Nom : _____ Date : _____ Note : _____

Comment masquer votre adresse IP Fiche de travail

Masquer les adresses IP, dissimuler sa localisation, proxy, Tor et prévention des fuites DNS/WebRTC

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

- Expliquer comment fonctionnent les adresses IP et comment elles révèlent la localisation.
- Comparez les proxys, Tor et les VPN pour masquer les adresses réseau.
- Identifier les méthodes permettant de détecter et de prévenir les fuites DNS et WebRTC.
- Comprendre comment les sites web suivent les utilisateurs grâce à leur IP publique.
- Évaluer le routage multi-saut et les tunnels chiffrés pour la protection de l'adresse IP.

CONSIGNES DE LA FICHE DE TRAVAIL SUR LA PROTECTION DE L'IP

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 masquage de votre adresse IP et à la prévention des fuites. Terminez par l'activité bonus Réflexion rapide.

MASQUER VOTRE ADRESSE IP (INTRODUCTION)

Votre adresse IP est une adresse postale numérique qui révèle votre localisation physique et vos habitudes en réseau. Masquer votre IP est la première ligne de défense contre le pistage en ligne, le profilage ciblé et le blocage géographique. Comprendre comment masquer votre adresse de façon sécurisée aide à protéger votre vie privée en ligne.

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

Point de contrôle 1 : Défi QCM

1. Que révèle l'adresse IP publique d'un appareil aux sites web que vous visitez ?

- A. Le numéro de carte de crédit de l'utilisateur
- B. Votre localisation approximative et le nom de votre FAI
- C. L'arborescence complète des fichiers locaux
- D. Les paramètres de langue du clavier

2. Quelle méthode masque votre IP et chiffre tout le trafic à l'échelle du système ?

- A. Un proxy web standard
- B. Effacer les cookies de votre navigateur
- C. Un réseau privé virtuel (VPN)
- D. Désactiver votre pare-feu natif

3. Quelle est une limite majeure, en matière de confidentialité, de l'utilisation d'un proxy web gratuit ?

- A. Il ne chiffre pas le trafic de données sur les réseaux publics
- B. Il nécessite l'installation d'un système d'exploitation externe
- C. Il est totalement illégal aux États-Unis
- D. Il nécessite une connexion par ligne téléphonique dédiée

4. Comment le réseau Tor offre-t-il un haut niveau d'anonymat aux utilisateurs ?

- A. En accélérant les vitesses de connexion
- B. En faisant passer le trafic par trois relais gérés par des bénévoles
- C. En enregistrant votre nom dans une base de données mondiale
- D. En limitant l'accès aux seules agences gouvernementales

5. Qu'est-ce qu'une fuite DNS ?

- A. Une erreur d'envoi d'e-mail à la mauvaise adresse
- B. Lorsque les requêtes DNS contournent le tunnel VPN et partent vers le FAI
- C. Une panne matérielle de l'alimentation du routeur local
- D. Une mise à jour du pilote de la carte réseau locale

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Un serveur proxy chiffre le trafic d'arrière-plan du système d'exploitation comme un VPN.

- ○ Vrai
- ○ Faux

7 Question 7

7. Le routage Tor est très sûr, mais réduit la vitesse de navigation.

- ○ Vrai
- ○ Faux

8 Question 8

8. Les fuites WebRTC peuvent exposer votre véritable IP pendant une session VPN active.

- ○ Vrai
- ○ Faux

9 Question 9

9. Avec un VPN activé et sans fuite, votre FAI ne peut pas voir quels sites web vous visitez.

- ○ Vrai
- ○ Faux

10 Question 10

10. Masquer votre adresse IP bloque le pistage par empreinte du navigateur.

- ○ 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. Un contournement du tunnel sécurisé qui expose vos requêtes de domaine s'appelle une _____ .

