Nom : _____ Date : _____ Note : _____

Sécurité de Mullvad

Analyser l'architecture de sécurité de Mullvad VPN, notamment les serveurs RAM uniquement sans disque, la politique sans journaux auditée, la génération locale des clés, le chiffrement WireGuard et les configurations de tunnel résistantes aux attaques quantiques.

SÉCURITÉ DE MULLVAD : PRÉSENTATION

APPRENANT
STATUT D'ÉTUDIANT
Parcours Défenseur du réseau

SÉCURISÉ
ÉTAT DE LA CONNEXION
Protéger les paquets de données

ACTIF
PROTECTION CONTRE LES FUITES
Protection contre les fuites DNS et IPv6

Bienvenue ! Ce dossier d'activités vous guide à travers l'architecture de sécurité de Mullvad. Vous étudierez les serveurs sans disque fonctionnant uniquement en RAM, les politiques de non-journalisation auditées, la génération locale des clés et les tunnels résistants aux ordinateurs quantiques.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez les configurations VPN et de sécurité réseau.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com des meilleurs VPN

URL: https://www.vpn.com/fr/vpn/mullvad/securite/

Votre parcours d'apprentissage : sécurité de Mullvad

- Analysez l'architecture technique et les règles de configuration de la sécurité de Mullvad.
- Configurez les paramètres du client pour éviter les fuites d'IP, de DNS et de trafic WebRTC.
- Comparez les tarifs personnalisés, l'essai et les performances avec ceux des modèles standard.

GUIDE DE SÉCURITÉ DE MULLVAD : CONSIGNES

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances aux contrôles de serveurs de Mullvad axés sur la confidentialité. Terminez par l'activité bonus Réflexion rapide.

ÉVALUER UNE INFRASTRUCTURE AXÉE SUR L'ANONYMAT ET LES SERVEURS EN RAM (INTRODUCTION)

Mullvad n'utilise pas de comptes classiques avec mot de passe et s'appuie sur des codes à 16 chiffres générés aléatoirement. Son infrastructure repose sur des nœuds sans disque fonctionnant uniquement en RAM, des clés WireGuard générées localement et des politiques de non-conservation auditées.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Quel protocole de tunneling est utilisé par défaut dans l'application Mullvad ?

- A) OpenVPN
- B) WireGuard
- C) IKEv2
- D) PPTP

2. Que demande Mullvad pour créer un nouveau compte ?

- A) Rien du tout
- B) Une adresse e-mail
- C) Un numéro de téléphone
- D) Une pièce d'identité

3. Quel tunnel cryptographique protège contre les ordinateurs quantiques ?

- A) AES-256-GCM
- B) Quantum WireGuard
- C) RSA-4096
- D) Proxy SOCKS5

4. Quel mécanisme de sécurité bloque les risques de fuite WebRTC ?

- A) Extension de navigateur
- B) Kill switch réseau
- C) Faire passer WebRTC par l'interface VPN
- D) Split tunneling

5. Quelle fonctionnalité multisaut fait passer le trafic par plusieurs nœuds ?

- A) Double NAT
- B) WireGuard Multihop
- C) Protocole Chameleon
- D) Bypasser

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Mullvad exige une adresse e-mail lors de la génération du compte.

○ Vrai ○ Faux

7 Question 7

7. Des proxys SOCKS5 peuvent être configurés à l'intérieur des tunnels Mullvad.

○ Vrai ○ Faux

8 Question 8

8. Mullvad possède et exploite l'ensemble de son matériel serveur.

○ Vrai ○ Faux

9 Question 9

9. Le Network Kill Switch est toujours actif par défaut.

○ Vrai ○ Faux

10 Question 10

10. Les paiements en espèces envoyés par courrier ne sont absolument pas remboursables.

○ Vrai ○ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Mullvad s'appuie sur _____ comme principal protocole de tunnel sécurisé à haut débit.

