Nom : _____ Date : _____ Note : _____

Qu'est-ce qu'un VPN Fiche de travail

Exercices pratiques sur les protocoles réseau, le tunneling et les contrôles de sécurité.

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 la notion de tunneling et d'encapsulation des données.
- Identifier les configurations de protocole standard et les méthodes de chiffrement.
- Analysez le rôle des serveurs et du masquage de l'adresse IP dans les réseaux privés virtuels.
- Comprendre comment les FAI suivent la navigation et comment un VPN l'empêche.
- Distinguer les limites opérationnelles de la topologie de réseau virtuel.

GUIDE « QU'EST-CE QU'UN VPN » : 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 scénarios réels de la section des études de cas. Terminez par l'activité bonus Réflexion rapide.

QU'EST-CE QU'UN VPN ? (INTRODUCTION)

Un réseau privé virtuel est bien plus qu'un simple bouton de confidentialité. C'est un tunnel chiffré qui fait passer votre trafic Internet par un serveur distant. Il cache votre adresse IP, empêche votre FAI de constituer des journaux de vos activités en ligne et sécurise vos données sur les réseaux publics. Comprendre la terminologie est essentiel pour assurer votre sécurité numérique.

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

Point de contrôle 1 : Défi QCM

1. Quelle est la fonction principale d'un réseau privé virtuel (VPN) ?

- A. Accélérer le rendu du navigateur web
- B. Chiffrer les paquets de données et masquer votre IP publique
- C. Pour stocker localement les bases de données de cookies des sites web
- D. Pour remplacer le matériel physique de votre ordinateur

2. Qu'est-ce que le tunneling réseau dans le contexte d'un VPN ?

- A. Supprimer les fichiers journaux réseau en double
- B. Installer des fichiers de stockage de base de données locale
- C. Partager des fichiers avec d'autres ordinateurs locaux
- D. Encapsuler un paquet réseau dans un autre paquet sécurisé

3. Quelle norme de chiffrement est largement utilisée pour protéger le trafic VPN ?

- A. Ancien chiffrement DES
- B. Norme moderne AES-256
- C. Encodage base64 en clair
- D. Chiffrement rot13 standard

4. Quelle partie de votre trafic réseau est chiffrée par un VPN ?

- A. Uniquement les travaux d'impression réseau des appareils locaux
- B. Le chemin physique du câble Ethernet
- C. Toute la partie données utiles (payload) du paquet réseau
- D. Uniquement l'historique de recherche de votre navigateur

5. Que signifie le terme « chiffrement » dans le domaine des réseaux ?

- A. Convertir des données en clair en texte chiffré illisible
- B. Supprimer les anciens enregistrements de communications
- C. Augmenter les limites de débit de votre bande passante locale
- D. Partager publiquement les clés d'accès à la base de données

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Un VPN chiffre votre trafic pour empêcher l'espionnage local sur les Wi-Fi publics.

- ◯ Vrai
- ◯ Faux

7 Question 7

7. Un VPN modifie physiquement la configuration matérielle de votre routeur.

- ◯ Vrai
- ◯ Faux

8 Question 8

8. Les protocoles de tunnelisation enveloppent les paquets de données dans une couche de transport chiffrée.

- ◯ Vrai
- ◯ Faux

9 Question 9

9. Le chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer le trafic.

- ◯ Vrai
- ◯ Faux

10 Question 10

10. Utiliser un VPN rend votre connexion Internet physiquement insensible à toute coupure de courant.

- ◯ 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. Pour sécuriser votre trafic, le VPN enveloppe vos paquets de données dans un autre protocole, un processus appelé _____ .

2. Si vos téléchargements sont lents pendant le streaming, cela peut être dû à une _____ réseau limitée.

3. Un service de streaming disponible uniquement dans un pays donné utilise un _____ pour restreindre l'accès des utilisateurs du reste du monde.