2. Les API de communication _____ des navigateurs peuvent accidentellement divulguer votre adresse IP réelle.

3. Un _____ redirige le trafic du navigateur mais ne chiffre pas le contenu des paquets.

4. Le chiffrement multicouche du réseau _____ offre un haut niveau d'anonymat.

5. Votre _____ publique est attribuée par votre opérateur et révèle votre région.

6. Le contournement des blocages régionaux de contenus multimédias passe par le masquage de la _____ .

BANQUE DE MOTS DE VOCABULAIRE

ADRESSE IP | FUITE DNS | LOCALISATION | MASQUAGE | PROXY WEB | TOR | TUNNEL VPN | WEBRTC

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions sur les réseaux

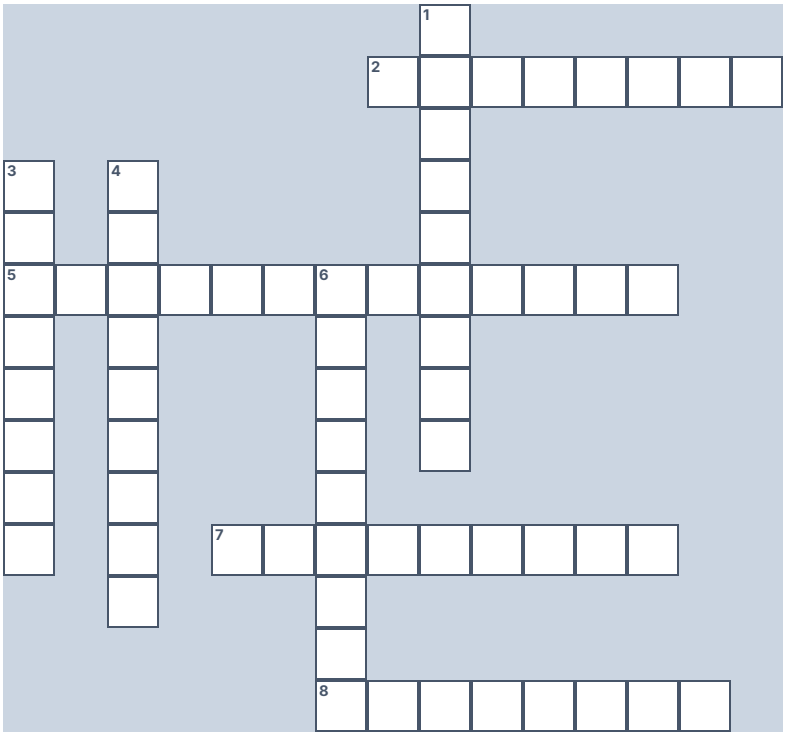
ASSOCIATION DE DÉFINITIONS

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. Adresse IP	A	Chiffre tout le trafic d'un appareil et le fait passer par un serveur VPN.
☐	2. Tunnel VPN	B	Fait passer les données par trois serveurs bénévoles, en chiffrant des couches à chaque étape.
☐	3. Réseau Tor	C	Acheminement de la connexion par un serveur situé dans un autre pays pour contourner les blocages géographiques.
☐	4. Proxy web	D	Étiquette numérique unique identifiant l'interface d'un appareil sur Internet.
☐	5. Fuite DNS	E	Redirige le trafic du navigateur au niveau de la couche application, sans chiffrement au niveau du système.
☐	6. API WebRTC	F	L'enregistrement par votre opérateur télécom des destinations de votre trafic Internet non chiffré.
☐	7. Masquage de la localisation	G	Requêtes résolues hors du tunnel VPN, ce qui expose les domaines visités au FAI.
☐	8. Suivi par le FAI	H	Fonction du navigateur pour la voix et la vidéo qui peut contourner les tunnels et exposer les adresses IP réelles.

