Nom : _____ Date : _____ Note : _____

Comment choisir un VPN
Fiche de travail

Évaluation des fournisseurs de VPN, des normes de sécurité, des audits et des politiques de journalisation

APERÇU DE L'APPRENTISSAGE : VPN

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 les principes fondamentaux des réseaux privés virtuels (VPN). Vous étudierez comment les tunnels chiffrés sécurisent vos données, comment fonctionnent les protocoles réseau et comment repérer et limiter les fuites de données personnelles.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez les notions et protocoles VPN.**
- [ ] **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 VPN

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

Votre parcours d'apprentissage : VPN

- Évaluer la juridiction des fournisseurs et leurs politiques sans journaux pour la confidentialité.
- Comparez la vitesse des protocoles de tunnelisation comme WireGuard et OpenVPN.
- Analysez les fonctions de sécurité comme les kill switches et les nœuds de serveurs RAM uniquement.
- Identifier les audits de sécurité indépendants et les formules tarifaires lors du choix.
- Choisissez les emplacements de serveurs en fonction de vos besoins de vitesse et de déblocage géographique.

CONSIGNES DE LA FICHE DE SÉLECTION

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 au choix d'une infrastructure VPN sécurisée. Terminez par l'activité bonus Réflexion rapide.

CHOISIR UN VPN (INTRODUCTION)

Pour choisir le bon VPN, il faut dépasser les arguments marketing. Un fournisseur fiable doit avoir une politique de non-journalisation éprouvée, des protocoles de chiffrement sûrs et des clients open source. En évaluant les fonctions de sécurité, la juridiction et les performances de vitesse, vous pouvez choisir un VPN adapté à vos besoins de protection numérique.

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

Point de contrôle 1 : Défi QCM

1. Quel est le facteur clé dans le choix d'un fournisseur de VPN sécurisé ?

- A. Le nombre de pays où se trouvent des serveurs
- B. Une politique sans journaux auditée de manière indépendante
- C. Le forfait mensuel le moins cher
- D. Parrainages publicitaires tape-à-l'œil

2. Quel protocole VPN offre le meilleur équilibre entre vitesse et facilité d'audit ?

- A. PPTP (obsolète)
- B. L2TP/IPSec
- C. OpenVPN en TCP uniquement
- D. WireGuard

3. Pourquoi les utilisateurs devraient-ils éviter les VPN gratuits pour les activités sensibles ?

- A. Ils sont interdits aux États-Unis
- B. Ils vendent souvent votre historique de navigation
- C. Ils ne prennent pas en charge la navigation web de base
- D. Ils nécessitent un matériel spécial pour se connecter

4. Que détermine la juridiction légale d'origine d'un fournisseur ?

- A. La vitesse de la connexion au serveur
- B. Les types d'appareils pris en charge
- C. Les lois locales régissant la conservation des données et les mandats de perquisition
- D. Le thème visuel de l'application cliente

5. Quel est le but principal de la fonction « kill switch » d'un client VPN ?

- A. Bloquer l'accès à Internet si la connexion VPN tombe
- B. Supprimer toutes les applications installées sur l'appareil
- C. Pour doubler la vitesse de la connexion au serveur
- D. Pour redémarrer le système d'exploitation en cas d'inactivité

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Un VPN protège votre appareil contre le téléchargement de logiciels malveillants et de fichiers infectés par des virus.

- ○ Vrai
- ○ Faux

7 Question 7

7. Des audits indépendants de cabinets comme Deloitte vérifient les affirmations d'absence de journaux.

- ○ Vrai
- ○ Faux

8 Question 8

8. Les lois du pays d'origine d'un fournisseur n'ont aucune incidence sur la confidentialité des données des utilisateurs.