4. Les règles de connexion qui définissent les paramètres de chiffrement et de connexion s'appellent le _____ VPN.

5. Votre ordinateur utilise un _____ local pour surveiller le trafic réseau et bloquer les connexions dangereuses.

6. Lorsque vous vous connectez à un VPN, vos données transitent par un _____ distant qui masque votre IP publique.

BANQUE DE MOTS DE VOCABULAIRE

BANDE PASSANTE CONFIDENTIALITÉ GÉOBLOCAGE OPÉRATEUR PARE-FEU
PROTOCOLE SERVEUR TUNNELISATION

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions sur les réseaux

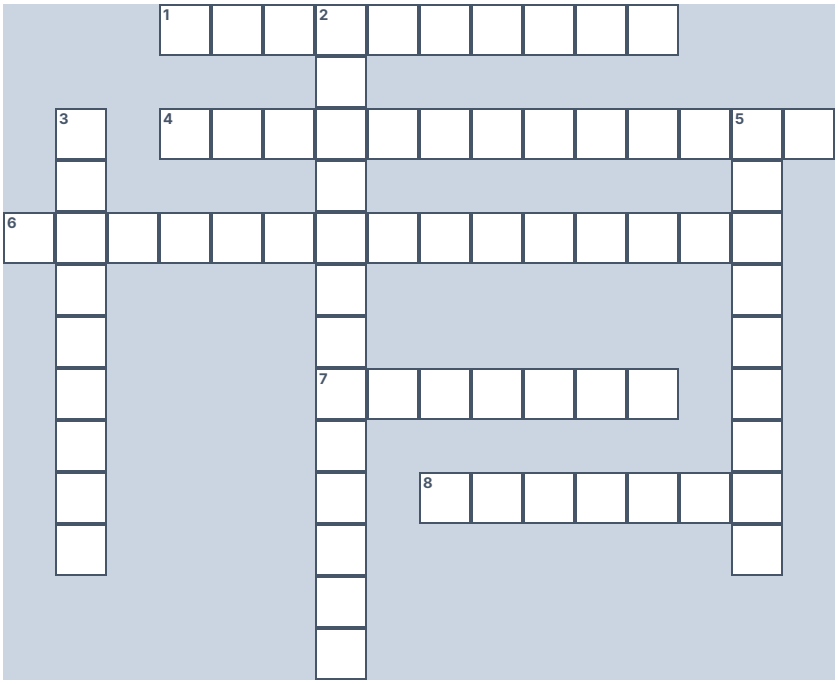
ASSOCIATION DE DÉFINITIONS

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. Tunnelisation	A	Un ordinateur distant qui achemine votre trafic et masque votre adresse IP.
☐	2. Protocole	B	Fournisseur d'accès à Internet qui achemine votre trafic et peut voir l'activité non chiffrée.
☐	3. Bande passante	C	Une restriction qui empêche l'accès au web en fonction de l'emplacement physique.
☐	4. Serveur	D	Un système de sécurité qui surveille et bloque le trafic non autorisé.
☐	5. Géoblocage	E	Un ensemble de règles qui déterminent la manière dont les données sont transmises sur le réseau.
☐	6. Pare-feu	F	Le fait d'être libre de tout pistage ou de toute surveillance publique.
☐	7. Confidentialité	G	Le débit maximal de transfert de données sur une connexion.
☐	8. FAI	H	Encapsulation de paquets de données dans un autre paquet pour un transit sécurisé.

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. Restriction qui empêche l'accès au web en fonction de la localisation physique (10)

4. Encapsulation de paquets de données dans un autre paquet pour un transit sécurisé (13)

6. Fait d'être à l'abri du pistage ou de la surveillance publique (15)

7. Ordinateur distant qui achemine votre trafic et masque votre IP (7)

8. Système de sécurité qui surveille et bloque le trafic non autorisé (7)

VERTICALEMENT

2. Débit maximal de transfert de données sur une connexion (13)

3. Ensemble de règles qui définit comment les données sont transmises sur le réseau (9)

5. Fournisseur d'accès à Internet (FAI), qui enregistre votre trafic s'il n'est pas chiffré (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

1 horizontal: Restriction qui empêche l'accès au web en fonction de la localisation physique (10 lettres):

4 horizontal: Encapsulation de paquets de données dans un autre paquet pour un transit sécurisé (13 lettres):

6 horizontal: Fait d'être à l'abri du pistage ou de la surveillance publique (15 lettres):

7 horizontal: Ordinateur distant qui achemine votre trafic et masque votre IP (7 lettres):

8 horizontal: Système de sécurité qui surveille et bloque le trafic non autorisé (7 lettres):

VERTICALEMENT

2 vertical: Débit maximal de transfert de données sur une connexion (13 lettres):

3 vertical: Ensemble de règles qui définit comment les données sont transmises sur le réseau (9 lettres):

5 vertical: Fournisseur d'accès à Internet (FAI), qui enregistre votre trafic s'il n'est pas chiffré (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.

