Nom : _____ Date : _____ Note : _____

Sécurité de ProtonVPN

Analyser l'architecture de sécurité de ProtonVPN, notamment les serveurs Secure Core, le filtrage DNS NetShield, la juridiction suisse protectrice de la vie privée, les applications open source auditées et le protocole Stealth.

PRÉSENTATION DE L'APPRENTISSAGE : SÉCURITÉ DE PROTONVPN

APPRENANT
STATUT D'ÉTUDIANT
Parcours Défenseur du réseau

SÉCURISÉ
ÉTAT DE LA CONNEXION
Protéger les paquets de données

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

Bienvenue ! Ce dossier d'activités vous guide à travers l'architecture de sécurité de Proton VPN. Vous étudierez les serveurs Secure Core à double saut, le blocage DNS de NetShield, le droit suisse sur la vie privée et l'obfuscation 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/securite/

Votre parcours d'apprentissage : sécurité de ProtonVPN

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

CONSIGNES DU GUIDE SUR LA SÉCURITÉ DE PROTONVPN

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 routage double saut Secure Core et à la gouvernance suisse de la vie privée. Terminez par l'activité bonus Réflexion rapide.

ARCHITECTURE DOUBLE SAUT SECURE CORE ET JURIDICTION SUISSE PROTECTRICE DE LA VIE PRIVÉE

Proton VPN protège le trafic des utilisateurs grâce à des serveurs Secure Core appartenant à Proton en Suisse, en Islande et en Suède, à des applications open source auditées et au protocole d'obfuscation Stealth conçu pour contourner l'inspection approfondie des paquets.

(INTRODUCTION)

Proton VPN protège le trafic des utilisateurs grâce à des serveurs Secure Core appartenant à Proton en Suisse, en Islande et en Suède, à des applications open source auditées et au protocole d'obfuscation Stealth conçu pour contourner l'inspection approfondie des paquets.

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

Point de contrôle 1 : Défi QCM

1. **1. Dans quel type d'installations se trouvent les serveurs Secure Core de Proton ?**
   - A) VM de cloud public
   - B) Sites hautement sécurisés
   - C) Centres de données publics
   - D) Baies partagées

2. **2. Quel protocole aide à contourner une censure gouvernementale stricte ?**
   - A) PPTP
   - B) Protocole Stealth
   - C) OpenVPN UDP
   - D) IKEv2

3. **3. Quelle est la fonction de NetShield, la fonctionnalité de Proton VPN ?**
   - A) Speed Booster
   - B) Blocage DNS des publicités et logiciels malveillants
   - C) Stockage cloud
   - D) Redirection de port

4. **4. Sous les lois de quel pays sur la vie privée Proton AG opère-t-elle ?**
   - A) États-Unis
   - B) Royaume-Uni
   - C) Suisse
   - D) Panama

5. **5. Comment les applications clientes de Proton VPN sont-elles vérifiées par des experts ?**
   - A) Code secret
   - B) Audits open source
   - C) Licence propriétaire
   - D) Examen gouvernemental

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Secure Core fait passer le trafic par des pays respectueux de la vie privée avant la sortie.

○ Vrai ○ Faux

7 Question 7

7. La Suisse est membre de l'alliance de surveillance et de renseignement des 14 Eyes.

○ Vrai ○ Faux

8 Question 8

8. NetShield bloque les publicités et les domaines malveillants directement au niveau DNS.

○ Vrai ○ Faux

9 Question 9

9. Les applications Proton VPN sont 100% open source et auditées publiquement.

○ Vrai ○ Faux

10 Question 10

10. Le protocole Stealth utilise les en-têtes WireGuard standard, sans obfuscation.

○ 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. Le routage multi-hop via des serveurs détenus par Proton dans des pays respectueux de la vie privée s'appelle l'architecture _____ .