- ○ Vrai
- ○ Faux

9 Question 9

9. Le code compact de WireGuard est plus facile à auditer que celui d'OpenVPN.

- ○ Vrai
- ○ Faux

10 Question 10

10. Les VPN gratuits vendent souvent de la publicité ou pistent les utilisateurs pour couvrir les coûts des serveurs.

- ○ 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. Une politique _____ vérifiée de manière indépendante engage un fournisseur VPN à ne pas enregistrer votre historique en ligne.

2. Le protocole moderne _____ offre une grande vitesse et repose sur une base de code très réduite.

3. Une fonction de sécurité appelée _____ interrompt tout le trafic si la connexion VPN tombe soudainement.

4. Évaluer la _____ dont relève un fournisseur permet de savoir s'il est soumis à des traités de surveillance.

5. Sécuriser l'infrastructure avec des _____ aide à empêcher les données utilisateur de persister après un redémarrage.

6. Vérifier une politique de confidentialité à connaissance nulle exige un _____ de sécurité réalisé par des cabinets tiers réputés.

BANQUE DE MOTS DE VOCABULAIRE

AUDIT FIVE EYES JURIDICTION KILL SWITCH SANS JOURNAUX
SERVEURS RAM VPN GRATUIT WIREGUARD

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions sur les réseaux

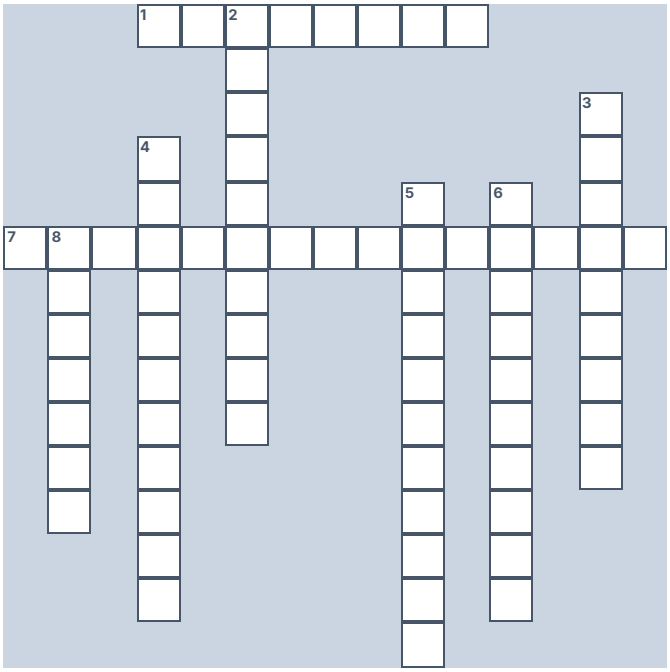
ASSOCIATION DE DÉFINITIONS

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	Service de connexion à haut risque qui se rémunère souvent en journalisant et en vendant les données de navigation.
☐	2. Journaux audités	B	Mécanisme de sécurité qui bloque l'acheminement vers Internet si le tunnel sécurisé se déconnecte.
☐	3. Juridiction	C	Alliance internationale de partage de renseignements entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.
☐	4. Kill switch	D	Infrastructure matérielle fonctionnant en mémoire volatile, de sorte qu'aucune donnée n'est stockée sur disque.
☐	5. Five Eyes (les « Cinq Yeux »)	E	La région géographique qui régit les obligations légales du fournisseur de VPN.
☐	6. VPN gratuit	F	Protocole moderne et rapide reposant sur environ 4 000 lignes de code facilement auditables.
☐	7. Serveurs RAM uniquement	G	Protocole open source mûr et largement audité, dont le code est bien plus volumineux que celui de WireGuard.
☐	8. OpenVPN	H	Engagement de confidentialité vérifié par des sociétés de cybersécurité tierces indépendantes.