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

LISTE DE MOTS DE VOCABULAIRE

TUNNELISATION PROTOCOLE BANDEPASSANTE SERVEUR GEOBLOCAGE
PAREFEU CONFIDENTIALITE OPERATEUR

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. TUNNELISATION
B. PROTOCOLE
C. BANDEPASSANTE
D. SERVEUR
E. GEOBLOCAGE
F. PAREFEU
G. CONFIDENTIALITE
H. OPERATEUR

	DÉFINITIONS ET CHAMPS D'ASSOCIATION
	1. Ensemble de règles qui définit comment les données sont transmises sur le réseau.
	2. Restriction qui empêche l'accès au web en fonction de la localisation physique.
	3. Système de sécurité qui surveille et bloque le trafic non autorisé.
	4. Fait d'être à l'abri du pistage ou de la surveillance publique.
	5. Fournisseur d'accès à Internet (FAI), qui enregistre votre trafic s'il n'est pas chiffré.
	6. Encapsulation de paquets de données dans un autre paquet pour un transit sécurisé.
	7. Ordinateur distant qui achemine votre trafic et masque votre IP.
	8. Débit maximal de transfert de données sur une connexion.

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. INAOLUSTTIN EN
2. TEAPNBNAES ASD
3. GOGCELEBAO
4. ETAFOTIDENI LCNI
5. OORECTPLO
6. URESVRE
7. PEFUAER
8. RAUORPTEE

Activité bonus : Réflexion rapide

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

1	Choses qu'une adresse IP peut révéler			
2	Idées reçues sur les VPN			
3	Choses qui circulent sur Internet			
4	Engagements d'un bon fournisseur de VPN			
5	Secrets que vous chiffreriez			
6	Choses contre lesquelles un VPN ne peut pas vous protéger			
7	Façons de repérer un faux réseau Wi-Fi			
8	Mots liés à la vie privée			
9	Appareils pouvant utiliser un VPN			
10	Choses qui se produisent quand vous appuyez sur 'Se connecter'			
11	Endroits où vous utiliseriez un VPN			
12	Raisons d'utiliser un VPN en voyage			
13	Choses de la vie réelle qui ressemblent à un tunnel			
14	Mots de cette fiche que vous voulez retenir			
15	Mots pour expliquer un VPN à un enfant			

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

Un VPN chiffre votre trafic pour le sécuriser. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message de cybersécurité 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

21	14		20	21	14	14	5	12		19	5	3	21	18	9	19	5		
16	18	15	20	5	7	5		22	15	20	18	5		22	9	5			
						16	18	9	22	5	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: L'utilisation d'un VPN est-elle légale ?

L'utilisation d'un VPN est légale dans de nombreux pays, mais certaines juridictions restreignent, réglementent ou bloquent les services VPN. Les utilisateurs doivent vérifier les lois locales en vigueur avant toute utilisation. Pour plus de détails, consultez les guides sur la légalité de VPN.com.

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. [4]

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 le trafic VPN pour qu'il ressemble à du trafic HTTPS ordinaire (port 443). Cela peut l'aider 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: Un VPN peut-il contourner le bridage de la connexion par le FAI ?

Parfois. Un VPN peut aider lorsqu'un FAI ralentit de manière sélective des activités identifiables, mais il ne résoudra pas la congestion, les plafonds de données, les limites de vitesse liées au compte ni une mauvaise qualité du réseau.

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) a été développé par un groupe de fournisseurs comprenant Microsoft et publié sous la forme de la RFC 2637 en juillet 1999 pour prendre en charge les VPN d'accès à distance. [6]

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. [4]

4. NORMES D'AUDIT STRICTES

Les principaux fournisseurs de VPN font appel à des auditeurs externes (comme Cure53 ou PwC) pour réaliser des revues de code indépendantes et vérifier qu'ils n'enregistrent aucune activité des utilisateurs.