2. L'acheminement des données via deux emplacements de serveurs s'appelle une configuration _____ .

3. Pour éviter les journaux de données sur disque, Mullvad déploie des nœuds dédiés fonctionnant en _____ .

4. Le trafic du système est bloqué en cas de défaillance du tunnel grâce au dispositif de sécurité intégré _____ .

5. Les rapports d'audit confirment que Mullvad maintient une architecture _____ stricte et vérifiée.

6. Le routage des applications internes peut être isolé grâce à une configuration _____ personnalisée.

7. Des algorithmes de chiffrement conçus contre les ordinateurs quantiques sécurisent les données à l'intérieur d'un tunnel _____ .

8. Des serveurs de noms privés sont déployés dans le monde entier pour aider à bloquer les risques dangereux de _____ .

BANQUE DE MOTS DE VOCABULAIRE

FUITES DNS KILL SWITCH MULTI-HOP POST-QUANTIQUE RAM UNIQUEMENT SANS JOURNAUX SOCKS5 WIREGUARD

Écrivez vos réponses ici :

1.
2.
3.
4.
5.
6.
7.
8.

Point de contrôle 4 : Association de notions sur les VPN et les réseaux

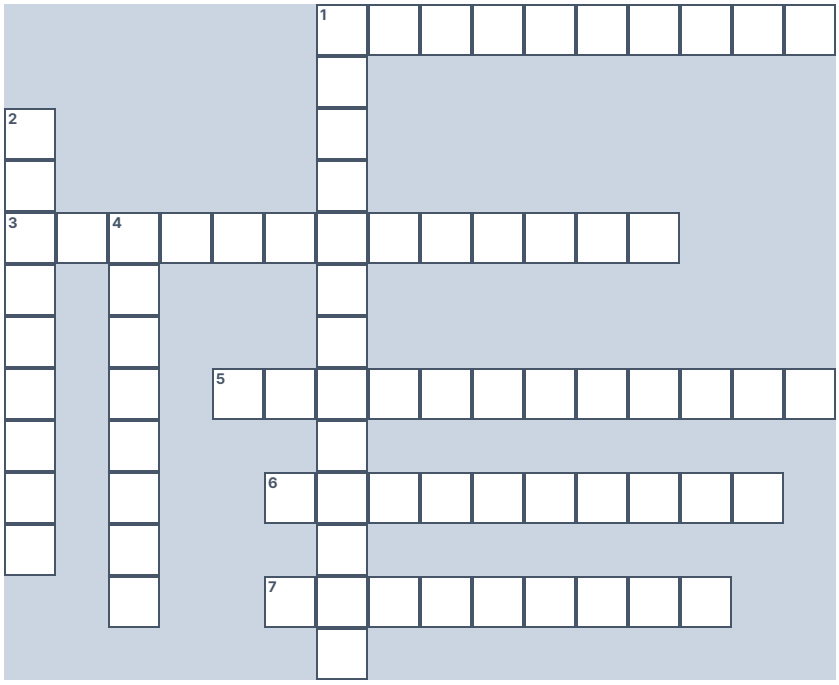
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. WIREGUARD	A	Une fonction de sécurité qui coupe le trafic lorsqu'un VPN tombe.
☐	2. MULTI-SAUT	B	Un protocole de tunnel sécurisé, léger et performant.
☐	3. UNIQUEMENT EN RAM	C	Un protocole proxy interne utilisé pour isoler les applications clientes.
☐	4. KILL SWITCH	D	Acheminement du trafic par un nœud de serveur d'entrée et un nœud de sortie.
☐	5. SANS JOURNAUX	E	Mécanismes de chiffrement conçus pour résister aux attaques quantiques.
☐	6. PROXY SOCKS5	F	Exposition des destinations des requêtes DNS en dehors du tunnel VPN.
☐	7. POST-QUANTIQUE	G	Matériel serveur à mémoire volatile qui ne conserve aucune donnée au redémarrage.
☐	8. FUITES DNS	H	Norme de non-conservation des données vérifiée par des audits indépendants.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