2. Pour déjouer l'inspection approfondie des paquets et les pare-feu réseau, les utilisateurs activent le mode _____ .

3. Les domaines malveillants, les traqueurs et les scripts publicitaires sont filtrés par le DNS _____ .

4. Proton affirme qu'en vertu du _____ , il n'est pas tenu de conserver de journaux d'activité des utilisateurs.

5. Si le tunnel VPN se déconnecte de manière inattendue, le trafic Internet est bloqué par la protection _____ .

6. Des chercheurs en sécurité indépendants vérifient l'intégrité du client, car les applications sont en code _____ .

BANQUE DE MOTS DE VOCABULAIRE

AES-GCM DROIT SUISSE KILL SWITCH NETSHIELD OPEN SOURCE SECURE CORE STEALTH WIREGUARD

Écrivez vos réponses ici :

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

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

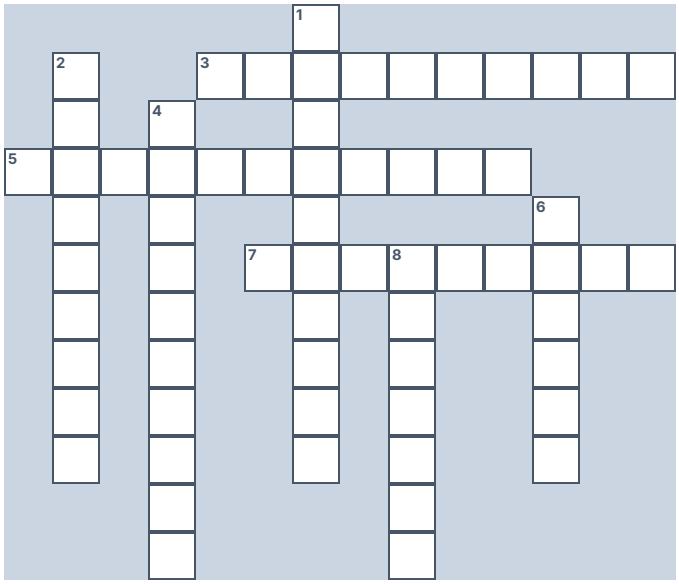
ASSOCIATION DE DÉFINITIONS

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	Logiciel client accessible au public et audité de manière indépendante.
☐	2. STEALTH	B	Norme de chiffrement symétrique qui chiffre les paquets de données du VPN.
☐	3. NETSHIELD	C	Lois strictes sur la protection de la vie privée en Suisse, hors de la juridiction des 14 Eyes.
☐	4. LOIS SUISSES	D	Un protocole de tunnel obscurci, déguisé en trafic web HTTPS standard.
☐	5. KILL SWITCH	E	Un protocole moderne et léger offrant une cryptographie robuste et des vitesses élevées.
☐	6. OPEN SOURCE	F	Un filtre basé sur le DNS qui bloque les publicités, les traceurs de télémétrie et les logiciels malveillants.
☐	7. WIREGUARD	G	Une architecture multi-sauts qui fait passer le trafic par des serveurs de premier saut appartenant à Proton.
☐	8. AES256-GCM	H	Une protection de sécurité qui interrompt la transmission réseau en cas de chute de la connexion.

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

3. Logiciel client accessible publiquement et audité de manière indépendante (10)

5. Lois strictes de protection de la vie privée en Suisse, hors de la juridiction des 14 Eyes (11)

7. Filtre DNS qui bloque les publicités, les traqueurs de télémétrie et les malwares (9)

VERTICALEMENT

1. Architecture multi-hop qui achemine le trafic via des serveurs de premier saut détenus par Proton (10)

2. Protocole moderne et léger offrant une cryptographie robuste et des vitesses élevées (9)

4. Protection de sécurité qui interrompt la transmission réseau lors des coupures de connexion (10)

6. Algorithme de chiffrement symétrique de niveau militaire qui sécurise tous les paquets VPN encapsulés (6)

8. Protocole de tunnel obscurci, déguisé en trafic web HTTPS standard (7)

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

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

HORIZONTALEMENT

3 horizontal: Logiciel client accessible publiquement et audité de manière indépendante (10 lettres):

5 horizontal: Lois strictes de protection de la vie privée en Suisse, hors de la juridiction des 14 Eyes (11 lettres):

7 horizontal: Filtre DNS qui bloque les publicités, les traqueurs de télémétrie et les malwares (9 lettres):

VERTICALEMENT

1 vertical: Architecture multi-hop qui achemine le trafic via des serveurs de premier saut détenus par Proton (10 lettres):