5. ORIGINES DE L'ALLIANCE DES 5 YEUX

L'alliance des Five Eyes est issue de l'accord UKUSA de 1946 sur le renseignement d'origine électromagnétique entre les États-Unis et le Royaume-Uni, rejoint plus tard par le Canada, l'Australie et la Nouvelle-Zélande.

6. INSPECTION APPROFONDIE DES PAQUETS

L'inspection approfondie des paquets (DPI) examine le contenu des paquets et les schémas de trafic, pas seulement les en-têtes, et certains pare-feu l'utilisent pour détecter et bloquer les protocoles VPN courants.

7. USAGE EN ENTREPRISE

Une grande partie des employés d'entreprise dans le monde utilisent des VPN sécurisés pour se connecter aux bases de données internes, ce qui en fait une norme de sécurité clé.

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 et sortie), de sorte qu'aucun relais ne connaît les deux extrémités.

10. COÛT DES VIOLATIONS DE DONNÉES

Adopter un modèle d'accès sécurisé zero trust avec un VPN aide les organisations à protéger leur propriété intellectuelle et à atténuer l'impact financier 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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Corrigé : fiche de travail « Qu'est-ce qu'un VPN ? »

1 Fonction principale PROTOCOLES

Bonne réponse : B

NOTE PÉDAGOGIQUE

Le rôle principal d'un VPN est d'établir un tunnel chiffré qui protège les données utiles des paquets et masque l'adresse IP publique de l'utilisateur. Source : IETF Tunnel RFC.

2 Tunnelisation réseau LATENCE

Bonne réponse : D

NOTE PÉDAGOGIQUE

Les protocoles de tunnelisation encapsulent les paquets de données d'origine dans des paquets porteurs externes pour traverser les réseaux publics en toute sécurité. Citation : IETF Tunnel RFC.

3 Question 3

Bonne réponse : B

NOTE PÉDAGOGIQUE

Quelle norme de chiffrement est largement utilisée pour protéger le trafic VPN ? → Norme moderne AES-256

4 Composants chiffrés CONTRÔLES DU ROUTAGE

Bonne réponse : C

NOTE PÉDAGOGIQUE

Un VPN chiffre l'intégralité du segment de données utiles des paquets IP, ce qui préserve la confidentialité du contenu transmis. Source : IETF Tunnel RFC.

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Le chiffrement utilise un algorithme et une clé pour transformer un texte en clair en texte chiffré illisible.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Blocage de l'écoute clandestine** MASQUAGE D'IP — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les tunnels chiffrés garantissent que les charges utiles des paquets restent illisibles pour les acteurs qui interceptent des données sur les réseaux Wi-Fi locaux. Source : Deloitte Advisory.

7 **Modifications matérielles** VITESSES — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Les VPN sont des tunnels réseau logiciels et ne modifient pas physiquement le matériel de votre routeur passerelle. Citation : Cure53 Audit.

8 **Paquets en tunnel** RISQUE D'INTERCEPTION — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

La tunnelisation consiste à envelopper les paquets réseau d'origine dans des en-têtes de transport pour leur acheminement. Citation : IETF Tunnel RFC.

9 **Clés symétriques** PARE-FEU — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

La cryptographie symétrique utilise une clé partagée à la fois pour chiffrer et déchiffrer les flux réseau. Source : WireGuard Project.

10 **Résistance aux coupures de courant** SANS JOURNAUX — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Un VPN ne chiffre que les signaux de connexion actifs; il ne peut pas empêcher les coupures de service causées par des pannes de courant locales. Source : 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

H 1. Tunnelisation	E 2. Protocole	G 3. Bande passante	A 4. Serveur
C 5. Géoblocage	D 6. Pare-feu	F 7. Confidentialité	B 8. FAI

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 TUNNELISATION	2 BANDE PASSANTE	3 GÉOBLOCAGE	4 PROTOCOLE
5 PARE-FEU	6 SERVEUR		

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

1 B – PROTOCOLE	2 E – GEOBLOCAGE	3 F – PAREFEU	4 G – CONFIDENTIALITE
5 H – OPERATEUR	6 A – TUNNELISATION	7 D – SERVEUR	8 C – BANDEPASSANTE