1. Protocole de proxy interne (SOCKS5) utilisé pour isoler les applications clientes (10)

3. Matériel serveur à mémoire volatile qui ne conserve aucune donnée au redémarrage (13)

5. Norme de non-conservation des données vérifiée par des audits indépendants (12)

6. Fonction de sécurité qui coupe le trafic lorsque le VPN se déconnecte (10)

7. Exposition des destinations des requêtes DNS hors du tunnel VPN (9)

VERTICALEMENT

1. Se dit des mécanismes de chiffrement conçus pour résister aux attaques quantiques (13)

2. Protocole de tunnel sécurisé, léger et performant (9)

4. Acheminement du trafic via un nœud serveur d'entrée et un nœud de sortie (8)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

1 horizontal: Protocole de proxy interne (SOCKS5) utilisé pour isoler les applications clientes (10 lettres):

3 horizontal: Matériel serveur à mémoire volatile qui ne conserve aucune donnée au redémarrage (13 lettres):

5 horizontal: Norme de non-conservation des données vérifiée par des audits indépendants (12 lettres):

6 horizontal: Fonction de sécurité qui coupe le trafic lorsque le VPN se déconnecte (10 lettres):

7 horizontal: Exposition des destinations des requêtes DNS hors du tunnel VPN (9 lettres):

VERTICALEMENT

1 vertical: Se dit des mécanismes de chiffrement conçus pour résister aux attaques quantiques (13 lettres):

2 vertical: Protocole de tunnel sécurisé, léger et performant (9 lettres):

4 vertical: Acheminement du trafic via un nœud serveur d'entrée et un nœud de sortie (8 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

S W G U V F W P H Y N U H V M
X K E L M F N O K U J G G R W
U F S R D Z D S U Q T J Z H M
A S F N V C A T R U B V M F O
N P U R Z P D Q T Y T Y S R F
R P O H I T L U M P D V J W P
U N J V N D R A U G E R I W R
O H C M B P V N W B T W R H O
J D E B T U K T X E J R Z X X
S I K M H C T I W S L L I K Y
N R A M U N I Q U E M E N T S
A X E M R M X U U P V C T S O
S P V F Z I I E J U Q A D Z C
N N D B R W F R J M V K X M K
Q F U I T E S D N S W J K L S

LISTE DE MOTS DE VOCABULAIRE

WIREGUARD MULTIHOP RAMUNIQUEMENT KILLSWITCH SANSJOURNAUX
PROXYSOCKS POSTQUANTIQUE FUITESDNS

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. WIREGUARD
B. MULTIHOP
C. RAMUNIQUEMENT
D. KILLSWITCH
E. SANSJOURNAUX
F. PROXYSOCKS
G. POSTQUANTIQUE
H. FUITESDNS

DÉFINITIONS ET CHAMPS D'ASSOCIATION
1. Protocole de proxy interne (SOCKS5) utilisé pour isoler les applications clientes.
2. Se dit des mécanismes de chiffrement conçus pour résister aux attaques quantiques.
3. Protocole de tunnel sécurisé, léger et performant.
4. Matériel serveur à mémoire volatile qui ne conserve aucune donnée au redémarrage.
5. Fonction de sécurité qui coupe le trafic lorsque le VPN se déconnecte.
6. Acheminement du trafic via un nœud serveur d'entrée et un nœud de sortie.
7. Exposition des destinations des requêtes DNS hors du tunnel VPN.
8. Norme de non-conservation des données vérifiée par des audits indépendants.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés sur les réseaux privés virtuels (VPN). Écrivez vos réponses dans les champs prévus.

1. UGEIWARDR
2. NNAIMREQTE MUU
3. SARUUNNOXJ AS
4. UUTSNQEAQI POT
5. IHUPTMOL
6. CSLITKIWHL
7. RXPOSCKSYO
8. SENFTUSDI

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Fonctionnalités de sécurité de Mullvad			
2	Questions à poser au service client de Mullvad			
3	Façons de créer un mot de passe robuste			
4	Personnes à qui vous recommanderiez Mullvad			
5	Choses qu'un audit peut vérifier			
6	Pays connus pour leurs lois strictes sur la vie privée			
7	Choses que vous faites en ligne chaque jour			
8	Pays où vous aimeriez avoir des serveurs Mullvad			
9	Paramètres à activer pour plus de sécurité			
10	Choses que le chiffrement protège			
11	Types de fuites VPN			
12	Mots de sécurité appris dans cette fiche			
13	Menaces sur les Wi-Fi publics			
14	Applications que vous utiliseriez avec Mullvad			
15	Appareils sur lesquels vous installeriez Mullvad			

Point de contrôle 8 : Études de cas sur les VPN et les réseaux

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : INTÉGRATION DE LA RÉSISTANCE QUANTIQUE



Scénario : Une société financière doit protéger ses transferts de fichiers contre un futur déchiffrement par ordinateur quantique.