2 vertical: Protocole moderne et léger offrant une cryptographie robuste et des vitesses élevées (9 lettres):

4 vertical: Protection de sécurité qui interrompt la transmission réseau lors des coupures de connexion (10 lettres):

6 vertical: Algorithme de chiffrement symétrique de niveau militaire qui sécurise tous les paquets VPN encapsulés (6 lettres):

8 vertical: Protocole de tunnel obscurci, déguisé en trafic web HTTPS standard (7 lettres):

Point de contrôle 6 : Mots cachés

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

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

LISTE DE MOTS DE VOCABULAIRE

SECURECORE STEALTH NETSHIELD DROITSUISSE KILLSWITCH OPENSOURCE WIREGUARD AESGCM

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. SECURECORE
B. STEALTH
C. NETSHIELD
D. DROITSUISSE
E. KILLSWITCH
F. OPENSOURCE
G. WIREGUARD
H. AESGCM

DÉFINITIONS ET CHAMPS D'ASSOCIATION

1. Protocole de tunnel obscurci, déguisé en trafic web HTTPS standard.
2. Protocole moderne et léger offrant une cryptographie robuste et des vitesses élevées.
3. Lois strictes de protection de la vie privée en Suisse, hors de la juridiction des 14 Eyes.
4. Architecture multi-hop qui achemine le trafic via des serveurs de premier saut détenus par Proton.
5. Algorithme de chiffrement symétrique de niveau militaire qui sécurise tous les paquets VPN encapsulés.
6. Protection de sécurité qui interrompt la transmission réseau lors des coupures de connexion.
7. Filtre DNS qui bloque les publicités, les traqueurs de télémétrie et les malwares.
8. Logiciel client accessible publiquement et audité de manière indépendante.

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. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. TESISSDRUOI
7. PNOUORCESE
8. SMACGE

Activité bonus : Réflexion rapide

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

1	Choses que vous faites en ligne chaque jour			
2	Pays connus pour leurs lois strictes sur la vie privée			
3	Fonctionnalités de sécurité de Proton VPN			
4	Types de fuites VPN			
5	Situations où un kill switch est utile			
6	Choses qu'un audit peut vérifier			
7	Paramètres à activer pour plus de sécurité			
8	Choses que le chiffrement protège			
9	Mots qui décrivent une bonne application VPN			
10	Raisons de choisir Proton VPN			
11	Boutons ou menus d'une application VPN			
12	Services de streaming que vous regardez			
13	Menaces sur les Wi-Fi publics			
14	Façons de créer un mot de passe robuste			
15	Pays où vous aimeriez avoir des serveurs 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 : CONTOURNER LES PARE-FEU RESTRICTIFS

👮

Scénario : Un utilisateur se rend dans un pays où le trafic VPN standard, comme OpenVPN et WireGuard, est bloqué par la DPI.

Question de discussion : Quelle configuration de protocole de Proton VPN permet à l'utilisateur de contourner l'inspection mise en place par l'État ?

ÉTUDE DE CAS 2 : PROTECTION CONTRE LES ADVERSAIRES AVANCÉS

👮

Scénario : Un auditeur financier soupçonne que le nœud de sortie de son FAI local pourrait être compromis par des menaces persistantes avancées.

Question de discussion : Comment Secure Core protège-t-il l'identité de l'auditeur en cas de compromission d'un nœud de sortie ?

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		19	5	3	21	18	5
3	15	18	5		16	18	15	20	5	7	5	14	20		22	15	19	
				4	15	14	14	5	5	19								

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 Proton VPN Secure Core ?

Secure Core fait passer le trafic par plusieurs serveurs situés dans des pays respectueux de la vie privée avant la sortie.

Q2: Qu'est-ce que le protocole Stealth ?

Stealth est un protocole obfusqué qui fait passer les connexions VPN pour du trafic TLS/HTTPS ordinaire.

Q3: Comment NetShield protège-t-il les utilisateurs ?

NetShield est un outil basé sur le DNS qui bloque automatiquement les publicités, les traqueurs et les domaines de logiciels malveillants.

Q4: Proton VPN est-il protégé juridiquement en Suisse ?

