, AH)**	**IPSec (ESP, AH)**
Liaison	**Ethernet/VPN driver**	**Ethernet/VPN driver**

4-4 Critères de sécurité pour le service de paiement (2 pts)

- **Confidentialité : assurée par IPSec/HTTPS (chiffrement AES)**
- **Authentification : certificats X.509, certificat client et serveur**
- **Intégrité : HMAC, SHA-1/SHA-256**
- **Non-répudiation : signatures numériques (RSA, DSA)**
- **Disponibilité : filtrage pare-feu, protection DoS**

4-5-1 Tunnel IPSec (2 pts)

	Proposition 1	Proposition 2
Configuration	**Tunnel serveur ↔ client**	**Tunnel client ↔ routeur/firewall**
Mode(s) supporté(s)	**Tunnel, Transport**	**Tunnel**
Protocole IPSec adéquat	**ESP**	**ESP + AH (si besoin)**
Nombre de SA	**2 (1 dans chaque sens)**	**2 (pareil)**

4-5-2 Avantage/Inconvénient (1 pt)

	Proposition 1	Proposition 2
Avantage	**Simplicité (moins d'équipements)**	**Filtrage possible dès le firewall**
Inconvénient	**Plus exposé en cas de compromission**	**Complexité de configuration supplémentaire**

4-5-3 SA utilisée dans la 2e proposition (0.5 pt)

✅ **Réponse :**

- **c. Identifiée par un SPI**

4-5-4 Protocole IKE (0.5 pt)

✅ **Réponse :**

- **b. Négociation du tunnel**

4-6-1 Clés pour signature et chiffrement (1 pt)

- **Pour signer, clé a. Privée de l'émetteur du message**
- **Pour chiffrer, clé b. Publique du récepteur du message**

4-6-2 et 4-6-3 Certificats (1 pt)

- **Le certificat client sert à : b. Authentifier le client**
- **Le certificat serveur sert à : a. Authentifier les clients du serveur**

4-6-4 Si le certificat serveur est révoqué (1 pt)

✅ **Réponse :**

- **d. Il faut publier un nouveau CRL par l'AC**

4-6-5 Chaîne de certification (1 pt)

✅ **Réponse :**

- **d. ACracine-ACI1-ACI2-certserveur**

4-6-6 Nouveau CRL (1 pt)

✅ **Réponse :**

- **b. Générer un nouveau CRL contenant le certificat révoqué**

4-6-7 Signature dans le certificat (0.5 pt)

✅ **Réponse :**

- **b. L'autorité de certification (AC)**

4-6-8 Cryptage symétrique (0.5 pt)

✅ **Réponse :**

- **c. Symétrique**

4-6-9 Hachage (0.5 pt)

✅ **Réponse :**

- **d. Utilise une fonction à sens unique**

4-6-10 Clé RSA (1 pt)

Donnée :

- **$e=3e = 3e=3$, $n=55n = 55n=55$**
- **Trouver ddd tel que $e \cdot d \equiv 1 \mod \phi(n)e \cdot d \equiv 1 \mod \phi(n)e⋅d≡1modϕ(n)$**
- **$n=5\times11 \Rightarrow \phi(n)=(5-1)(11-1)=4\times10=40n = 5 \times 11 \Rightarrow \phi(n) = (5-1)(11-1) = 4 \times 10 = 40n=5×11⇒ϕ(n)=(5−1)(11−1)=4×10=40$**
- **Trouver ddd tel que $3 \cdot d \equiv 1 \mod 403 \cdot d \equiv 1 \mod 40$**

✅ **$d=27d = 27d=27$ car $3 \cdot 27 = 81 \equiv 1 \mod 403 \cdot 27 = 81 \equiv 1 \mod 40$**

Donc la clé privée est : $d=27d = 27d=27$, $n=55n = 55n=55$