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. Alliance internationale de partage de renseignements entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande (8)

7. Promesse de confidentialité vérifiée par des sociétés de cybersécurité tierces indépendantes (15)

VERTICALEMENT

2. Service de connexion à haut risque qui se rémunère souvent en enregistrant et en vendant les données de navigation (10)

3. Protocole moderne et rapide reposant sur environ 4 000 lignes de code facilement auditable (9)

4. Infrastructure matérielle fonctionnant entièrement en mémoire volatile, ce qui empêche le stockage de données (11)

5. Région géographique dont le droit régit les obligations légales du fournisseur VPN (11)

6. Mécanisme de sécurité qui bloque le routage Internet si le tunnel sécurisé se déconnecte (10)

8. Protocole open source mature et largement audité, dont la base de code est bien plus volumineuse que celle de WireGuard (7)

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: Alliance internationale de partage de renseignements entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande (8 lettres):

7 horizontal: Promesse de confidentialité vérifiée par des sociétés de cybersécurité tierces indépendantes (15 lettres):

VERTICALEMENT

2 vertical: Service de connexion à haut risque qui se rémunère souvent en enregistrant et en vendant les données de navigation (10 lettres):

3 vertical: Protocole moderne et rapide reposant sur environ 4 000 lignes de code facilement auditable (9 lettres):

4 vertical: Infrastructure matérielle fonctionnant entièrement en mémoire volatile, ce qui empêche le stockage de données (11 lettres):

5 vertical: Région géographique dont le droit régit les obligations légales du fournisseur VPN (11 lettres):

6 vertical: Mécanisme de sécurité qui bloque le routage Internet si le tunnel sécurisé se déconnecte (10 lettres):

8 vertical: Protocole open source mature et largement audité, dont la base de code est bien plus volumineuse que celle de WireGuard (7 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.

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

LISTE DE MOTS DE VOCABULAIRE

WIREGUARD JOURNAUXAUDITES JURIDICTION KILLSWITCH FIVEEYES
VPNGRATUIT SERVEURSRAM OPENVPN

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. JOURNAUXAUDITES
C. JURIDICTION
D. KILLSWITCH
E. FIVEEYES
F. VPNGRATUIT
G. SERVEURSRAM
H. OPENVPN

	DÉFINITIONS ET CHAMPS D'ASSOCIATION
	1. Alliance internationale de partage de renseignements entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.
	2. Protocole moderne et rapide reposant sur environ 4 000 lignes de code facilement auditable.
	3. Protocole open source mature et largement audité, dont la base de code est bien plus volumineuse que celle de WireGuard.
	4. Service de connexion à haut risque qui se rémunère souvent en enregistrant et en vendant les données de navigation.
	5. Mécanisme de sécurité qui bloque le routage Internet si le tunnel sécurisé se déconnecte.
	6. Infrastructure matérielle fonctionnant entièrement en mémoire volatile, ce qui empêche le stockage de données.
	7. Région géographique dont le droit régit les obligations légales du fournisseur VPN.
	8. Promesse de confidentialité vérifiée par des sociétés de cybersécurité tierces indépendantes.

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 VPN. Écrivez vos réponses dans les champs à remplir.

1. UGEIWARDR
2. DNUJOIRITCI
3. EIFEYSEV
4. RAMURERSSEV
5. UDRJTAUASUIXOEN
6. CSLITKIWHL
7. PGVTAUITRN
8. PNNOPVE

Activité bonus : Réflexion rapide

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

1	Choses qu'un VPN peut cacher			
2	Choses qui comptent plus que le prix			
3	Endroits où lire des avis sur les VPN			
4	Choses contre lesquelles un VPN ne peut pas vous protéger			
5	Questions à poser à l'équipe commerciale d'un VPN			
6	Choses que votre fournisseur d'accès à Internet peut voir			
7	Points de votre liste de contrôle pour choisir un VPN			
8	Endroits où vous utiliseriez un VPN			
9	Signaux d'alerte chez un fournisseur de VPN			
10	Mots liés à la vie privée			
11	Choses que vous testeriez en premier			
12	Engagements d'un bon fournisseur de VPN			
13	Raisons d'utiliser un VPN en voyage			
14	Appareils pouvant utiliser un VPN			
15	Idées reçues sur les VPN			

Point de contrôle 8 : Études de cas sur les VPN

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

SARAH (ÉTUDIANTE AU CAFÉ)

👩‍💻 "Salut ! Je suis au Coffee & Bytes. Il y a un réseau public non sécurisé appelé 'Free_Wi-Fi_No_Password'. Je veux me connecter à ma messagerie scolaire et envoyer mon devoir, mais j'ai peur des pirates. Quels sont les risques si j'utilise ce réseau sans VPN, et comment un VPN sécurise-t-il mes données ?"