Oui, la Suisse a des lois strictes sur la vie privée et se situe en dehors des juridictions américaine et de l'UE/des 14 Eyes. [4]

Q5: Les applications Proton VPN sont-elles open source ?

Oui. Les applications de Proton VPN sont open source et ont fait l'objet d'audits de sécurité publiés.

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: Quels algorithmes de chiffrement sont utilisés ?

Proton VPN utilise AES-256-GCM ou ChaCha20-Poly1305 avec HMAC-SHA384 et des handshakes RSA-4096.

Q7: Proton VPN dispose-t-il d'un Kill Switch ?

Oui, Proton VPN inclut un Kill Switch standard et un Kill Switch permanent pour éviter les fuites non chiffrées.

Q8: Proton VPN peut-il laisser fuiter des requêtes DNS ?

Non, toutes les requêtes DNS passent par des serveurs DNS privés et chiffrés appartenant à Proton.

Q9: Proton VPN conserve-t-il des journaux de connexion ?

Non, Proton VPN applique une politique stricte d'absence de journaux, confirmée par des audits annuels de Securitum. [3]

Q10: Proton VPN est-il vulnérable aux fuites WebRTC ?

Non, les clients Proton intègrent des règles de pare-feu et des politiques de routage qui bloquent les fuites WebRTC.

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: Où se trouvent physiquement les centres de données Secure Core ?

Ils se trouvent en Suisse, dans une ancienne base militaire en Islande et sur un site souterrain en Suède. [1]

Q2: Comment fonctionne la confidentialité persistante (Perfect Forward Secrecy) dans Proton VPN ?

Une clé de chiffrement éphémère unique est générée pour chaque session, ce qui empêche tout déchiffrement rétroactif.

Q3: Qu'est-ce que le Kill Switch permanent sur Windows/Linux ?

Le kill switch permanent bloque tout le trafic réseau même si l'application VPN est complètement fermée ou plante.

Q4: Proton VPN prend-il en charge le routage IPv6 et la protection contre les fuites ?

Proton VPN fait passer entièrement le trafic IPv6 par les tunnels ou le désactive de façon sûre pour éviter les fuites.

Q5: Comment le filtrage DNS de NetShield gère-t-il l'inspection HTTPS ?

NetShield agit uniquement au niveau de la résolution DNS, sans nécessiter de déchiffrement TLS intrusif.

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: Qui a réalisé les audits de code indépendants de Proton VPN ?

SEC Consult a audité les applications, et Securitum audite les applications et la politique de non-journalisation.

Q7: Comment le protocole Stealth se compare-t-il à OpenVPN XOR ou à Shadowsocks ?

Stealth fait passer WireGuard dans un tunnel TLS obfusqué et offre de meilleures performances que l'ancienne obfuscation basée sur OpenVPN. [5]

Q8: Les autorités suisses peuvent-elles contraindre Proton VPN à enregistrer le trafic ?

Proton déclare qu'en vertu du droit suisse, il n'est pas tenu de conserver des journaux de l'activité ou des données des utilisateurs.

Q9: Comment les serveurs de Proton VPN sont-ils protégés contre la saisie ?

Tous les serveurs de Proton VPN sont des machines physiques dédiées protégées par un chiffrement intégral du disque. [2]

Q10: Proton VPN prend-il en charge la configuration de serveurs DNS personnalisés ?

Oui, les abonnés payants peuvent configurer des serveurs DNS en amont personnalisés directement dans les préférences de l'application.

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

1. Proton possède et installe lui-même ses serveurs Secure Core, dans des sites hautement sécurisés en Suisse, en Islande et en Suède. [1]

2. APERÇU VPN

2. Les applications clientes de Proton VPN sont open source et font l'objet d'audits de code réguliers par des tiers.

3. APERÇU VPN

3. Le protocole d'obfuscation Stealth contourne l'inspection approfondie des paquets en simulant du trafic TLS standard.

4. APERÇU VPN

4. La Suisse est en dehors des alliances internationales de partage de renseignements 5-Eyes, 9- Eyes et 14-Eyes. [4]

5. APERÇU VPN

5. NetShield agit au niveau du résolveur DNS, empêchant publicités et logiciels malveillants avant le téléchargement du contenu.