Question de discussion : Quelle configuration de tunnel doit-elle déployer dans l'application Mullvad ?

ÉTUDE DE CAS 2 : ROUTAGE DISCRET POUR L'ENQUÊTE



Scénario : Un enquêteur veut faire passer sa connexion par un double routage pour masquer son point d'entrée.

Question de discussion : Quelle fonctionnalité de Mullvad faut-il activer pour obtenir un routage via plusieurs serveurs ?

Point de contrôle 9 : Déchiffrer le code

Un ingénieur réseau sécurise les canaux de routage et les tunnels des clients. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

13	21	12	12	22	1	4		14	5		4	5	13	1	14	4	5		14	9
13	**15**	**20**		**4**	**5**		**16**	**1**	**19**	**19**	**5**		**14**	**9**		**5**	**13**	**1**	**9**	**12**

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur les VPN (Partie A)

Passez en revue les questions et réponses les plus courantes sur les réseaux privés virtuels (VPN) et le tunneling.

Q1: Comment Mullvad sécurise-t-il les comptes ?

Mullvad utilise un numéro de compte généré à 16 chiffres, sans mot de passe ni e-mail. [1]

Q2: Quel protocole Mullvad privilégie-t-il ?

Mullvad privilégie WireGuard pour sa vitesse, sa simplicité et sa cryptographie moderne. [9]

Q3: Les serveurs de Mullvad sont-ils audités ?

Oui, des sociétés de sécurité tierces effectuent régulièrement des audits de l'infrastructure et du code.

Q4: Mullvad prend-il en charge OpenVPN ?

Non, Mullvad a supprimé OpenVPN le 15 janvier 2026 ; il fonctionne uniquement avec WireGuard. [7]

Q5: Qu'est-ce que le kill switch de Mullvad ?

Il s'agit d'une règle de pare-feu intégrée qui bloque le trafic Internet si le VPN tombe en panne.

Point de contrôle 10 : Questions fréquentes de base sur les VPN (Partie B)

Passez en revue les questions et réponses les plus courantes sur les réseaux privés virtuels (VPN) et le tunneling.

Q6: L'IPv6 est-il pris en charge par Mullvad ?

Oui, Mullvad prend en charge le routage IPv6 natif et la protection contre les fuites.

Q7: Mullvad propose-t-il le multihop ?

Oui, le multisaut WireGuard permet d'enchaîner plusieurs emplacements de serveurs.

Q8: Puis-je utiliser des résolveurs DNS personnalisés ?

Oui, des adresses DNS personnalisées peuvent être configurées dans les paramètres du client Mullvad.

Q9: Comment la journalisation est-elle évitée ?

Les configurations système désactivent la journalisation et vident les caches de tous les démons des serveurs.

Q10: Où Mullvad est-il constitué ?

Mullvad est immatriculé à Göteborg, en Suède, sous juridiction suédoise.

Point de contrôle 10 : Questions fréquentes avancées sur les VPN (Partie C)

Découvrez les aspects techniques avancés des protocoles de tunnel VPN, de l'intégration des clients mobiles et du déploiement en entreprise.

Q1: Comment fonctionne la rotation des clés ?

L'application fait tourner automatiquement les clés WireGuard ; l'intervalle par défaut de la CLI est de 30 jours. [3]

Q2: Que sont les tunnels résistants au quantique ?

Ils ajoutent à WireGuard un échange de clés ML-KEM et Classic McEliece pour résister aux futures attaques quantiques. [2]

Q3: En quoi les nœuds fonctionnant uniquement en RAM sont-ils sécurisés ?