ALEX (ÉTUDIANT VOYAGEUR)

👩‍💻 "Oh non ! Je voyage à l'étranger pour un projet et j'essaie de regarder un documentaire de biologie hébergé sur un serveur de mon pays d'origine. Mais le site affiche : 'Cette vidéo n'est pas disponible dans votre pays.' Pourquoi suis-je bloqué, et comment un VPN peut-il m'aider à le regarder ?"

Point de contrôle 9 : Déchiffrer le code

Pour terminer votre formation au guide de sélection, déchiffrez ce message caché sur le choix d'une infrastructure sécurisée.

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

3	15	13	16	1	18	5	26		22	15	19		18	1	16	16	15	18	20	19
			1	22	5	3		21	14		19	25	19	20	5	13	5			
						19	5	3	21	18	9	19	5							

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 que se posent les clients potentiels sur l'utilisation des réseaux privés virtuels.

Q1: Qu'est-ce qu'un VPN et comment fonctionne-t-il ?

Un réseau privé virtuel (VPN) chiffre votre connexion Internet et fait passer votre trafic par un serveur distant sécurisé. Cela masque votre adresse IP publique et limite ce que les observateurs du réseau local et votre FAI peuvent voir du trafic acheminé par le tunnel VPN.

Q2: Pourquoi devrais-je utiliser un VPN ?

Un VPN protège votre vie privée numérique, sécurise votre connexion sur les réseaux Wi-Fi publics (comme dans les cafés ou les aéroports), peut réduire le bridage lié à l'activité lorsque le FAI ne peut pas identifier le type de trafic chiffré, contourne les restrictions géographiques pour accéder à des contenus du monde entier et aide à sécuriser les ressources de télétravail.

Q3: Un VPN me rend-il complètement anonyme en ligne ?

Non. Même si un VPN masque votre adresse IP et chiffre votre trafic, vous pouvez toujours être pisté via les cookies du navigateur, les comptes actifs (comme Google ou Facebook), l'empreinte du navigateur, ou si votre fournisseur de VPN journalise vos données.

Q4: Un VPN va-t-il ralentir ma connexion Internet ?

Oui, légèrement. Le processus de chiffrement et la distance physique jusqu'au serveur VPN ajoutent de la latence et une surcharge. L'impact varie selon le fournisseur, le protocole, la distance du serveur, l'appareil et les conditions du réseau.

Q5: Comment gagne-t-il de l'argent ?

Examinez le modèle économique. Les abonnements, les offres freemium et la vente de données influencent tous le degré de confiance que vous pouvez accorder à un VPN, et un service qui ne collecte jamais vos données ne peut pas les vendre. Lisez d'abord la politique de confidentialité. [1]

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

Passez en revue les questions et réponses les plus courantes que se posent les clients potentiels sur l'utilisation des réseaux privés virtuels.

Q6: Puis-je utiliser un VPN gratuit ?

Les VPN gratuits peuvent reposer sur la publicité, des fonctionnalités limitées, l'analyse d'utilisation, des plafonds de données ou d'autres modèles de monétisation. Les utilisateurs devraient examiner la politique de confidentialité, la structure de propriété, les audits et le modèle économique du fournisseur avant de l'utiliser.

Q7: Qu'est-ce qu'une politique de « non-conservation des journaux » (no-logs) ?

Une politique sans journaux décrit les données d'activité et de connexion qu'un fournisseur déclare ne pas conserver. Sa portée exacte varie : il convient donc de lire la politique et les conclusions des audits indépendants.