6. APERÇU VPN

6. La confidentialité persistante (Perfect Forward Secrecy) garantit que des clés compromises ne peuvent pas déchiffrer des sessions de trafic capturées auparavant. [7]

7. ZOOM SUR LES VPN

7. Proton VPN utilise le chiffrement intégral du disque sur des serveurs physiques dédiés pour protéger les configurations des serveurs. [2]

8. ZOOM SUR LES VPN

8. Le kill switch permanent empêche les fuites de données non chiffrées même pendant les redémarrages du système d'exploitation.

9. ZOOM SUR LES VPN

9. Securitum a audité et confirmé la politique sans journaux de Proton VPN lors de cinq audits annuels consécutifs. [3]

10. APERÇU VPN

10. Proton VPN a été développé par des scientifiques qui se sont rencontrés au CERN (Organisation européenne pour la recherche nucléaire). [4]

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. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

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

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

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

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] 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

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

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

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1 — Bonne réponse : B

NOTE PÉDAGOGIQUE

Les serveurs Secure Core se trouvent dans des sites hautement sécurisés, dont une ancienne base militaire en Islande et un centre de données souterrain en Suède. [1]

2 Protocole d'obfuscation furtif DÉFENSE CONTRE LA CENSURE — Bonne réponse : B

NOTE PÉDAGOGIQUE

Le protocole Stealth de Proton déguise les connexions WireGuard en trafic TLS/HTTPS standard pour contourner les pare-feu d'inspection approfondie des paquets (DPI). Source : Proton Stealth Protocol Whitepaper.

3 Bloqueur de publicités DNS NetShield FILTRAGE DNS — Bonne réponse : B

NOTE PÉDAGOGIQUE

NetShield utilise un filtrage au niveau DNS pour bloquer les domaines de logiciels malveillants, les logiciels espions, la publicité intrusive et les traqueurs de télémétrie avant le chargement des pages web. Source : NetShield Security Specs.

4 Juridiction suisse JURIDICTION — Bonne réponse : C

NOTE PÉDAGOGIQUE

Proton AG a son siège à Genève, en Suisse, et bénéficie de solides lois suisses sur la vie privée, en dehors des alliances de surveillance américaines et européennes des 14 Eyes. Source : Swiss Federal Data Protection Act.

5 Question 5 — Bonne réponse : B

NOTE PÉDAGOGIQUE

Toutes les applications Proton VPN sont open source ; SEC Consult, puis Securitum, les ont auditées.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Secure Core multi-juridictions** ARCHITECTURE DE ROUTAGE — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Secure Core fait passer le trafic par des juridictions à la protection renforcée de la vie privée avant de sortir vers le pays de destination, ce qui aide à se protéger contre un serveur de sortie compromis. Source : Secure Core Architecture.

7 **Alliance de surveillance suisse** ALLIANCES DE SURVEILLANCE — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

La Suisse n'est membre d'aucun des accords de partage de renseignements 5 Eyes, 9 Eyes ou 14 Eyes, ce qui préserve sa souveraineté juridique indépendante. Source : International Surveillance Treaties.

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

NOTE PÉDAGOGIQUE

NetShield utilise les serveurs DNS de Proton pour comparer les domaines à des listes de domaines connus de publicité, de traçage et de logiciels malveillants.

9 **Audit du client open source** TRANSPARENCE EN MATIÈRE DE SÉCURITÉ — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Proton a rendu ses applications pour ordinateur et mobile open source et publie les rapports d'audit de tiers. Source : SEC Consult Security Report.

10 **Question 10** — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Faux : Stealth encapsule WireGuard dans du TLS obfusqué sur TCP, de sorte que le trafic ressemble à du HTTPS ordinaire.

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

G 1. SECURE CORE	D 2. STEALTH	F 3. NETSHIELD	C 4. LOIS SUISSES
H 5. KILL SWITCH	A 6. OPEN SOURCE	E 7. WIREGUARD	B 8. AES256-GCM

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 DROIT SUISSE
5 KILL SWITCH	6 OPEN SOURCE		

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

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

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer SECURE CORE, STEALTH et NETSHIELD 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.

