**Universite de Mila** **Département informatique**

**Master I I2A** **Matière : sécurité des réseaux**

# Exercices VPN IPSEC

## Exercice 1.1 — Questions de cours

Répondez de manière précise aux questions suivantes :

1. Donner une définition d'un VPN et expliquer pourquoi on qualifie ce réseau de « virtuel » et de « privé ».
2. Expliquer ce que signifie « tunneling » (ou protocole de tunnel).
3. Citer les quatre services de sécurité fondamentaux qu'un VPN doit fournir.
4. Qu'est-ce que la « Gestion des clés » dans un VPN ? Pourquoi est-elle indispensable ?
5. Un VPN peut-il, selon vous, remplacer totalement un pare-feu ? Justifier.

## Exercice 1.2 — Typologie des VPN

On distingue trois catégories de VPN selon l'usage : VPN d'accès, Intranet VPN et Extranet VPN.

1. Pour chacune des trois catégories, donner un exemple concret dans un contexte d'entreprise.
2. Un commercial en déplacement doit consulter le serveur de fichiers interne de son entreprise depuis l'hôtel où il séjourne. De quelle catégorie de VPN s'agit-il ? Faire un schéma.
3. Deux filiales d'un même groupe, situées à Alger et Sétif, veulent partager en permanence le même plan d'adressage IP privé. Quelle catégorie de VPN convient ? Justifier.
4. Une société s'associe à un fournisseur de pièces détachées et veut lui donner un accès limité à son ERP. Quelle catégorie de VPN convient ?

## Exercice 1.3 — Choix d'une technologie

Pour chacun des scénarios suivants, indiquer quel type de tunnel (IPsec, SSL/TLS ou SSH) vous recommanderiez et justifier votre choix :

a) Un utilisateur nomade veut accéder à son serveur web interne d'entreprise à partir d'un cybercafé, sans installer de client lourd.

b) Un administrateur système veut administrer à distance un serveur Linux en ligne de commande.

c) Deux routeurs doivent interconnecter deux réseaux locaux d'entreprise en chiffrant tout le trafic IP échangé.

d) Une application mobile doit envoyer des requêtes HTTPS à un serveur REST.

e) Un développeur doit copier un dépôt Git entier depuis un serveur distant en toute sécurité.

## Exercice 1.4 — Avantages et inconvénients

Remplir le tableau comparatif suivant en indiquant au moins deux éléments par case :

| Critère | VPN sur ligne dédiée (MPLS) | VPN sur Internet |
|---|---|---|
| Coût | | |
| Sécurité intrinsèque | | |
| Qualité de service (QoS) | | |
| Déploiement / Flexibilité | | |
| Dépendance vis-à-vis de l'opérateur | | |

## Exercice 2.1 — Architecture générale

1. Citer les principaux composants de l'architecture IPsec (schéma du cours).
2. Quelle est la différence entre ISAKMP et IKE ?
3. Quel est le rôle du DOI (Domain of Interpretation) ?
4. IPsec est obligatoire dans IPv6 et optionnel dans IPv4. Expliquer pourquoi.
5. Sur quel(s) port(s) IKE communique-t-il ? Sur quel protocole de transport ?

## Exercice 2.2 — AH vs ESP

Compléter le tableau suivant en mettant une croix (X) dans les cases correspondant aux services fournis par chaque protocole :

| Service de sécurité | AH | ESP (chiffrement seul) | ESP (chiffrement + auth.) |
|---|---|---|---|
| Intégrité des données | | | |
| Authentification de l'origine | | | |
| Confidentialité | | | |
| Protection anti-rejeu | | | |
| Intégrité de l'en-tête IP externe | | | |

1. Dans quelles situations choisirait-on AH seul ? Dans quelles situations choisirait-on ESP ? Peut-on combiner les deux ?
2. Pourquoi AH n'est-il pas compatible avec la traversée de NAT ? Comment IPsec contourne-t-il cette limitation (NAT-T) ?

## Exercice 2.3 — Security Association (SA)

1. Par quel triplet une SA est-elle identifiée de manière unique ?
2. Une SA est unidirectionnelle. Combien de SA faut-il pour sécuriser une communication bidirectionnelle entre deux hôtes A et B ?
3. Expliquer la différence entre IPsec SA et ISAKMP SA. Laquelle a la durée de vie la plus longue et pourquoi ?
4. Qu'appelle-t-on SPD (Security Policy Database) ? Qu'appelle-t-on SAD (Security Association Database) ? Quelle est leur différence de rôle ?
5. Citer les deux paramètres utilisés pour la durée de vie (Lifetime) d'une SA.

## Exercice 2.4 — Négociation IKE

IKE se déroule en deux phases. Répondre aux questions suivantes :

1. Quel est l'objectif principal de la phase 1 d'IKE ? Et celui de la phase 2 ?
2. Citer les trois méthodes d'authentification des pairs en phase 1 IKE.
3. Décrire brièvement le rôle de l'échange Diffie-Hellman dans la phase 1.
4. Pourquoi la phase 2 est-elle en général plus courte et plus rapide que la phase 1 ?
5. Qu'est-ce qu'un « transform set » en phase 2 ?

