Université Libanaise **ISSAE - Cnam Liban** **Centre du Liban associé au Cnam Paris**	**Date : vendredi 1/6/2018** **Durée : 14h-16h**	**Semestre : 2** **Année : 2017-2018**
Code UE : RSX112 **Intitule de l'UE : sécurité et réseaux**		**Ce sujet comporte : 3 pages**

Type d'examen :	**Semestriel**	Partiel	X Final	Rattrapage	
	Annuel	☐ E1	☐ E'1	☐ E2	☐ E'2

Documents autorisés : X Tous Aucun Autre (A préciser : ……..)

Consignes particulières :

Calculatrice: ☐ Aucune ☐ Programmable X Non programmable

Centres concernés	**X Beyrouth**	**Baakline**	**X Baalbeck**	**X Nahr Ibrahim**
	X Bickfaya	**Ghazza**	**X Tripoli**	

I- (chiffrement et protocoles 8 points) :

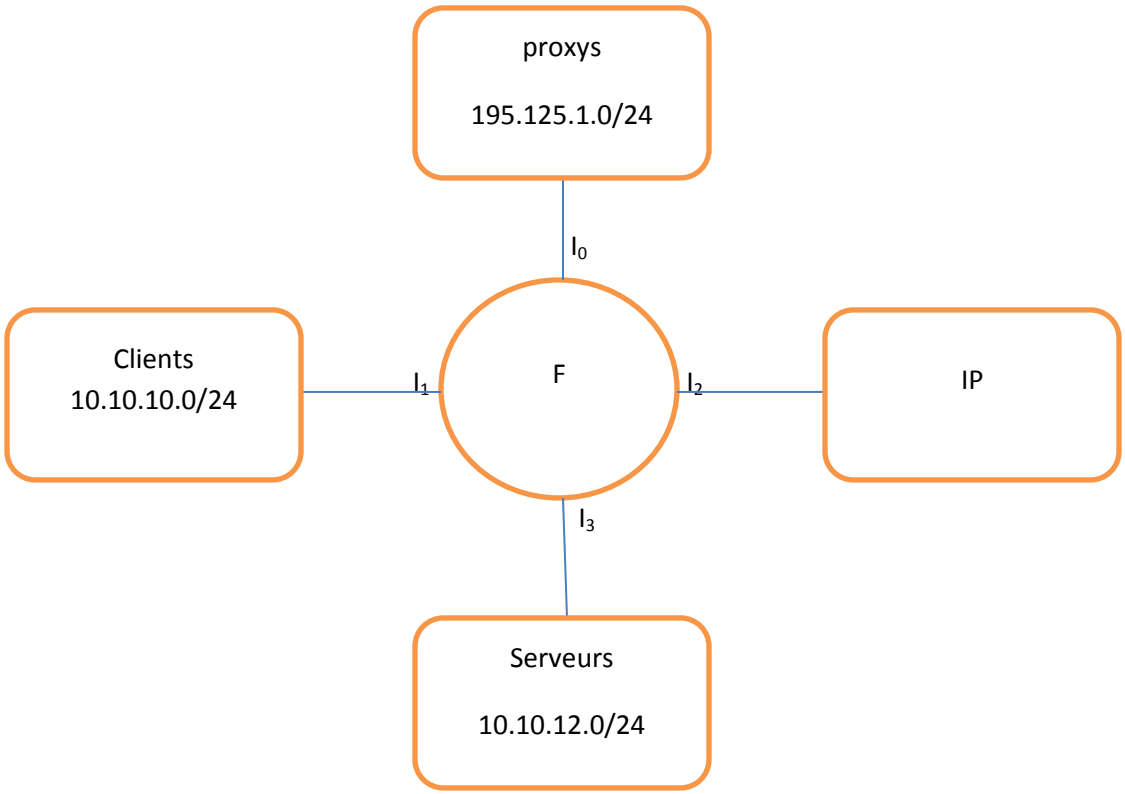
Soit le protocole SSL. Soit A et B deux entités qui veulent créer une session sécurisée entre eux. Soit CA l'autorité de certification. A et B demandent d'abord un certificat du CA.