Ces nœuds n'écrivent aucune donnée sur des disques durs, ce qui rend inutile le vol des serveurs physiques.

Q4: Qu'est-ce que la fonction de proxy SOCKS5 ?

Il aide à acheminer le trafic de certaines applications à l'intérieur du tunnel, ce qui évite les fuites vers des réseaux externes.

Q5: Mullvad protège-t-il contre les fuites WebRTC ?

Oui, l'application force les requêtes WebRTC à passer par l'interface VPN pour protéger les IP locales.

Point de contrôle 10 : Questions fréquentes avancées sur les VPN (Partie D)

Découvrez les aspects techniques avancés des protocoles de tunnel VPN, de l'intégration des clients mobiles et du déploiement en entreprise.

Q6: Comment Mullvad gère-t-il les perquisitions de police ?

Mullvad ne conserve aucun journal dans ses bases de données d'utilisateurs : aucune information sur les utilisateurs ne peut donc être extraite.

Q7: Quel est le risque lié à la juridiction suédoise ?

La Suède est membre des 14 Eyes, mais l'architecture sans journaux de Mullvad élimine le risque lié aux données.

Q8: Les audits des applications clientes sont-ils open source ?

Oui, les applications sont open source (GPL-3) et auditées par des sociétés comme X41 D-Sec. [6]

Q9: Comment fonctionne le split tunneling ?

Il utilise les tables de routage du système d'exploitation pour exclure certaines applications de la surcharge du VPN.

Q10: Comment Mullvad gère-t-il les paiements en espèces ?

Les espèces sont envoyées par courrier avec un code jeton, créditées manuellement, puis les enveloppes sont détruites.

Partie 11 : 10 faits et enseignements concrets sur les VPN

Découvrez des faits concrets sur les vitesses de chiffrement des VPN, les audits de protocoles, la connectivité mobile et le télétravail en entreprise.

1. APERÇU VPN

Mullvad a été fondé en 2009 par Amagicom AB à Göteborg, en Suède.

2. APERÇU VPN

Les numéros de compte sont le seul identifiant utilisé pour créditer les comptes et y accéder.

3. APERÇU VPN

Aucun nom, e-mail, mot de passe ni numéro de téléphone n'est stocké dans la base de données des utilisateurs.

4. APERÇU VPN

Les clés WireGuard sont générées localement sur les appareils clients pour éviter une compromission côté serveur.

5. APERÇU VPN

L'audit d'infrastructure réalisé par Cure53 en 2024 n'a trouvé aucune faille compromettant l'anonymat du trafic VPN. [5]

6. APERÇU VPN

Chaque serveur WireGuard de Mullvad exécute un proxy SOCKS5, accessible uniquement dans le tunnel. [8]

7. ZOOM SUR LES VPN

Le trafic WireGuard peut être obfusqué avec Shadowsocks, QUIC ou LWO pour franchir les pare-feu. [10]

8. ZOOM SUR LES VPN

Mullvad a achevé sa migration vers des serveurs VPN fonctionnant uniquement en RAM en septembre 2023. [4]

9. ZOOM SUR LES VPN

ML-KEM et Classic McEliece négocient une clé prépartagée post-quantique pour WireGuard. [2]

10. APERÇU VPN

Les enveloppes d'espèces et leur contenu non monétaire sont détruits une fois le temps d'abonnement crédité.

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés de normes techniques, de spécifications et de cadres réglementaires internationaux.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] Mullvad VPN. (n.d.). Why Mullvad VPN?
https://mullvad.net/en/why-mullvad-vpn

[2] Mullvad VPN. (n.d.). Quantum-resistant tunnels with WireGuard.
https://mullvad.net/en/help/quantum-resistant-tunnels-with-wireguard

[3] Mullvad VPN. (n.d.). CLI commands for using WireGuard.
https://mullvad.net/en/help/cli-command-wg

[4] Mullvad VPN. (2023). We have successfully completed our migration to RAM-only VPN infrastructure.
https://mullvad.net/en/blog/we-have-successfully-completed-our-migration-to-ram-only-vpn-infrastructure