## Exercice 2.5 — Étude de cas : politique IPsec

Une entreprise doit configurer un tunnel IPsec entre ses routeurs R1 (192.168.1.0/24) et R2 (192.168.2.0/24). Elle choisit la politique suivante :

- Protocole : ESP
- Chiffrement : AES-256
- Authentification : HMAC-SHA256
- Mode : Tunnel
- Diffie-Hellman : groupe 14
- Durée de vie de la SA : 3600 secondes ou 4 608 000 Ko

1. Pourquoi choisit-on ici le mode Tunnel et non le mode Transport ?
2. Quels services de sécurité cette configuration fournit-elle (confidentialité, intégrité, authentification, anti-rejeu) ?
3. Représenter schématiquement la structure d'un paquet IP après encapsulation.
4. Si l'entreprise remplaçait AES-256 par DES et HMAC-SHA256 par MD5, quelles critiques de sécurité pourriez-vous émettre ?

## Exercice 3.1 — Comparaison des deux modes

Compléter le tableau suivant :

| Critère | Mode Transport | Mode Tunnel |
|---|---|---|
| Partie du paquet protégée | | |
| En-tête IP d'origine | | |
| Ajout d'un nouvel en-tête IP ? | | |
| Utilisation typique | | |
| Traversée NAT | | |
| Surcharge réseau (overhead) | | |

## Exercice 3.2 — Structure des paquets

Soit un paquet IP initial de la forme : [ IP_h | TCP_h | Données ].

1. Dessiner la structure du paquet après application de AH en mode Transport.
2. Dessiner la structure du paquet après application de ESP en mode Transport.
3. Dessiner la structure du paquet après application de ESP en mode Tunnel.
4. Dessiner la structure du paquet après application conjointe de AH + ESP en mode Transport.

5. Dans le cas du mode Tunnel, préciser ce que contiennent l'en-tête IP interne et l'en-tête IP externe, et qui les génère.

## Exercice 3.3 — Étude de cas

Une organisation dispose de deux sites A et B séparés par Internet. Le réseau interne du site A est 10.1.0.0/16 et celui du site B est 10.2.0.0/16. Les passerelles VPN ont respectivement les adresses publiques 200.1.1.1 et 200.2.2.2.

1. Quel mode IPsec doit-on utiliser pour que les hôtes des deux réseaux puissent communiquer en conservant leurs adresses privées ?
2. Un hôte 10.1.0.5 envoie un segment TCP vers 10.2.0.10. Décrire, étape par étape, la transformation subie par le paquet entre l'hôte source et l'hôte destination.
3. Que contient l'en-tête IP externe lorsque le paquet traverse Internet ?
4. Que se passerait-il si on tentait d'utiliser ici le mode Transport ? Expliquer.

## Exercice 3.4 — Fonctionnement complet d'un IPsec VPN

D'après le schéma du cours « Un complet fonctionne IPsec VPN », reconstituer l'enchaînement des opérations effectuées côté émission :

Ordonner correctement ces étapes (certaines sont déjà dans l'ordre). Indiquer pour chaque étape à quelle base de données on accède.

- Recherche dans la SPD selon les adresses source et destination.
- Décision d'action (Apply IPsec / Bypass / Discard).
- Recherche de la SA correspondante dans la SAD.
- Si aucune SA n'existe, déclenchement d'une négociation IKE.
- Application des traitements (chiffrement ESP, calcul AH, etc.).
- Encapsulation et émission du datagramme.

## Exercice 4.1 — Situation dans la pile TCP/IP

1. À quelle couche du modèle OSI (et de TCP/IP) se situe SSL/TLS ?
2. SSL/TLS s'appuie sur quel protocole de transport ? Pourquoi ce choix et non pas UDP ?
3. Expliquer pourquoi SSL/TLS est plus simple à déployer qu'IPsec pour un utilisateur nomade.
4. Citer au moins trois applications de niveau 7 qui utilisent SSL/TLS pour leur version sécurisée (par exemple HTTPS) avec leurs numéros de ports.

## Exercice 4.2 — Architecture SSL

L'architecture SSL est composée de plusieurs sous-protocoles :

1. Citer les quatre sous-protocoles de SSL et expliquer le rôle de chacun.
2. Quel sous-protocole est responsable de l'établissement des clés de session ?
3. Quel sous-protocole fournit la confidentialité et l'intégrité des données utilisateur ?
4. Que signifie « Change Cipher Spec » et à quel moment ce message est-il échangé ?

## Exercice 4.3 — Handshake SSL/TLS

Le handshake se décompose en 4 phases. Répondre aux questions suivantes :

1. Que contient le message ClientHello ? Citer au moins 4 champs.
2. À quoi sert le champ « random » envoyé par le client et par le serveur ?

