Nom : _____ Date : _____ Note : _____

Test de Proton VPN

Analyse technique de Proton VPN, dont le siège est à Genève : routage multi-saut Secure Core, filtres DNS NetShield, audits des clients open source et obfuscation par le protocole Stealth.

PRÉSENTATION DE L'APPRENTISSAGE : TEST DE PROTON 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 l'examen technique de Proton VPN. Vous étudierez le routage multi-saut Secure Core, le blocage DNS NetShield, les audits de clients open source et l'obfuscation par le protocole Stealth.

POINTS DE CONTRÔLE DE LA FICHE

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

Ouvrir le guide VPN.com des meilleurs VPN

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

Votre parcours d'apprentissage : Proton VPN

- Analysez l'architecture technique et les normes de chiffrement abordées dans le test de Proton VPN.
- Configurez les paramètres du client pour éviter les fuites d'IP, de DNS et de trafic WebRTC.
- Comparez les protocoles de tunnelisation propriétaires avec les implémentations standard.

CONSIGNES DU TEST DE PROTON VPN

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 nœuds Secure Core et aux blocages NetShield. Terminez par l'activité bonus Réflexion rapide.

NŒUDS SECURE CORE ET CLIENTS OPEN SOURCE (INTRODUCTION)

Proton VPN est réputé pour son routage multihop Secure Core et son bloqueur de contenu DNS NetShield. Ses applications clientes sont entièrement open source et auditées de manière indépendante, et il relève de la juridiction de Genève, en Suisse.

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

Point de contrôle 1 : Défi QCM

1. Quelle fonctionnalité de Proton fait passer le trafic par des pays sûrs ?

- A) Secure Core
- B) NetShield
- C) Tunnel furtif
- D) VPN Accelerator

2. Quelle est la fonction principale de NetShield de Proton VPN ?

- A) Bloqueur de publicités et de logiciels malveillants basé sur le DNS
- B) Chiffrement AES-256 des données utiles
- C) Rotation dynamique des adresses IP
- D) Gestionnaire de redirection multiport

3. Quel protocole de Proton contourne la DPI grâce aux poignées de main TLS ?

- A) Protocole furtif
- B) WireGuard
- C) OpenVPN TCP
- D) L2TP/IPSec

4. Qu'a de particulier le code source du client Proton VPN ?

- A) Entièrement open source et audité publiquement
- B) Binaires propriétaires à code source fermé
- C) Loué à partir de modèles de dépôts open source
- D) Code source fermé avec portails d'accès pour le gouvernement

5. Comment VPN Accelerator de Proton optimise-t-il la vitesse ?

- A) Il utilise le contrôle de congestion BBR et plusieurs cœurs de processeur
- B) Il bascule automatiquement vers du HTTP non chiffré
- C) Il fait passer le trafic par des proxys web publics
- D) Il désactive les règles du pare-feu du client

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. La technologie Secure Core de Proton VPN fait d'abord passer le trafic des utilisateurs par des serveurs physiques renforcés, situés dans des juridictions neutres et hautement sécurisées.

○ Vrai ○ Faux

7 Question 7

7. NetShield fonctionne en interceptant et en bloquant les demandes de connexion vers des domaines de traqueurs et de logiciels malveillants au stade de la requête DNS.

○ Vrai ○ Faux

8 Question 8

8. Le code source des clients Proton VPN est gardé strictement propriétaire pour empêcher la découverte de vulnérabilités.

○ Vrai ○ Faux

9 Question 9

9. Le protocole Stealth encapsule les paquets VPN dans un chiffrement TLS standard pour les rendre impossibles à distinguer du trafic HTTPS.

○ Vrai ○ Faux

10 Question 10

10. Proton VPN relève du droit panaméen et est soumis aux accords de renseignement des 14 Eyes.

○ 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 contourner les pare-feu DPI avancés, les utilisateurs peuvent activer le protocole personnalisé _____ dans les paramètres du client.

2. Les applications clientes de Proton VPN sont développées en code _____ , ce qui permet à des chercheurs externes de les auditer.

3. Le bloqueur DNS dynamique qui filtre les domaines malveillants est connu sous le nom de protection _____ .

4. Pour se défendre contre les attaques par corrélation au niveau du réseau, le trafic passe par des nœuds serveurs _____ .