[5] Mullvad VPN. (2024). Fourth Infrastructure audit completed by Cure53.
https://mullvad.net/en/blog/fourth-infrastructure-audit-completed-by-cure53

[6] Mullvad VPN. (2024). The report for the 2024 security audit of the app is now available.
https://mullvad.net/en/blog/the-report-for-the-2024-security-audit-of-the-app-is-now-available

[7] Mullvad VPN. (2024). Removing OpenVPN 15th January 2026.
https://mullvad.net/en/blog/removing-openvpn-15th-january-2026

[8] Mullvad VPN. (n.d.). SOCKS5 proxy.
https://mullvad.net/en/help/socks5-proxy

[9] Mullvad VPN. (n.d.). Why WireGuard?
https://mullvad.net/en/help/why-wireguard

[10] Mullvad VPN. (n.d.). Using Mullvad VPN in restrictive locations.
https://mullvad.net/en/help/connecting-to-mullvad-vpn-from-restrictive-locations

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

[12] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1

Bonne réponse : B

NOTE PÉDAGOGIQUE

Quel protocole de tunneling est utilisé par défaut dans l'application Mullvad ? → WireGuard

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

Un clic sur « generate account » vous donne un numéro de compte ; aucune adresse e-mail ni autre information personnelle n'est demandée.

3 Question 3

Bonne réponse : B

NOTE PÉDAGOGIQUE

Les tunnels WireGuard résistants aux ordinateurs quantiques de Mullvad utilisent ML-KEM et Classic McEliece pour convenir d'une clé pré-partagée.

4 Question 4

Bonne réponse : C

NOTE PÉDAGOGIQUE

Quel mécanisme de sécurité bloque les risques de fuite WebRTC ? → Faire passer WebRTC par l'interface VPN

5 Question 5

Bonne réponse : B

NOTE PÉDAGOGIQUE

Quelle fonctionnalité multisaut fait passer le trafic par plusieurs nœuds ? → WireGuard Multihop

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : Mullvad ne demande jamais d'adresse e-mail ; les comptes sont identifiés uniquement par un numéro généré.

7 Question 7

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Des proxys SOCKS5 peuvent être configurés à l'intérieur des tunnels Mullvad.

8 Question 8

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : Mullvad possède certains serveurs mais loue aussi des serveurs dédiés auprès de fournisseurs.

9 Question 9

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Le Network Kill Switch est toujours actif par défaut.

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les paiements en espèces envoyés par courrier ne sont absolument pas remboursables.

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (8 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

B 1. WIREGUARD	D 2. MULTI-SAUT	G 3. UNIQUEMENT EN RAM	A 4. KILL SWITCH
H 5. SANS JOURNAUX	C 6. PROXY SOCKS5	E 7. POST-QUANTIQUE	F 8. FUITES DNS

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 WIREGUARD	2 MULTI-HOP	3 RAM UNIQUEMENT	4 KILL SWITCH
5 SANS JOURNAUX	6 SOCKS5	7 POST-QUANTIQUE	8 FUITES DNS

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 F – PROXYSOCKS	2 G – POSTQUANTIQUE	3 A – WIREGUARD	4 C – RAMUNIQUEMENT
5 D – KILLSWITCH	6 B – MULTIHOP	7 H – FUITESDNS	8 E – SANSJOURNAUX

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer WIREGUARD, MULTI-SAUT et UNIQUEMENT EN RAM avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

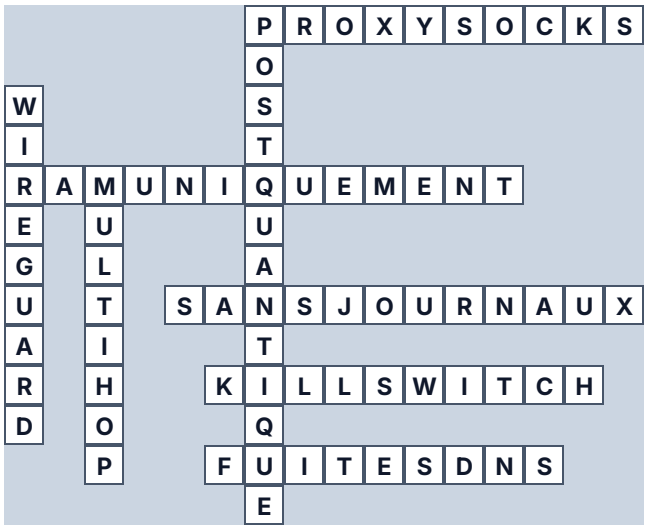
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