Q8: Comment choisir le meilleur VPN ?

Recherchez des politiques d'absence de journaux auditées, des protocoles robustes (WireGuard, OpenVPN), des emplacements de serveurs sûrs, des vitesses élevées, des serveurs fonctionnant uniquement en RAM, une fonction kill switch et une juridiction en dehors des alliances de partage de renseignements (comme les 5/9/14 Eyes).

Q9: Puis-je utiliser un VPN sur mon téléphone et ma smart TV ?

Oui. Les fournisseurs de VPN modernes proposent des applications dédiées pour iOS, Android, macOS, Windows, Linux et les téléviseurs connectés, ainsi que des configurations pour routeur afin de protéger tous les appareils de votre réseau domestique.

Q10: Qu'est-ce qu'un kill switch ?

Un kill switch est une fonction de sécurité qui déconnecte automatiquement votre appareil d'Internet si la connexion VPN tombe. Cela empêche la fuite de vos données non chiffrées ou de votre véritable adresse IP.

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

Découvrez les aspects techniques et structurels des réseaux privés virtuels et des protocoles de tunnel sécurisés.

Q1: Quelle est la différence entre WireGuard, OpenVPN et IKEv2 ?

WireGuard est un protocole moderne et léger (environ 4 000 lignes de code seulement) qui offre des vitesses élevées et des temps de connexion courts. OpenVPN est un protocole open source très sûr et éprouvé. IKEv2 est excellent pour les appareils mobiles grâce à sa capacité à se reconnecter rapidement lors d'un changement de réseau.

Q2: Qu'est-ce que le double VPN ou routage Multi-Hop ?

Le multi-saut fait passer votre trafic par deux serveurs VPN ou plus, l'un après l'autre. Cela ajoute une seconde couche de chiffrement et aide à garder votre véritable adresse IP cachée du second saut si un serveur est compromis.

Q3: Qu'est-ce qu'une fuite WebRTC et comment un VPN l'empêche-t-il ?

WebRTC est un protocole de navigateur qui peut révéler vos véritables adresses IP locale et publique même lorsqu'un VPN est actif. Les VPN premium bloquent ou falsifient les requêtes WebRTC dans leurs applications pour ordinateur et mobile et dans leurs extensions de navigateur.

Q4: Que sont les serveurs fonctionnant uniquement en RAM et pourquoi sont-ils importants ?

Les serveurs traditionnels écrivent les données sur des disques durs, qui peuvent être saisis ou compromis. Les serveurs RAM uniquement (sans disque) fonctionnent entièrement en mémoire volatile (RAM). Lorsque le serveur redémarre ou est mis hors tension, les données en mémoire sont effacées.

Q5: Comment l'obfuscation contourne-t-elle les blocages de VPN ?

L'obfuscation (ou « VPN furtif ») déguise les paquets du trafic VPN pour qu'ils ressemblent à du trafic Web HTTPS ordinaire (port 443). Cela aide à passer l'inspection approfondie des paquets (DPI) utilisée par les gouvernements ou les réseaux scolaires et professionnels pour bloquer les VPN.

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

Découvrez les aspects techniques et structurels des réseaux privés virtuels et des protocoles de tunnel sécurisés.

Q6: Qu'est-ce que le split tunneling et quand l'utiliser ?

Le tunnel fractionné (split tunneling) vous permet de choisir quelles applications passent par le tunnel VPN chiffré et lesquelles se connectent directement à internet. Utilisez-le pour faire passer les applications bancaires sensibles par le VPN tandis que les jeux locaux se connectent directement, ce qui évite la latence ajoutée par le VPN.

Q7: Comment fonctionne la confidentialité persistante (Perfect Forward Secrecy) ?

La PFS garantit qu'une clé de chiffrement unique et temporaire est générée pour chaque session. Même si une clé privée est compromise à l'avenir, elle ne peut pas servir à déchiffrer les sessions passées ou futures, car celles-ci utilisaient des clés indépendantes.