1. Que contient les certificats et comment A et B sont sures que ce n'est pas un pirate qui a créé ce certificat ?
2. Comment est-elle envoyée la clé publique du CA d'une façon sécurisée ?
3. Si un hacker a pu créer un certificat avec le même numéro de série. Que peut-il faire pour attaquer ? que ce que se passe chez les clients ?
4. Le client A doit créer une session SSL avec authentification réciproque et échange d'une clé secrète avec le serveur B. donner les messages échangées. Spécifier dans chaque message les paramètres essentiels échangés.
5. Pour calculer la clé « master » on utilise avec la clé « premaster » les nombres aléatoires. Pourquoi ?
6. Le client crée une clé « premaster key K_{pr} = 532» calculer le chiffrement de cette clé réalisée par le client si Le certificat du serveur est cert-serv=(…,I_s , K_s=(391, 13),..). donner la valeur chiffrée en binaire.
7. A la fin de la phase de handshake le client et le serveur échange un message comprenant le mot « finished » chiffré par la clé « master ». Expliquer le rôle de ce message.
8. Le protocole de chiffrement de data est le AES en mode CBC (le calcul de l'étage précèdent est récupéré avant le AES) donc C_{i+1}=AES($S_i \oplus E_{i+1}$) avec $S_i=E_i \oplus S_{i-1}$. Et S_0 est donnée. Donner le schéma avec « n » blocs AES.

9. Si la durée de calcul de « XOR » est de 0.01ms alors que celle de AES est 1 ms. Combien faut-il des blocs AES dans le schéma CBC pour avoir un débit de 1Mb/s.

II-(Firewall 6 points) :

Soit le réseau suivant avec un seul firewall de 4 interfaces. On va appliquer les règles de firewall sur l'interface convenable mais seulement dans le sens « IN » :



1. Qu'appelle-t-on le réseau de proxy ?
2. Quel est le rôle de proxy. Pourquoi on peut considérer que la stratégie de défense est en profondeur ?
3. Sur toutes les interfaces dans le sens IN on va interdire à la fin tout par défaut. Pourquoi utiliser cette politique ? donner la règle convenable.
4. Les clients doivent accéder au serveur interne web (10.10.12.80) en utilisant http et sans passer par le proxy. L'accès au web externe doit passer par le proxy web (195.125.1.80). Donner les règles de firewall sur les interfaces convenables.
5. Le serveur DNS (10.10.12.53) doit envoyer et recevoir des requêtes avec l'extérieur via le proxy (195.125.1.53). les clients accèdent directement au serveur. Donner les règles de firewall sur les interfaces convenables.
6. Le serveur MX (10.10.12.25) doit envoyer et recevoir les emails avec l'extérieur via le proxy d'adresse (195.125.1.25). les clients accèdent directement au serveur pour envoyer et recevoir les emails. Donner les règles de firewall sur les interfaces convenables.

III-(VPN 6 points) :

Soit un utilisateur qui veut créer un VPN avec le routeur d'accès R de son entreprise.

1. Il demande l'authentification, la confidentialité et l'intégrité de ses données. Son adresse IP est 192.168.1.5. la création de ce VPN a échoué. Expliquer pourquoi ?
2. Pour pouvoir créer ce VPN il a encapsulé son paquet IP dans UDP (une autre entête IP est en dessous de UDP). Donner l'architecture en couche sur le client, sur le NAS de ISP et sur le routeur R de son entreprise.
3. Quel est le mode et le protocole utilisé ? expliquer comment les propriétés de sécurité demandées sont réalisées ?
4. La réponse de l'entreprise vers l'utilisateur passe aussi par un VPN. Donner les messages échangés entre l'utilisateur et le routeur R pour créer ces VPNs. En utilisant quelle identité l'utilisateur doit s'authentifier ?
5. Donner le format d'un paquet IP sur l'internet en spécifiant les adresses IP, les entêtes, les parties chiffrées et authentifiées. Pourquoi la natting n'affecte pas le VPN ?
6. Si la connexion avec l'ISP utilise le PPP avec serveur Radius pour l'authentification. Quelle est l'avantage de cette solution ? donner les messages échangés entre l'utilisateur, le NAS et le serveur Radius.