5. La latence sortante et la perte de paquets sont atténuées par le moteur VPN propriétaire _____ .

6. Le siège juridique de Proton AG se trouve à Genève, en _____ , ce qui protège les métadonnées des comptes.

BANQUE DE MOTS DE VOCABULAIRE

ACCELERATOR KILL SWITCH NETSHIELD OPEN SOURCE SECURE CORE STEALTH SUISSE WIREGUARD

Écrivez vos réponses ici :

1. 2.
3. 4.
5. 6.

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

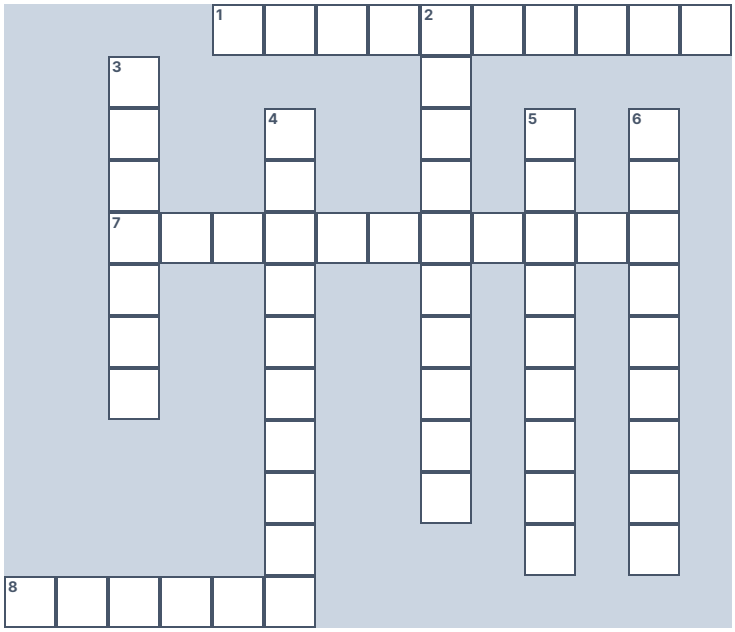
ASSOCIATION DE DÉFINITIONS

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

☐	1. Secure Core	A	Protocole de connexion open source moderne et rapide.
☐	2. NetShield	B	Dépôt de code source d'application lisible publiquement.
☐	3. Stealth	C	Moteur d'optimisation des performances qui répartit les charges du processeur.
☐	4. Accélérateur	D	Bloqueur de publicités, de traqueurs et de logiciels malveillants basé sur le DNS.
☐	5. Open source	E	Juridiction centrale de protection de la vie privée basée en Suisse.
☐	6. Suisse	F	Protocole obfusqué personnalisé conçu pour contourner les filtres DPI.
☐	7. WireGuard	G	Filtre de sécurité qui coupe le trafic réseau en cas de chute.
☐	8. Kill switch	H	Routage multi-saut via des nœuds serveurs hautement sécurisés.

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. Filtre de sécurité qui coupe le trafic réseau en cas de déconnexion (10)

7. Moteur d'optimisation des performances qui répartit les charges de travail du processeur (11)

8. Juridiction centrale en matière de confidentialité, au cœur de l'Europe (6)

VERTICALEMENT

2. Routage multi-hop via des nœuds serveurs hautement sécurisés (10)

3. Protocole obscurci personnalisé, conçu pour contourner les filtres DPI (7)

4. Dépôt de code source de l'application lisible par tous (10)

5. Bloqueur DNS de publicités, de traqueurs et de malwares (9)

6. Protocole de connexion open source moderne à haut débit (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: Filtre de sécurité qui coupe le trafic réseau en cas de déconnexion (10 lettres):

7 horizontal: Moteur d'optimisation des performances qui répartit les charges de travail du processeur (11 lettres):

8 horizontal: Juridiction centrale en matière de confidentialité, au cœur de l'Europe (6 lettres):

VERTICALEMENT

2 vertical: Routage multi-hop via des nœuds serveurs hautement sécurisés (10 lettres):

3 vertical: Protocole obscurci personnalisé, conçu pour contourner les filtres DPI (7 lettres):

4 vertical: Dépôt de code source de l'application lisible par tous (10 lettres):

5 vertical: Bloqueur DNS de publicités, de traqueurs et de malwares (9 lettres):

6 vertical: Protocole de connexion open source moderne à haut débit (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.