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

2. Requêtes résolues hors du tunnel VPN, qui exposent les domaines visités au FAI (8)

5. Enregistrement par votre opérateur des destinations du trafic Internet non chiffré (13)

7. Achemine les données via trois serveurs bénévoles en ajoutant une couche de chiffrement à chaque étape (9)

8. Redirige le trafic du navigateur au niveau de la couche application, sans chiffrement au niveau du système (8)

VERTICALEMENT

1. Chiffre tout le trafic d'un appareil et l'achemine via un serveur VPN (9)

3. Acheminement de la connexion via un serveur d'un autre pays pour contourner les blocages géographiques (8)

4. Fonction du navigateur pour la voix et la vidéo qui peut contourner les tunnels et exposer les vraies adresses IP (9)

6. Identifiant numérique unique désignant l'interface d'un appareil sur Internet (9)

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

2 horizontal: Requêtes résolues hors du tunnel VPN, qui exposent les domaines visités au FAI (8 lettres):

5 horizontal: Enregistrement par votre opérateur des destinations du trafic Internet non chiffré (13 lettres):

7 horizontal: Achemine les données via trois serveurs bénévoles en ajoutant une couche de chiffrement à chaque étape (9 lettres):

8 horizontal: Redirige le trafic du navigateur au niveau de la couche application, sans chiffrement au niveau du système (8 lettres):

VERTICALEMENT

1 vertical: Chiffre tout le trafic d'un appareil et l'achemine via un serveur VPN (9 lettres):

3 vertical: Acheminement de la connexion via un serveur d'un autre pays pour contourner les blocages géographiques (8 lettres):

4 vertical: Fonction du navigateur pour la voix et la vidéo qui peut contourner les tunnels et exposer les vraies adresses IP (9 lettres):

6 vertical: Identifiant numérique unique désignant l'interface d'un appareil sur Internet (9 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.

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

LISTE DE MOTS DE VOCABULAIRE

ADRESSEIP TUNNELVPN RESEAUTOR PROXYWEB FUITEDNS APIWEBRTC MASQUAGE SUIVIPARLEFAI

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. ADRESSEIP
B. TUNNELVPN
C. RESEAUTOR
D. PROXYWEB
E. FUITEDNS
F. APIWEBRTC
G. MASQUAGE
H. SUIVIPARLEFAI

DÉFINITIONS ET CHAMPS D'ASSOCIATION
1. Redirige le trafic du navigateur au niveau de la couche application, sans chiffrement au niveau du système.
2. Acheminement de la connexion via un serveur d'un autre pays pour contourner les blocages géographiques.
3. Fonction du navigateur pour la voix et la vidéo qui peut contourner les tunnels et exposer les vraies adresses IP.
4. Identifiant numérique unique désignant l'interface d'un appareil sur Internet.
5. Achemine les données via trois serveurs bénévoles en ajoutant une couche de chiffrement à chaque étape.
6. Enregistrement par votre opérateur des destinations du trafic Internet non chiffré.
7. Requêtes résolues hors du tunnel VPN, qui exposent les domaines visités au FAI.
8. Chiffre tout le trafic d'un appareil et l'achemine via un serveur VPN.

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. SSEDAEIPR
2. RROEEUTAS
3. TUFEDSNI
4. QGEAUMAS
5. VEUNLNTPN
6. EBXWPYRO
7. BATCRWPEI
8. LIIPFRISAUAEV

Activité bonus : Réflexion rapide

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

1	Raisons d'utiliser un VPN en voyage			
2	Navigateurs que vous connaissez			
3	Choses qu'un VPN peut cacher			
4	Mots liés à la vie privée			
5	Mots de cette fiche que vous voulez retenir			
6	Choses qu'un site web peut deviner à partir de votre IP			
7	Chiffres ou symboles d'une adresse IP			
8	Idées reçues sur les VPN			
9	Services VPN que vous connaissez			
10	Choses que votre fournisseur d'accès à Internet peut voir			
11	Engagements d'un bon fournisseur de VPN			
12	Choses qui peuvent faire fuiter votre véritable IP			
13	Raisons de masquer votre localisation			
14	Façons de masquer votre adresse IP			
15	Appareils pouvant utiliser un 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 sur le masquage d'IP, déchiffrez ce message secret sur l'effacement de vos traces numériques.

