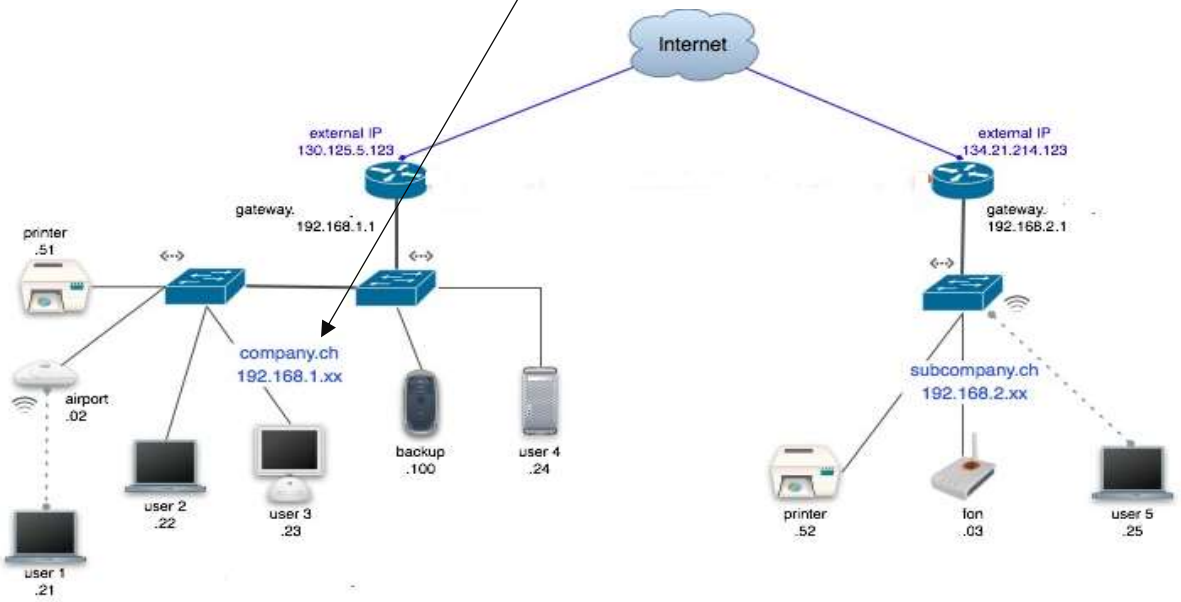
Faculté des Sciences, Département d'Informatique
ETLD du Module : Sécurité des SI,
2017/2018, Durée 1h15 Min
MA. RIAHLA

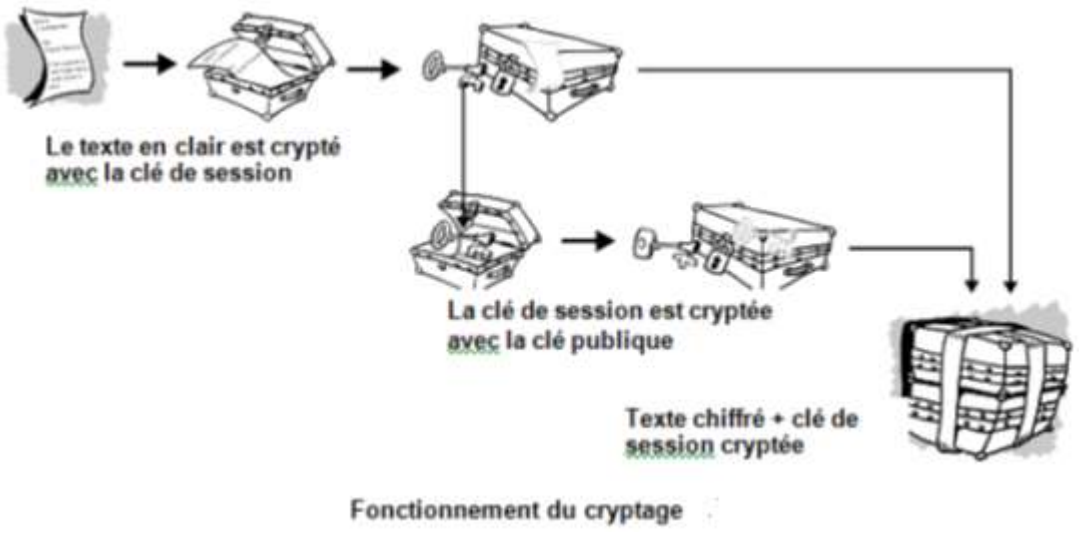
Sujet 1

Exercice 1 (12 points) :

Soit le réseau suivant :

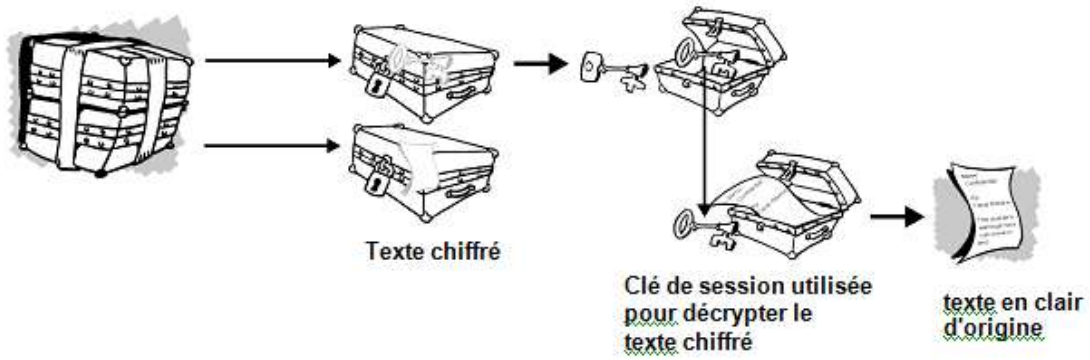


1. On souhaite connecter (en sécurisé) les deux réseaux du schéma, quelles sont les différentes solutions possibles ?
   SSH et VPN (1 point)
   Expliquez le principe de fonctionnement global de chaque solution en montrant le rôle des certificats numériques.
   Principe de fonctionnement : cryptographie hybride=symétrique + asymétrique (0.5)