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

LISTE DE MOTS DE VOCABULAIRE

SECURECORE NETSHIELD STEALTH ACCELERATOR OPENSOURCE SUISSE
WIREGUARD KILLSWITCH

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	DÉFINITIONS ET CHAMPS D'ASSOCIATION
A. SECURECORE	_____ 1. Moteur d'optimisation des performances qui répartit les charges de travail du processeur.
B. NETSHIELD	_____ 2. Dépôt de code source de l'application lisible par tous.
C. STEALTH	_____ 3. Protocole de connexion open source moderne à haut débit.
D. ACCELERATOR	_____ 4. Juridiction centrale en matière de confidentialité, au cœur de l'Europe.
E. OPENSOURCE	_____ 5. Protocole obscurci personnalisé, conçu pour contourner les filtres DPI.
F. SUISSE	_____ 6. Bloqueur DNS de publicités, de traqueurs et de malwares.
G. WIREGUARD	_____ 7. Filtre de sécurité qui coupe le trafic réseau en cas de déconnexion.
H. KILLSWITCH	_____ 8. Routage multi-hop via des nœuds serveurs hautement sécurisés.

Point de contrôle 7 : Défi des mots mélangés

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

1. RCERESOEUC
2. SEHTLAT
3. OOCUPSENRE
4. GDREAUWIR
5. EHEDISNLT
6. LREAOTACRCE
7. SSSEIU
8. CLWHKSIITL

Activité bonus : Réflexion rapide

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

1	Mots qui décrivent une bonne application VPN			
2	Situations où un kill switch est utile			
3	Raisons de choisir Proton VPN			
4	Questions à poser au service client de Proton VPN			
5	Choses que Proton VPN peut cacher à votre réseau			
6	Personnes à qui vous recommanderiez Proton VPN			
7	Appareils sur lesquels vous installeriez Proton VPN			
8	Services de streaming que vous regardez			
9	Fonctionnalités que vous recherchez dans Proton VPN			
10	Choses à vérifier avant d'acheter un VPN			
11	Choses que vous faites en ligne chaque jour			
12	Signes que votre connexion VPN est lente			
13	Pays où vous aimeriez avoir des serveurs Proton VPN			
14	Services VPN autres que Proton VPN			
15	Endroits où vous activeriez Proton VPN			

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

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

ÉTUDE DE CAS 1 : DÉFENSE SECURE CORE



Scénario : Un militant des droits humains, dans un pays restrictif, doit envoyer des documents à un média étranger. Craignant que son FAI local ne surveille le nœud de sortie du VPN, il fait passer son trafic par le serveur Secure Core de Proton VPN en Suisse avant d'atteindre le nœud de destination.

Question de discussion : Comment Secure Core empêche-t-il les autorités locales de remonter jusqu'à l'IP de l'utilisateur au niveau du nœud de sortie ?

ÉTUDE DE CAS 2 : CONTOURNEMENT PAR PROTOCOLE FURTIF



Scénario : Un chercheur universitaire en voyage à l'étranger constate que sa résidence étudiante bloque les ports OpenVPN standard (1194) et les connexions UDP de WireGuard. Il active le protocole Stealth de Proton VPN sur son client Android.

Question de discussion : Quelle méthode technique le protocole Stealth utilise-t-il pour contourner les blocages du pare-feu ?

Point de contrôle 9 : Déchiffrer le code

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

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

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

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

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

12	5	19		19	5	18	22	5	21	18	19		16	18	15	20	15	14
22	16	14		21	20	9	12	9	19	5	14	20		19	5	3	21	18	5
								3	15	18	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 sur les réseaux privés virtuels (VPN) et le tunneling.

Q1: Qu'est-ce que la fonction Secure Core de Proton VPN ?

Secure Core fait passer votre trafic par plusieurs serveurs physiques situés dans des pays très sécurisés et respectueux de la vie privée (Suisse, Islande ou Suède) avant de sortir vers votre destination finale, ce qui protège contre les attaques par corrélation du réseau.

Q2: Comment fonctionne NetShield de Proton VPN ?

NetShield est un filtre DNS qui bloque les requêtes DNS vers des domaines connus de publicité, de traqueurs et de logiciels malveillants, ce qui les empêche de se charger dans votre navigateur et économise de la bande passante.

Q3: Les applications Proton VPN sont-elles open source ?

Oui, toutes les applications Proton VPN sont entièrement open source et leur code source est publié sur GitHub, accompagné de rapports d'audit professionnels indépendants.