Q8: Que sont les alliances 5/9/14 Eyes et pourquoi devrais-je m'en soucier ?

La juridiction peut influer sur les procédures juridiques auxquelles un fournisseur peut être confronté, mais le risque concret pour la vie privée dépend aussi des données que le fournisseur conserve, de son architecture technique, de sa structure de propriété, de ses rapports de transparence et de l'historique de ses audits.

Q9: Qu'est-ce que la protection contre les fuites DNS ?

La protection contre les fuites DNS oblige votre appareil à envoyer les requêtes de recherche de sites web (requêtes DNS) aux serveurs DNS privés et chiffrés du VPN plutôt qu'aux serveurs de votre FAI. Cela empêche votre FAI de suivre les sites que vous visitez.

Q10: Pourquoi vérifier qui exploite et qui recommande un VPN ?

La réputation compte. Renseignez-vous sur les propriétaires et les dirigeants de l'entreprise, recherchez des audits publics réalisés par des tiers et vérifiez ce qu'en disent des experts en sécurité indépendants et la presse avant de lui faire confiance. [1]

Partie 11 : 10 faits intéressants et enseignements concrets sur les VPN

Découvrez ces faits et informations concrets et précieux sur l'histoire, le marché et la technologie des VPN.

1. PREMIER PROTOCOLE VPN

PPTP (Point-to-Point Tunneling Protocol), un des premiers protocoles VPN, issu d'un groupe mené par Microsoft dans les années 1990, est aujourd'hui considéré comme non sécurisé ; les VPN modernes utilisent donc WireGuard ou OpenVPN. [1]

2. ÉVALUATION DU MARCHÉ

Le marché mondial des VPN a connu une croissance rapide, portée par les besoins croissants du télétravail et les exigences de sécurité des entreprises.

3. LA RÉVOLUTION WIREGUARD

WireGuard dispose d'un code très épuré, conçu pour l'efficacité, ce qui le rend plus facile à auditer que les protocoles traditionnels pour y rechercher des vulnérabilités. [3]

4. NORMES D'AUDIT STRICTES

Les principaux fournisseurs de VPN font appel à des cabinets comme Deloitte, KPMG ou PwC pour vérifier leurs affirmations de non-journalisation, et à des sociétés de sécurité comme Cure53 pour tester leurs applications et leurs serveurs. [4]

5. ORIGINES DE L'ALLIANCE DES 5 YEUX

Le partenariat de renseignement des Five Eyes, qui réunit les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande, est né de la coopération des Alliés en matière de renseignement d'origine électromagnétique pendant la Seconde Guerre mondiale.

6. INSPECTION APPROFONDIE DES PAQUETS

Les pare-feu avancés utilisent l'inspection approfondie des paquets (DPI) pour analyser les métadonnées des paquets réseau et bloquer les caractéristiques des connexions VPN standard.

7. USAGE EN ENTREPRISE

De nombreuses organisations fournissent un VPN à leurs employés à distance pour accéder aux systèmes internes comme les bases de données, ce qui fait des VPN un outil de sécurité courant en entreprise.

8. VPN DÉCENTRALISÉS

Les VPN décentralisés (dVPN) répartissent le trafic sur un réseau de nœuds gérés par des pairs, ce qui réduit la dépendance envers un fournisseur centralisé unique.

9. ANONYMAT : TOR OU VPN

Un VPN fait passer le trafic par un seul fournisseur, alors que Tor (The Onion Router) l'envoie à travers trois relais bénévoles (garde, intermédiaire, sortie) pour maximiser la confidentialité. [5]

10. COÛT DES VIOLATIONS DE DONNÉES

Associer un VPN à un modèle d'accès Zero Trust, qui vérifie chaque utilisateur et chaque appareil, aide les organisations à protéger leurs données et à limiter les dégâts des violations de données.