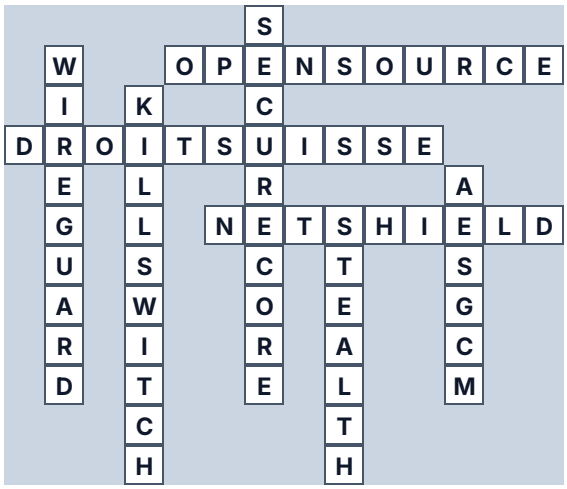
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

3 horizontal: OPENSOURCE Logiciel client accessible publiquement et audité de manière indépendante (10 lettres)

5 horizontal: DROITSUISSE Lois strictes de protection de la vie privée en Suisse, hors de la juridiction des 14 Eyes (11 lettres)

7 horizontal: NETSHIELD Filtre DNS qui bloque les publicités, les traqueurs de télémétrie et les malwares (9 lettres)

VERTICALEMENT

1 vertical: SECURECORE Architecture multi-hop qui achemine le trafic via des serveurs de premier saut détenus par Proton (10 lettres)

2 vertical: WIREGUARD Protocole moderne et léger offrant une cryptographie robuste et des vitesses élevées (9 lettres)

4 vertical: KILLSWITCH Protection de sécurité qui interrompt la transmission réseau lors des coupures de connexion (10 lettres)

6 vertical: AESGCM Algorithme de chiffrement symétrique de niveau militaire qui sécurise tous les paquets VPN encapsulés (6 lettres)

8 vertical: STEALTH Protocole de tunnel obscurci, déguisé en trafic web HTTPS standard (7 lettres)

Corrigé des mots mélangés et du code

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

CORRIGÉ DES MOTS MÉLANGÉS

1. RCERESOEUC — **SECURECORE**
2. DNLSEIEHT — **NETSHIELD**
3. KWCIISHLTL — **KILLSWITCH**
4. GDREAUWIR — **WIREGUARD**
5. LHAESTT — **STEALTH**
6. TESISSDRUOI — **DROITSUISSE**
7. PNOUORCESE — **OPENSOURCE**
8. SMACGE — **AESGCM**

CORRIGÉ DU DÉFI DU CODE SECRET

"LES SERVEURS SECURE CORE PROTEGENT VOS DONNEES"

Corrigé des études de cas

A ÉTUDE DE CAS 1 : CONTOURNER LES PARE-FEU RESTRICTIFS

Corrigé de l'enseignant

GRILLE DE NOTATION ET ÉLÉMENTS DE CORRECTION

- Analyse de scénario : un utilisateur se rend dans un pays où le trafic VPN standard comme OpenVPN et WireGuard est bloqué par DPI.
- Question clé : quelle configuration de protocole Proton VPN permet à l'utilisateur de contourner l'inspection imposée par l'État ?
- Stratégie et solution recommandées : l'utilisateur doit activer le protocole Stealth, qui obfusque les en-têtes des paquets VPN pour qu'ils ressemblent à du trafic web TLS/HTTPS ordinaire, et passer ainsi les filtres DPI.

B ÉTUDE DE CAS 2 : PROTECTION CONTRE LES ADVERSAIRES AVANCÉS

Corrigé de l'enseignant

GRILLE DE NOTATION ET ÉLÉMENTS DE CORRECTION

- Analyse de scénario : un auditeur financier soupçonne que le nœud de sortie de son FAI local pourrait être compromis par des menaces persistantes avancées.
- Question clé : comment Secure Core protège-t-il l'identité de l'auditeur en cas de compromission d'un nœud de sortie ?
- Stratégie et solution recommandées : Secure Core fait d'abord passer le trafic par des serveurs appartenant à Proton en Suisse, en Islande ou en Suède, de sorte qu'un serveur de sortie compromis ne peut pas remonter jusqu'à l'IP de l'utilisateur.