Q4: Qu'est-ce que le Proton VPN Accelerator ?

Proton VPN Accelerator est un ensemble de technologies qui utilisent le contrôle de congestion BBR, plusieurs cœurs de processeur et une pile réseau optimisée pour augmenter les vitesses de connexion jusqu'à 400% sur les serveurs éloignés.

Q5: Sous quelle juridiction Proton VPN opère-t-il ?

Proton VPN relève de la juridiction suisse et est régi par des lois suisses strictes sur la vie privée, indépendamment de l'UE et des États-Unis.

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

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

Q6: Qu'est-ce que NetShield de Proton VPN ?

NetShield est un filtre de contenu basé sur le DNS qui bloque les logiciels malveillants, les scripts de pistage et les publicités, ce qui économise la bande passante mobile.

Q7: Proton VPN prend-il en charge Tor over VPN ?

Oui, Proton VPN propose des serveurs dédiés qui font automatiquement passer tout le trafic par le réseau d'anonymat Tor, ce qui permet d'accéder aux sites onion sans le navigateur Tor.

Q8: Combien d'appareils puis-je connecter à Proton VPN ?

Proton VPN prend en charge jusqu'à 10 connexions d'appareils simultanées avec les formules premium standard. [2]

Q9: Puis-je utiliser Proton VPN pour partager des fichiers en toute sécurité ?

Oui, Proton VPN dispose de serveurs dédiés optimisés pour le P2P, avec une bande passante à haut débit, conçus pour le torrent sécurisé.

Q10: Proton VPN a-t-il une formule gratuite ?

Oui, Proton VPN propose une version gratuite avec bande passante illimitée, mais elle limite l'accès aux serveurs de quelques pays et n'inclut ni NetShield ni Secure Core.

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

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

Q1: En quoi le protocole Stealth diffère-t-il d'OpenVPN standard ?

Contrairement à OpenVPN standard, qui utilise des ports et des en-têtes reconnaissables, Stealth fait passer WireGuard dans un tunnel TLS obfusqué sur TCP. Le trafic VPN ressemble ainsi à des connexions HTTPS courantes, ce qui aide à éviter les blocages par DPI dans les pays pratiquant la censure.

Q2: Où se trouvent physiquement les installations des serveurs Secure Core ?

Les serveurs Secure Core sont situés en Suisse, sur une ancienne base militaire en Islande et dans un centre de données souterrain en Suède, tous entièrement détenus et provisionnés par Proton. [1]

Q3: Proton VPN prend-il en charge la protection contre les fuites IPv6 ?

Oui, Proton VPN offre un routage IPv6 natif et une protection contre les fuites : il bloque automatiquement le trafic IPv6 au niveau du système si celui-ci n'est pas pris en charge par le tunnel sécurisé, afin d'éviter l'exposition des données.

Q4: Comment NetShield distingue-t-il les domaines publicitaires des domaines malveillants ?

NetShield compare les requêtes DNS sortantes à des listes noires de domaines connus. Le niveau 1 bloque les logiciels malveillants, tandis que le niveau 2 bloque les logiciels malveillants, les pixels de suivi et les réseaux publicitaires.

Q5: Comment le VPN Accelerator optimise-t-il la mise à l'échelle de la fenêtre TCP ?

Il utilise l'algorithme de contrôle de congestion BBR, divise les longs trajets en segments plus courts et exécute des processus parallèles sur les serveurs Proton afin de réduire la latence et les baisses de vitesse sur les nœuds éloignés.

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

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

Q6: Comment le réseau Secure Core résiste-t-il à la manipulation physique des serveurs ?

Proton expédie, installe et exploite lui-même ses serveurs Secure Core dans des installations hautement sécurisées, et tous les serveurs Proton VPN utilisent le chiffrement intégral du disque pour protéger leurs certificats et leur configuration.

Q7: Quel est le fondement cryptographique des listes NetShield de Proton ?

NetShield utilise des serveurs DNS Proton dédiés qui comparent chaque domaine à des bases de données de domaines connus pour héberger des logiciels malveillants, des publicités ou des traqueurs.

Q8: Comment le VPN Accelerator optimise-t-il l'utilisation des cœurs du processeur ?

L'Accelerator répartit le traitement des connexions sur plusieurs cœurs de processeur au lieu d'un seul thread, ce qui réduit les goulots d'étranglement sur les serveurs à haut débit.