Références techniques et sources

Publications citées, spécifications cryptographiques et normes documentaires officielles utilisées dans cette fiche.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

Corrigé : évaluation des fournisseurs de VPN, des normes de sécurité, des audits et des politiques de journalisation

1 **Politique de journalisation auditée** PROTOCOLES — **Bonne réponse : B**

NOTE PÉDAGOGIQUE

Une politique sans journaux auditée de manière indépendante est le moyen le plus pratique de vérifier les promesses de confidentialité « zero knowledge » d'un fournisseur. Un marketing tape-à-l'œil ou de simples déclarations ne suffisent pas. Source : Deloitte Advisory, Cure53 Audit.

2 **Supériorité de WireGuard** LATENCE — **Bonne réponse : D**

NOTE PÉDAGOGIQUE

WireGuard offre un routage des connexions moderne et rapide dans l'espace noyau, avec un code compact (~4 000 lignes), ce qui rend les audits très efficaces. Citation : IETF Protocol RFC, WireGuard Project.

3 **Question 3** — **Bonne réponse : B**

NOTE PÉDAGOGIQUE

Les VPN gratuits doivent tout de même payer leurs serveurs, et la FTC avertit que certaines applications VPN partagent les données des utilisateurs avec des tiers, par exemple pour diffuser des publicités.

4 **Juridictions légales** CONTRÔLES DU ROUTAGE — **Bonne réponse : C**

NOTE PÉDAGOGIQUE

La juridiction détermine si le VPN est soumis aux lois de surveillance, aux obligations locales de conservation des données et aux injonctions secrètes des autorités. Source : Privacy Rights Clearinghouse.

5 **Protection par kill switch** CONFIDENTIALITÉ — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Le kill switch coupe immédiatement le routage de l'adaptateur réseau du système si le tunnel tombe, ce qui évite les fuites exposant l'IP réelle et le DNS. Citation : IETF Tunnel RFC.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Limites face aux logiciels malveillants** MASQUAGE D'IP — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Un VPN fournit un canal chiffré sécurisé, mais il n'analyse ni les données ni les fichiers. Un logiciel antivirus est nécessaire pour bloquer les logiciels malveillants. Source : Deloitte Advisory.

7 **Audit indépendant** VITESSES — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les rapports d'audit vérifient la configuration des logiciels des serveurs, la conformité du fonctionnement en RAM uniquement et l'absence de bases de données de journalisation. Source : Deloitte Advisory, Cure53 Audit.

8 **Question 8** — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Les fournisseurs doivent respecter les lois de leur pays d'origine, qui peuvent inclure des règles de conservation des données et des ordres de remise des données qu'ils détiennent.

9 **Taille de la base de code du protocole** PARE-FEU — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Une base de code plus petite réduit la surface d'attaque potentielle et permet aux équipes de sécurité de vérifier plus facilement l'intégrité du protocole. Source : WireGuard Project.

10 **Monétisation par la publicité** SANS JOURNAUX — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Faute de frais d'abonnement, les VPN gratuits comptent sur l'exploitation des données, le profilage du trafic et l'injection de publicités dans le navigateur pour générer des revenus. Citation : EDRi Retention Guidelines.

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 (6 points au total).

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

F 1. WireGuard	H 2. Journaux audités	E 3. Juridiction	B 4. Kill switch
C 5. Five Eyes (les « Cinq Yeux »)	A 6. VPN gratuit	D 7. Serveurs RAM uniquement	G 8. OpenVPN

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 SANS JOURNAUX	2 WIREGUARD	3 KILL SWITCH	4 JURIDICTION
5 SERVEURS RAM	6 AUDIT		

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

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – VPNGRATUIT
5 D – KILLSWITCH	6 G – SERVEURSRAM	7 C – JURIDICTION	8 B – JOURNAUXAUDITES

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer WireGuard, Journaux audités et Juridiction 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.