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	1	19	17	21	5	26		22	15	20	18	5		1	4	18	5	19	19	5
1	22	5	3		21	14		19	25	19	20	5	13	5		3	1	3	8	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 proxy web masque-t-il mon adresse IP ?

Oui, mais uniquement pour le trafic qui passe par lui, généralement celui de votre navigateur. La plupart des proxys web ne chiffrent pas vos données : votre FAI ou l'opérateur du réseau peut donc toujours voir ce que vous envoyez et recevez.

Q5: Masquer mon IP est-il légal ?

Dans de nombreux pays, oui, mais certains restreignent ou interdisent les VPN et les autres outils servant à masquer une adresse IP. Masquer votre IP ne rend jamais légal un acte illégal : vérifiez donc la législation locale avant d'en utiliser un.

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: Tor masque-t-il mon IP ?

Oui. Tor fait passer votre trafic par trois relais bénévoles (garde, intermédiaire et sortie), de sorte que les sites web voient l'adresse du relais de sortie, et qu'aucun relais ne sait à la fois qui vous êtes et où vous allez. [1]

Q7: Que révèle mon IP ?

Votre IP publique révèle généralement votre FAI et une localisation approximative, comme votre pays ou votre ville. Les sites peuvent aussi s'en servir pour relier vos visites entre elles et appliquer des blocages géographiques.

Q8: Comment vérifier qu'elle est masquée ?

Connectez-vous à votre VPN, puis rendez-vous sur un site de vérification d'IP et lancez des tests de fuite DNS et WebRTC. L'IP et les serveurs DNS affichés doivent appartenir au VPN, pas à votre FAI. Si votre IP réelle apparaît, activez la protection contre les fuites.

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: Pourquoi les sites Web peuvent-ils encore me suivre après que j'ai masqué mon adresse IP ?

Masquer votre IP n'empêche pas l'empreinte du navigateur. Les traqueurs peuvent combiner des éléments comme la résolution de votre écran, les polices installées et les paramètres du navigateur pour créer un identifiant, et les cookies ou les comptes connectés peuvent aussi vous identifier : utilisez donc également un navigateur axé sur la confidentialité. [3]

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: Le trafic IPv6 peut-il divulguer ma véritable adresse IP ?

Oui, si votre VPN ne fait passer que l'IPv4 dans le tunnel. Votre appareil peut alors envoyer du trafic IPv6 hors du tunnel, exposant une adresse attribuée par votre FAI. Utilisez un VPN qui fait passer l'IPv6 dans le tunnel ou le bloque, et vérifiez-le avec un test de fuite IPv6.

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: Le split tunneling expose-t-il ma véritable adresse IP ?

Oui, pour les applications que vous excluez. Le trafic envoyé hors du tunnel utilise votre véritable IP, et la RFC 8828 indique que WebRTC peut révéler l'adresse du FAI sous un VPN à tunnel fractionné, sauf si le navigateur le limite. [2]

Q7: Qu'est-ce qu'une adresse IP partagée et en quoi aide-t-elle la confidentialité ?

Avec une IP partagée, de nombreux utilisateurs du VPN apparaissent en ligne avec la même adresse au même moment. Il est alors bien plus difficile pour un site web de relier une visite précise à vous qu'avec une IP dédiée utilisée par vous seul.

Q8: Mon FAI peut-il voir que j'utilise un VPN pour masquer mon IP ?

Généralement, oui. Votre FAI peut voir que vous vous connectez à l'adresse IP d'un serveur VPN, à quel moment et quelle quantité de données vous envoyez, mais pas les sites web que vous consultez ni le contenu du tunnel chiffré.

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: Vaut-il mieux un proxy ou un VPN pour masquer mon IP ?