Q9: Quel mécanisme d'obfuscation le protocole Stealth utilise-t-il ?

Stealth fait fonctionner WireGuard dans un tunnel TLS obfusqué sur TCP au lieu d'UDP, de sorte que le trafic ressemble à du HTTPS ordinaire et est plus difficile à repérer par l'inspection approfondie des paquets.

Q10: Comment Proton VPN garantit-il un routage DNS sans fuite sur les systèmes Linux ?

L'application Linux envoie les requêtes DNS par le tunnel VPN vers les serveurs DNS de Proton, et son kill switch bloque le trafic si le tunnel tombe.

Partie 11 : 10 faits et enseignements concrets sur les VPN

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

1. APERÇU VPN

Proton VPN est développé par Proton AG, l'entreprise suisse fondée par des scientifiques qui se sont rencontrés au CERN, à Genève. [5]

2. APERÇU VPN

Le fournisseur possède et héberge des serveurs Secure Core sur des sites à haute sécurité en Suisse, en Islande (ancienne base militaire) et en Suède. [1]

3. APERÇU VPN

Le code source des clients Proton VPN est entièrement open source et hébergé publiquement sur GitHub pour permettre des audits par des tiers. [6]

4. APERÇU VPN

La technologie NetShield bloque les publicités, les scripts malveillants et les traqueurs au niveau DNS avant qu'ils n'atteignent l'appareil de l'utilisateur.

5. APERÇU VPN

Le protocole Stealth fait passer WireGuard dans un tunnel TLS obfusqué pour contourner les blocages par inspection approfondie des paquets. [4]

6. APERÇU VPN

Proton VPN Accelerator utilise une optimisation du traitement multicœur pour augmenter les vitesses sur les serveurs éloignés. [3]

7. ZOOM SUR LES VPN

La loi suisse sur la protection des données exige en général une procédure judiciaire suisse avant que les métadonnées des utilisateurs puissent être remises. [5]

8. ZOOM SUR LES VPN

Le réseau de serveurs haut débit de Proton offre des connexions allant jusqu'à 10 Gbps (en septembre 2026). [2]

9. ZOOM SUR LES VPN

Un kill switch au niveau du système bloque tout le trafic Internet si la connexion VPN active est interrompue.

10. APERÇU VPN

Le tunnel fractionné fonctionne sous Windows, macOS, Linux, Android et Android TV, et fait passer les applications choisies en dehors du VPN. [2]

Références techniques et sources

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

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (2021). Increase VPN speeds by up to 400% with VPN Accelerator.
https://protonvpn.com/blog/vpn-accelerator

[4] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[5] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] Cardwell, N., & Cheng, Y. (2017). TCP BBR congestion control comes to GCP – your Internet just got faster.
https://cloud.google.com/blog/products/networking/tcp-bbr-congestion-control-comes-to-gcp-your-internet-just-got-faster

[9] Tor Project. (n.d.). Onion services - Features - Tor Browser.
https://support.torproject.org/onionservices/

[10] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

[11] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quelle fonctionnalité de Proton fait passer le trafic par des pays sûrs ? → Secure Core

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quelle est la fonction principale de NetShield de Proton VPN ? → Bloqueur de publicités et de logiciels malveillants basé sur le DNS

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quel protocole de Proton contourne la DPI grâce aux poignées de main TLS ? → Protocole furtif

4 Question 4

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'a de particulier le code source du client Proton VPN ? → Entièrement open source et audité publiquement [6]

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Proton indique que VPN Accelerator associe le contrôle de congestion BBR à un traitement multithread pour augmenter la vitesse.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

La technologie Secure Core de Proton VPN fait d'abord passer le trafic des utilisateurs par des serveurs physiques renforcés, situés dans des juridictions neutres et hautement sécurisées.

7 Question 7

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

NetShield fonctionne en interceptant et en bloquant les demandes de connexion vers des domaines de traqueurs et de logiciels malveillants au stade de la requête DNS.

8 Question 8

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : toutes les applications Proton VPN sont open source et ont été auditées de manière indépendante.

9 Question 9

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Le protocole Stealth encapsule les paquets VPN dans un chiffrement TLS standard pour les rendre impossibles à distinguer du trafic HTTPS.

10 Question 10

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : Proton VPN est basé en Suisse, qui ne fait pas partie de l'alliance 14-Eyes.