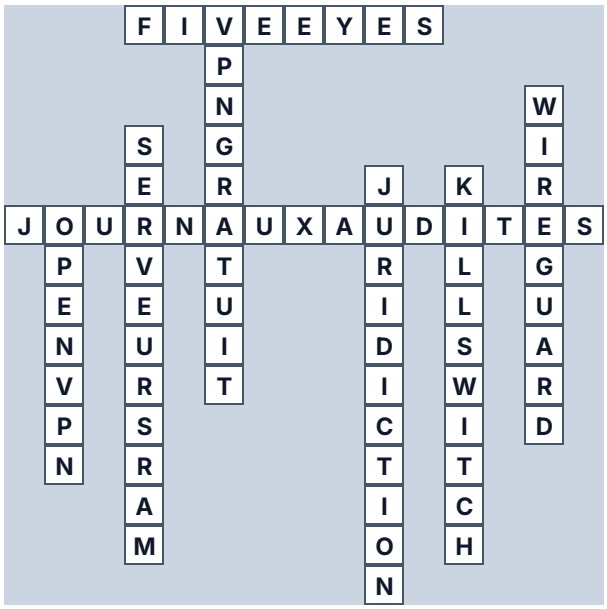
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

1 horizontal: FIVEEYES Alliance internationale de partage de renseignements entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande (8 lettres)

7 horizontal: JOURNAUXAUDITES Promesse de confidentialité vérifiée par des sociétés de cybersécurité tierces indépendantes (15 lettres)

VERTICALEMENT

2 vertical: VPNGRATUIT Service de connexion à haut risque qui se rémunère souvent en enregistrant et en vendant les données de navigation (10 lettres)

3 vertical: WIREGUARD Protocole moderne et rapide reposant sur environ 4 000 lignes de code facilement auditable (9 lettres)

4 vertical: SERVEURSRAM Infrastructure matérielle fonctionnant entièrement en mémoire volatile, ce qui empêche le stockage de données (11 lettres)

5 vertical: JURIDICTION Région géographique dont le droit régit les obligations légales du fournisseur VPN (11 lettres)

6 vertical: KILLSWITCH Mécanisme de sécurité qui bloque le routage Internet si le tunnel sécurisé se déconnecte (10 lettres)

8 vertical: OPENVPN Protocole open source mature et largement audité, dont la base de code est bien plus volumineuse que celle de WireGuard (7 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. UGEIWARDR — **WIREGUARD**
2. DNUJOIRITCI — **JURIDICTION**
3. EIFEYSEV — **FIVEEYES**
4. RAMURERSSEV — **SERVEURSRAM**
5. UDRJTAUASUIXOEN — **JOURNAUXAUDITES**
6. CSLITKIWHL — **KILLSWITCH**
7. PGVTAUITRN — **VPNGRATUIT**
8. PNNOPVE — **OPENVPN**

CORRIGÉ DU DÉFI DU CODE SECRET

"COMPAREZ VOS RAPPORTS AVEC UN SYSTEME SECURISE"

Corrigé des études de cas

A Scénario A : sécurité sur un réseau public

INTERCEPTION ET CHIFFREMENT

Le dilemme de Sarah

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Risques : interception de paquets (packet sniffing), interception de données et attaques de l'homme du milieu. Une personne connectée au même réseau du café pourrait capturer ses identifiants de connexion ou son fichier de devoirs.
- Protection VPN : chiffre le contenu des paquets réseau, ce qui rend le trafic du tunnel intercepté illisible pour les espions passifs du réseau local lorsque le VPN est correctement configuré.

B Scénario B : accéder à des ressources bloquées

GÉOBLOCAGE ET IPS

Le dilemme d'Alex

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Pourquoi c'est bloqué : le service de streaming utilise le géoblocage, qui associe l'adresse IP locale du voyageur à son pays physique et la bloque en fonction des licences territoriales.
- Comment le VPN aide : il masque sa localisation réelle en acheminant le trafic par un serveur situé dans son pays d'origine. Le site voit une IP de ce pays et autorise l'accès.