Un VPN est généralement préférable. Il cache votre adresse IP pour toutes les applications de l'appareil et chiffre le trafic, alors qu'un proxy web ne couvre généralement que le navigateur et n'ajoute souvent aucun chiffrement.

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.

2. EMPREINTE NUMÉRIQUE (FINGERPRINTING)

Masquer votre IP n'empêche pas l'empreinte du navigateur (fingerprinting), qui peut vous identifier à partir d'éléments comme la résolution d'écran et les polices installées. [3]

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.

4. EXPOSITION DE L'ADRESSE VIA WEBRTC

La RFC 8828 avertit que WebRTC peut découvrir à la fois l'adresse publique d'un VPN et l'adresse du FAI sur laquelle le VPN fonctionne, sauf si le navigateur le limite. [2]

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. RÉUTILISATION DES CIRCUITS TOR

Tor réutilise le même circuit pendant environ dix minutes puis en construit un nouveau, ce qui rend votre activité de navigation plus difficile à relier. [1]

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. [1]

10. PROXYS ET TUNNELS VPN

Un proxy web modifie l'adresse IP qu'un site voit pour le trafic de votre navigateur, mais contrairement à un VPN, il ne chiffre généralement pas ce trafic et ne couvre pas les autres applications de votre appareil. [5]

Références techniques et sources

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

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] 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

Corrigé : masquer son adresse IP, dissimuler sa localisation, proxy, Tor et prévention des fuites DNS/WebRTC

1 Question 1

Bonne réponse : B

NOTE PÉDAGOGIQUE

Que révèle l'adresse IP publique d'un appareil aux sites web que vous visitez ? → Votre localisation approximative et le nom de votre FAI

2 Chiffrement du système VPN

LATENCE

Bonne réponse : C

NOTE PÉDAGOGIQUE

Contrairement aux proxys qui ne redirigent que le trafic du navigateur, un VPN crée un tunnel chiffré à l'échelle du système, qui protège les applications en arrière-plan, les jeux et les requêtes du système d'exploitation. Citation : Tor Project Relays, W3C WebRTC API.

3 Absence de chiffrement du proxy

SÉCURITÉ WI-FI

Bonne réponse : A

NOTE PÉDAGOGIQUE

Les proxys web se contentent de transférer le trafic du navigateur sans chiffrer le contenu des paquets, si bien que votre opérateur réseau ou votre FAI peut toujours suivre le contenu de votre trafic. Citation : IETF Proxy Vulnerabilities.

4 Question 4

Bonne réponse : B

NOTE PÉDAGOGIQUE

Comment le réseau Tor offre-t-il un haut niveau d'anonymat aux utilisateurs ? → En faisant passer le trafic par trois relais gérés par des bénévoles

5 Fuites DNS hors du tunnel

CONFIDENTIALITÉ

Bonne réponse : B

NOTE PÉDAGOGIQUE

Une fuite DNS se produit lorsque les requêtes de résolution de noms de domaine contournent le tunnel VPN et vont directement aux résolveurs de votre FAI, ce qui expose la liste des domaines visités. Source : DNSSEC Tunnel Testing, EFF Tracking Evasion.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Détails des limites du proxy** MASQUAGE D'IP — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Les proxys fonctionnent au niveau de la couche application et n'ont pas l'intégration système au pilote réseau qu'offre un tunnel VPN. Source : IETF Proxy Vulnerabilities.

7 **Question 7** — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Le relais du trafic par trois relais bénévoles avec un chiffrement en couches ajoute de la latence : Tor est donc généralement plus lent qu'une connexion directe.

8 **Question 8** — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

WebRTC peut révéler les adresses locales et, avec certaines configurations VPN, l'IP publique attribuée par le FAI sous le tunnel (RFC 8828).

9 **Question 9** — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Sans fuite DNS ni WebRTC, le FAI ne voit que du trafic chiffré vers le serveur VPN, et non les sites que vous visitez.