S	W	G	U	V	F	W	P	H	Y	N	U	H	V	M
X	K	E	L	M	F	N	O	K	U	J	G	G	R	W
U	F	S	R	D	Z	D	S	U	Q	T	J	Z	H	M
A	S	F	N	V	C	A	T	R	U	B	V	M	F	O
N	P	U	R	Z	P	D	Q	T	Y	T	Y	S	R	F
R	P	O	H	I	T	L	U	M	P	D	V	J	W	P
U	N	J	V	N	D	R	A	U	G	E	R	I	W	R
O	H	C	M	B	P	V	N	W	B	T	W	R	H	O
J	D	E	B	T	U	K	T	X	E	J	R	Z	X	X
S	I	K	M	H	C	T	I	W	S	L	L	I	K	Y
N	R	A	M	U	N	I	Q	U	E	M	E	N	T	S
A	X	E	M	R	M	X	U	U	P	V	C	T	S	O
S	P	V	F	Z	I	I	E	J	U	Q	A	D	Z	C
N	N	D	B	R	W	F	R	J	M	V	K	X	M	K
Q	F	U	I	T	E	S	D	N	S	W	J	K	L	S

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

1 horizontal: PROXYSOCKS Protocole de proxy interne (SOCKS5) utilisé pour isoler les applications clientes (10 lettres)

3 horizontal: RAMUNIQUEMENT Matériel serveur à mémoire volatile qui ne conserve aucune donnée au redémarrage (13 lettres)

5 horizontal: SANSJOURNAUX Norme de non-conservation des données vérifiée par des audits indépendants (12 lettres)

6 horizontal: KILLSWITCH Fonction de sécurité qui coupe le trafic lorsque le VPN se déconnecte (10 lettres)

7 horizontal: FUITESDNS Exposition des destinations des requêtes DNS hors du tunnel VPN (9 lettres)

VERTICALEMENT

1 vertical: POSTQUANTIQUE Se dit des mécanismes de chiffrement conçus pour résister aux attaques quantiques (13 lettres)

2 vertical: WIREGUARD Protocole de tunnel sécurisé, léger et performant (9 lettres)

4 vertical: MULTIHOP Acheminement du trafic via un nœud serveur d'entrée et un nœud de sortie (8 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. U G E I W A R D R — **WIREGUARD**
2. N N A I M R E Q T E M U U — **RAMUNIQUEMENT**
3. S A R U U N N O X J A S — **SANSJOURNAUX**
4. U U T S N Q E A Q I P O T — **POSTQUANTIQUE**
5. I H U P T M O L — **MULTIHOP**
6. C S L I T K I W H L — **KILLSWITCH**
7. R X P O S C K S Y O — **PROXYSOCKS**
8. S E N F T U S D I — **FUITESDNS**

CORRIGÉ DU DÉFI DU CODE SECRET

"MULLVAD NE DEMANDE NI MOT DE PASSE NI EMAIL"

Corrigé des études de cas

A ÉTUDE DE CAS 1 : INTÉGRATION DE LA RÉSISTANCE QUANTIQUE

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : une société financière doit sécuriser ses transferts de fichiers contre un futur déchiffrement quantique.
- Stratégie et solution recommandées : déployer des tunnels WireGuard résistants au quantique à l'aide de clés prépartagées post-quantiques.

B ÉTUDE DE CAS 2 : ROUTAGE DISCRET POUR L'ENQUÊTE

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un enquêteur veut faire passer son trafic par un double routage pour masquer son point d'entrée.
- Stratégie et solution recommandées : activer la fonction WireGuard Multihop de Mullvad pour enchaîner des nœuds d'entrée et de sortie.