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. Secure Core	D 2. NetShield	F 3. Stealth	C 4. Accélérateur
B 5. Open source	E 6. Suisse	A 7. WireGuard	G 8. Kill switch

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 STEALTH	2 OPEN SOURCE	3 NETSHIELD	4 SECURE CORE
5 ACCELERATOR	6 SUISSE		

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

1 D – ACCELERATOR	2 E – OPENSOURCE	3 G – WIREGUARD	4 F – SUISSE
5 C – STEALTH	6 B – NETSHIELD	7 H – KILLSWITCH	8 A – SECURECORE

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Secure Core, NetShield et Stealth avec leurs propres mots et donner un exemple pour chacun.

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

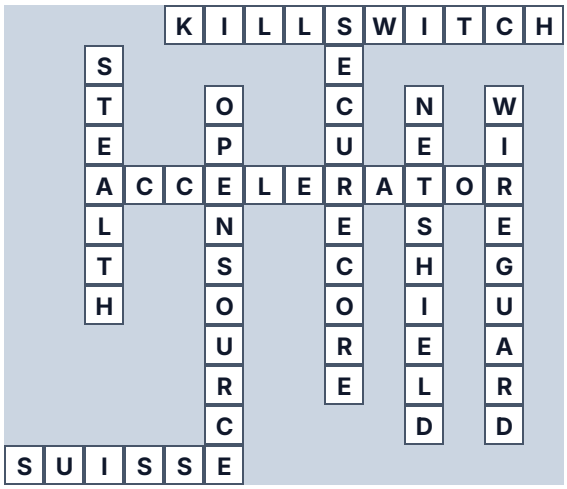
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

1 horizontal: KILLSWITCH Filtre de sécurité qui coupe le trafic réseau en cas de déconnexion (10 lettres)

7 horizontal: ACCELERATOR Moteur d'optimisation des performances qui répartit les charges de travail du processeur (11 lettres)

8 horizontal: SUISSE Juridiction centrale en matière de confidentialité, au cœur de l'Europe (6 lettres)

VERTICALEMENT

2 vertical: SECURECORE Routage multi-hop via des nœuds serveurs hautement sécurisés (10 lettres)

3 vertical: STEALTH Protocole obscurci personnalisé, conçu pour contourner les filtres DPI (7 lettres)

4 vertical: OPENSOURCE Dépôt de code source de l'application lisible par tous (10 lettres)

5 vertical: NETSHIELD Bloqueur DNS de publicités, de traqueurs et de malwares (9 lettres)

6 vertical: WIREGUARD Protocole de connexion open source moderne à haut débit (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. RCERESOEUC — **SECURECORE**
2. SEHTLAT — **STEALTH**
3. OOCUPSENRE — **OPENSOURCE**
4. GDREAUWIR — **WIREGUARD**
5. EHEDISNLT — **NETSHIELD**
6. LREAOTACRCE — **ACCELERATOR**
7. SSSEIU — **SUISSE**
8. CLWHKSIITL — **KILLSWITCH**

CORRIGÉ DU DÉFI DU CODE SECRET

"LES SERVEURS PROTON VPN UTILISENT SECURE CORE"

Corrigé des études de cas

A ÉTUDE DE CAS 1 : DÉFENSE SECURE CORE

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un militant des droits humains dans un pays répressif doit envoyer des documents à un média étranger. Craignant que son FAI local ne surveille le nœud de sortie du VPN, il fait passer son trafic par le serveur Secure Core de Proton VPN en Suisse avant d'atteindre le nœud de destination.
- Stratégie et solution recommandées : comme le nœud de sortie ne voit que le trafic provenant du serveur Secure Core en Suisse, une attaque par corrélation réseau sur le serveur de sortie ne peut pas révéler la véritable IP nationale de l'activiste.

B ÉTUDE DE CAS 2 : CONTOURNEMENT PAR PROTOCOLE FURTIF

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un chercheur universitaire à l'étranger constate que sa résidence étudiante bloque les ports OpenVPN standard (1194) et les connexions UDP WireGuard. Il active le protocole Stealth de Proton VPN sur son client Android.
- Stratégie et solution recommandées : Stealth fait fonctionner WireGuard à l'intérieur d'un tunnel TLS obfusqué sur TCP, si bien que le trafic ressemble à une navigation web sécurisée ordinaire pour les pare-feu à inspection approfondie des paquets.