3. Quelle est la différence entre les messages server_key_exchange et certificate ?
4. Dans quel cas le serveur envoie-t-il un message CertificateRequest ?
5. Quel message termine chacune des deux directions du handshake ? Est-il chiffré ?
6. Expliquer le mécanisme de « reprise de session » (session resumption). Pourquoi est-il important ?

## Exercice 4.4 — Authentification et certificats

1. Dans une session HTTPS classique, qui est authentifié : le client, le serveur, ou les deux ?
2. Pourquoi l'authentification du serveur repose-t-elle sur le DNS ? Quelle vulnérabilité cela introduit-il ?
3. Que vérifie un navigateur lorsqu'il reçoit un certificat X.509 d'un serveur ?
4. Expliquer ce qu'est une « chaîne de certification » et le rôle d'une autorité de certification (CA) racine.
5. Citer deux méthodes d'authentification possibles du client dans SSL/TLS.

## Exercice 4.5 — Étude de cas HTTPS

Un utilisateur tape l'URL https://www.banque.dz dans son navigateur.

1. Quel port TCP est utilisé ?
2. Décrire sommairement les échanges qui ont lieu avant que la première requête HTTP chiffrée ne parte.
3. Quels éléments de la requête HTTP sont chiffrés par SSL/TLS : l'URL, les en-têtes, le corps, les cookies ?
4. Que se passe-t-il si le certificat présenté par le serveur a expiré ?
5. Un attaquant placé en MITM pourrait-il lire les données ? Justifier.

## Exercice 5.1 — Généralités

1. Que signifie l'acronyme SSH ? Quel est l'objectif de ce protocole ?
2. Sur quel port TCP SSH fonctionne-t-il par défaut ?
3. Citer au moins trois commandes non sécurisées que SSH permet de remplacer.
4. Quels services de sécurité SSH fournit-il ? (confidentialité, intégrité, authentification, compression ?)

## Exercice 5.2 — Architecture SSH

La pile SSH est composée de trois sous-protocoles :

1. Citer les trois sous-protocoles SSH et expliquer le rôle de chacun.
2. Quelle partie de la pile est responsable de l'authentification du serveur auprès du client ?
3. Quelle partie de la pile permet de multiplexer plusieurs canaux logiques dans le tunnel chiffré ?
4. Citer les trois messages principaux du sous-protocole SSH User Authentication.

## Exercice 5.3 — Méthodes d'authentification

SSH propose plusieurs méthodes d'authentification du client :

1. Lister les trois méthodes principales d'authentification du client.

2. Comparer l'authentification par mot de passe et l'authentification par clé publique en termes de sécurité et d'ergonomie.
3. Décrire les étapes de génération d'une paire de clés SSH (RSA ou ED25519) sur la machine cliente.
4. Où faut-il déposer la clé publique du client sur le serveur pour que l'authentification par clé fonctionne ?
5. Que stocke le fichier ~/.ssh/known_hosts du côté client ?

## Exercice 5.4 — Tunneling avec SSH

SSH permet de rediriger différents flux dans le tunnel chiffré.

1. Qu'appelle-t-on « port forwarding » local ? Donner la syntaxe de la commande ssh correspondante.
2. Qu'appelle-t-on « port forwarding » distant ? Donner la syntaxe de la commande ssh correspondante.
3. Qu'appelle-t-on X11 forwarding ? À quoi cela sert-il ?
4. Dans quelle mesure SSH peut-il être considéré comme un VPN ?

## Exercice 6.1 — Tableau de synthèse

Remplir soigneusement ce tableau de synthèse :

| Critère | IPsec | SSL/TLS | SSH |
|---|---|---|---|
| Couche OSI concernée | | | |
| Protocole de transport utilisé | | | |
| Protocole de gestion des clés | | | |
| Authentification du serveur | | | |
| Authentification du client | | | |
| Type de trafic encapsulé | | | |
| Déploiement côté client | | | |
| Exemple d'usage typique | | | |

## Exercice 6.2 — Scénarios à choix multiple

Pour chaque scénario, choisir la solution la plus appropriée parmi {IPsec Tunnel, IPsec Transport, SSL/TLS, SSH} et justifier brièvement en 2 lignes :

a) Interconnexion permanente de deux réseaux d'entreprise via Internet.

b) Accès d'un commercial nomade à l'intranet depuis un navigateur web.

c) Administration distante d'un cluster de serveurs Linux.

d) Protection de l'API REST d'une application mobile.

e) Communication sécurisée hôte-à-hôte au sein d'un même data center sur IPv6.

f) Tunnel chiffré permettant de consulter un intranet web depuis un hôtel.

g) Copie sécurisée de sauvegardes entre deux serveurs Unix.

h) Téléphonie IP (VoIP) entre deux sites.

## Exercice 6.3

« La tendance actuelle va vers les VPN SSL, moins coûteux et moins lourds pour les machines clientes. » (extrait du cours).

Discuter cette affirmation dans une réponse structurée d'environ 15 lignes en évoquant : les coûts de déploiement, la complexité côté utilisateur, les performances, le type de trafic supporté, et les éventuelles limitations de sécurité.