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

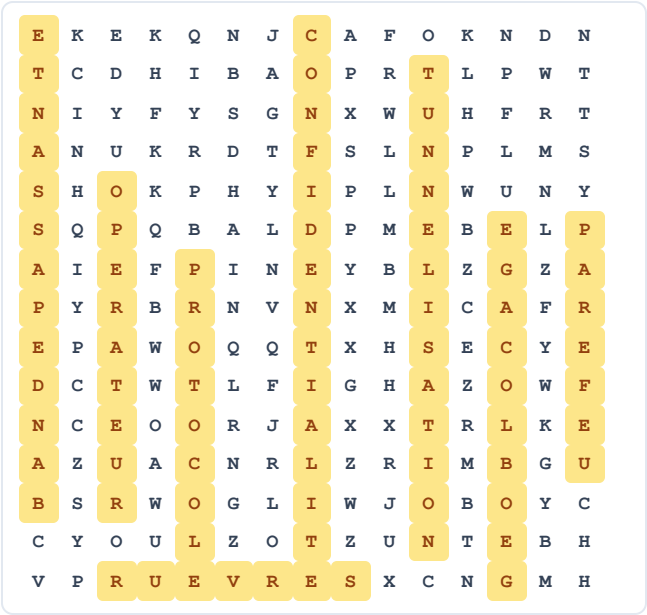
Termes clés :
Vérifiez que les élèves savent expliquer Tunnelisation, Protocole et Bande passante avec leurs propres mots et donner un exemple pour chacun.

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

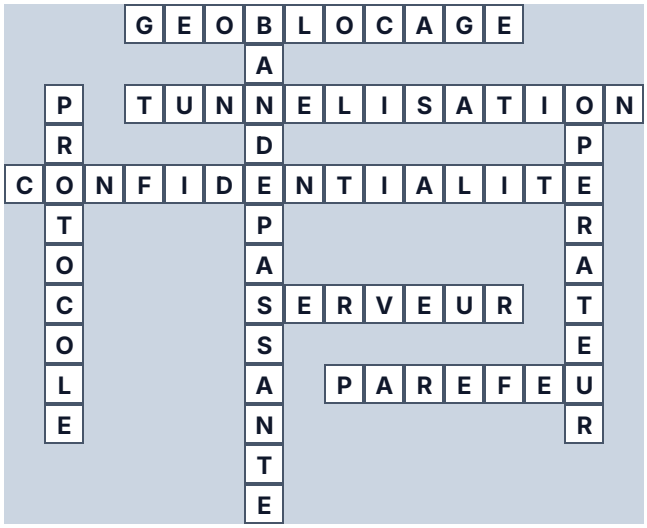
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS



SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

1 horizontal: GEOBLOCAGE Restriction qui empêche l'accès au web en fonction de la localisation physique (10 lettres)

4 horizontal: TUNNELISATION Encapsulation de paquets de données dans un autre paquet pour un transit sécurisé (13 lettres)

6 horizontal: CONFIDENTIALITE Fait d'être à l'abri du pistage ou de la surveillance publique (15 lettres)

7 horizontal: SERVEUR Ordinateur distant qui achemine votre trafic et masque votre IP (7 lettres)

8 horizontal: PAREFEU Système de sécurité qui surveille et bloque le trafic non autorisé (7 lettres)

VERTICALEMENT

2 vertical: BANDEPASSANTE Débit maximal de transfert de données sur une connexion (13 lettres)

3 vertical: PROTOCOLE Ensemble de règles qui définit comment les données sont transmises sur le réseau (9 lettres)

5 vertical: OPERATEUR Fournisseur d'accès à Internet (FAI), qui enregistre votre trafic s'il n'est pas chiffré (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. INAOLUSTTINEN — **TUNNELISATION**
2. TEAPNBNAESASD — **BANDEPASSANTE**
3. GOGCELEBAO — **GEOBLOCAGE**
4. ETAFOTIDENILCNI — **CONFIDENTIALITE**
5. OORECTPLO — **PROTOCOLE**
6. URESVRE — **SERVEUR**
7. PEFUAER — **PAREFEU**
8. RAUORPTEE — **OPERATEUR**

CORRIGÉ DU DÉFI DU CODE SECRET

"UN TUNNEL SECURISE PROTEGE VOTRE VIE PRIVEE"

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.