10 **Limites de l'empreinte numérique** SANS JOURNAUX — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

L'empreinte numérique (fingerprinting) cible les caractéristiques de configuration de l'appareil (résolution d'écran, polices, plug-ins), qui restent visibles même lorsque l'IP est masquée. Source : EFF Tracking Evasion.

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

D 1. Adresse IP	A 2. Tunnel VPN	B 3. Réseau Tor	E 4. Proxy web
G 5. Fuite DNS	H 6. API WebRTC	C 7. Masquage de la localisation	F 8. Suivi par le FAI

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 FUITE DNS	2 WEBRTC	3 PROXY WEB	4 TOR
5 ADRESSE IP	6 LOCALISATION		

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

1 D – PROXYWEB	2 G – MASQUAGE	3 F – APIWEBRTC	4 A – ADRESSEIP
5 C – RESEAUTOR	6 H – SUIVIPARLEFAI	7 E – FUITEDNS	8 B – TUNNELVPN

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Adresse IP, Tunnel VPN et Réseau Tor 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.

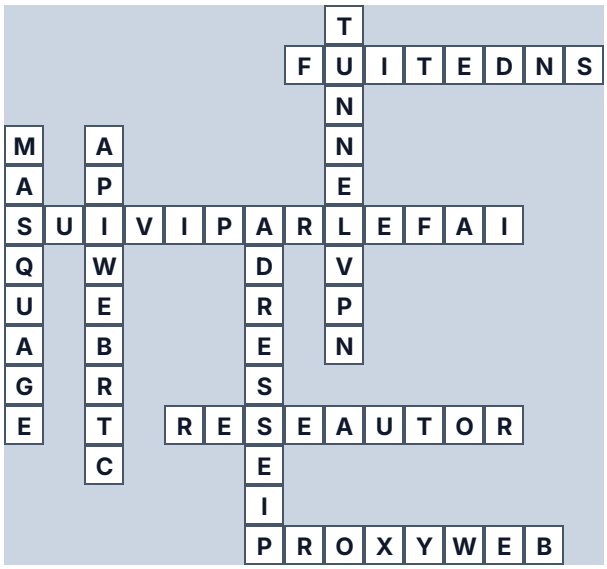
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

2 horizontal: FUITEDNS Requêtes résolues hors du tunnel VPN, qui exposent les domaines visités au FAI (8 lettres)

5 horizontal: SUIVIPARLEFAI Enregistrement par votre opérateur des destinations du trafic Internet non chiffré (13 lettres)

7 horizontal: RESEAUTOR Achemine les données via trois serveurs bénévoles en ajoutant une couche de chiffrement à chaque étape (9 lettres)

8 horizontal: PROXYWEB Redirige le trafic du navigateur au niveau de la couche application, sans chiffrement au niveau du système (8 lettres)

VERTICALEMENT

1 vertical: TUNNELVPN Chiffre tout le trafic d'un appareil et l'achemine via un serveur VPN (9 lettres)

3 vertical: MASQUAGE Acheminement de la connexion via un serveur d'un autre pays pour contourner les blocages géographiques (8 lettres)

4 vertical: APIWEBRTC Fonction du navigateur pour la voix et la vidéo qui peut contourner les tunnels et exposer les vraies adresses IP (9 lettres)

6 vertical: ADRESSEIP Identifiant numérique unique désignant l'interface d'un appareil sur Internet (9 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. SSEDAEIPR — **ADRESSEIP**
2. RROEEUTAS — **RESEAUTOR**
3. TUFEDSNI — **FUITEDNS**
4. QGEAUMAS — **MASQUAGE**
5. VEUNLNTPN — **TUNNELVPN**
6. EBXWPYRO — **PROXYWEB**
7. BATCRWPEI — **APIWEBRTC**
8. LIIPFRISAUAEV — **SUIVIPARLEFAI**

CORRIGÉ DU DÉFI DU CODE SECRET

"MASQUEZ VOTRE ADRESSE AVEC UN SYSTEME CACHE"

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.