Fonctionnement du cryptage

Faculté des Sciences, Département d'Informatique
ETLD du Module : Sécurité des SI,
2017/2018, Durée 1h15 Min
MA. RIAHLA



Fonctionnement du décryptage PGP

Rôle des certificats numériques : éviter l'attaque man in the middle (0.5)

2. Pourquoi faut-il ajouter un routeur entre le switch et le point d'accès wifi « airport » ?
   Pour isoler le réseau local câblé du réseau wifi (2 points)
   D'autres réponses logiques sont correctes

3. Quel est l'intérêt pour un pirate de savoir que le port 80 de la machine user 1 est ouvert ?
   Connaitre la configuration du serveur (système d'exploitation, version du serveur web,..etc) (1 point)

Port 80 ouvert donc l'existence d'un serveur web-> le pirate peut envoyer des requêtes http au serveur et observer les réponses http qui divulguent des informations sur la machine serveur (système d'exploitation, version d'apache. etc.)

Quelle est son étape suivante ?
Trouver et exploiter les failles de sécurité de cette configuration (1 point)

4. Proposez une table NAT pour la passerelle 192.168.1.1 sachant que les machines user1, user 2, user 3 et user 4 sont respectivement un serveur WEB, un serveur FTP, un serveur SSH et un deuxième serveur WEB. **(2 points)**

Table de translation NAT							
Interne				Externe			
source	port	dest	port	source	port	dest	port
192.168.10.21	80 (ou web)	Peu import	Peu import	130.125.5.123	80 ou web	Peu import	Peu import
192.168.10.22	21 (ou ftp)	Peu import	Peu import	130.125.5.123	21 ou ftp	Peu import	Peu import
192.168.10.23	22 (ou ssh)	Peu import	Peu import	130.125.5.123	22 ou ssh	Peu import	Peu import
192.168.10.24	80 (ou web)	Peu import	Peu import	?	80 ou web	Peu import	Peu import

Faculté des Sciences, Département d'Informatique
ETLD du Module : Sécurité des SI,
2017/2018, Durée 1h15 Min
MA. RIAHLA

5. L'administrateur réseau souhaite mettre en place un firewall au niveau de la passerelle 192.168.1.1, Quels sont les types de filtrage qu'il peut utiliser ? expliquez un exemple d'attaque évité par chaque type. **(2 points)**
   Filtrage par : IP source ou destination : bloquer les adresses IP des pirates.
   Filtrage par : Protocoles (TCP, UDP, ICMP,etc) : interdire smurf ICMP par exemple
   Filtres Applicatifs (proxy HTTP, FTP, SMTP,…etc) : Dos, DDos, CSS/XSS, virus sur des fichiers..etc

6. Proposez une table de filtrage pour le réseau 192.168.1.0 au niveau de la passerelle 192.168.1.1. **(2 points)**

IP source	IP destination	Port source	Port destination	Paquet SYN	Action
any	192.168.1.21ou pub	any	80 (ou web)	Ok	Permis
any	192.168.1.22 ou pub	any	21 (ou ftp)	Ok	Permis
any	192.168.1.23 ou pub	any	22 (ou ssh)	Ok	Permis
any	192.168.1.24	any	80 (ou web)	Ok	Permis
any	any	any	any	any	Interdit (deny)

Exercice 2 : (8 points)

1. Quelles sont les techniques de détection utilisées par les antivirus ?
   Signature, Analyse du code ou intelligence artificielle (statique et dynamique) et contrôle d'intégrité (1 point)
   Expliquez comment utiliser les trois méthodes conjointement. **(1 point)**
   Pour les virus détectés par l'analyse du code, il n'est pas nécessaire de les mette dans les signatures.
   Pour les virus de démarrage ou furtif par exemple : contrôle d'intégrité.
   Utiliser les signatures justes quand c'est nécessaire pour ne pas encombrer la base de données des signatures.

D'autres réponses logiques sont correctes

2. Expliquez l'impact des réseaux sociaux (Facebook, twitter, etc.) sur la sécurité des systèmes d'information des entreprises. **(2 points)**
   Un pirate peut se faire des amis avec les employés de l'entreprise via ces réseaux pour récupérer des informations confidentielles de l'entreprise.

D'autres réponses logiques sont correctes

3. Donnez un exemple d'une attaque phishing.
   < a href=''http://www.pirate.com''>www.banque.com (2 points)

D'autres réponses logiques sont correctes

4. Quel type d'attaque peut révéler un fichier log d'un serveur WEB ? expliquez **(deux réponses suffisent)**
CSS/XSS : explication (1 point)
Phishing : explication (1 point)
Dos ou ddos : explication

D'autres réponses logiques sont correctes