Nom : _____ Date : _____ Note : _____

Sécurité de Surfshark

Étude des fonctions de sécurité de Surfshark : blocage des publicités CleanWeb, routage dynamique MultiHop, architecture SDN Nexus, parc de serveurs uniquement en RAM et mode Camouflage.

SÉCURITÉ DE SURFSHARK : APERÇU DE L'APPRENTISSAGE

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 Surfshark. Vous découvrirez les serveurs fonctionnant uniquement en RAM, la rotation dynamique des IP du SDN Nexus, les bloqueurs de publicités CleanWeb et le routage MultiHop.

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/surfshark/securite/

Votre parcours d'apprentissage : sécurité de Surfshark

- Analysez l'architecture technique et les règles de configuration de la sécurité de Surfshark.
- 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 SURFSHARK

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 à l'infrastructure RAM uniquement, à Nexus SDN et à CleanWeb. Terminez par l'activité bonus Réflexion rapide.

PARC DE SERVEURS FONCTIONNANT UNIQUEMENT EN RAM, SDN NEXUS ET ARCHITECTURE CLEANWEB (INTRODUCTION)

Surfshark protège la vie privée des utilisateurs grâce à un parc de serveurs fonctionnant entièrement en RAM, au réseau défini par logiciel Nexus avec IP Rotator, au blocage des publicités CleanWeb et aux chemins de chiffrement Dynamic MultiHop.

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

Point de contrôle 1 : Défi QCM

1. **1. Quel est le nom du bloqueur de publicités et de logiciels malveillants intégré à Surfshark ?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Quelle architecture matérielle Surfshark utilise-t-il sur tous ses serveurs ?**
   - A) Disques durs
   - B) 100 % en RAM uniquement
   - C) Stockage optique
   - D) Bande magnétique

3. **3. Quelle fonctionnalité fait passer le trafic par deux serveurs VPN distincts ?**
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) Réseau Nexus
   - D) IP statique

4. **4. Quelle fonctionnalité d'obfuscation déguise le trafic VPN en données web ordinaires ?**
   - A) Kill switch
   - B) Mode camouflage
   - C) CleanWeb 2.0
   - D) Split tunnel

5. **5. Quelle est la fonction de l'outil Bypasser de Surfshark ?**
   - A) Speed Booster
   - B) Split tunneling (tunnel fractionné)
   - C) Gestionnaire de mots de passe
   - D) Résolveur DNS

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Les serveurs fonctionnant uniquement en RAM effacent toutes les données de fonctionnement dès le redémarrage du serveur.

- ○ Vrai
- ○ Faux

7 Question 7

7. Le mode Camouflage empêche les FAI de détecter que vous utilisez un VPN.

- ○ Vrai
- ○ Faux

8 Question 8

8. CleanWeb 2.0 fonctionne dans les extensions de navigateur pour bloquer les fenêtres de consentement aux cookies.

- ○ Vrai
- ○ Faux

9 Question 9

9. Surfshark conserve temporairement les horodatages de connexion et des journaux d'utilisation de la bande passante.

- ○ Vrai
- ○ Faux

10 Question 10

10. Le réseau Nexus fait tourner périodiquement les adresses IP des utilisateurs sans déconnexion.

- ○ 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. Les publicités gênantes, les scripts de pistage et les liens d'hameçonnage sont bloqués par les filtres _____ .

2. L'activité des utilisateurs ne laisse aucune trace exploitable, car les serveurs fonctionnent en mode _____ .

3. L'acheminement des données via deux sauts de serveurs chiffrés distincts est assuré par les tunnels _____ .

4. Pour dissimuler l'usage du VPN aux fournisseurs d'accès à Internet, les utilisateurs activent le mode _____ .

5. Permettre aux applications bancaires de contourner le tunnel VPN se gère dans les paramètres _____ .

6. L'architecture SDN de nouvelle génération qui relie le parc de serveurs est le système _____ .

BANQUE DE MOTS DE VOCABULAIRE

BYPASSER CAMOUFLAGE CLEANWEB IP ROTATIVE KILL SWITCH MULTI-HOP NEXUS RAM UNIQUEMENT

Écrivez vos réponses ici :

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

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

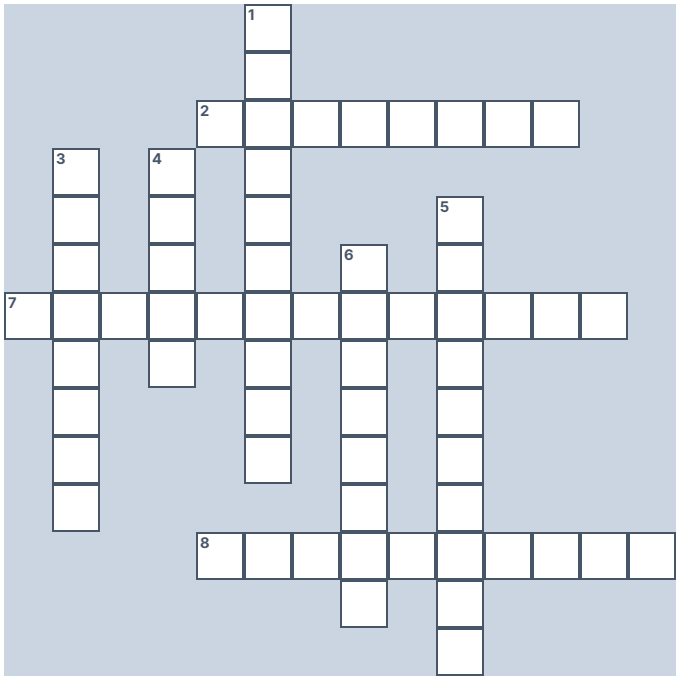
ASSOCIATION DE DÉFINITIONS

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. CLEANWEB	A	Une fonction de sécurité automatique qui bloque le trafic réseau lorsque le VPN tombe.
☐	2. RAM UNIQUEMENT	B	Fonction de tunnel fractionné permettant à certaines applications de contourner le VPN.
☐	3. MULTI-SAUT	C	Un filtre avancé qui bloque les publicités, les logiciels malveillants et les bandeaux de consentement aux cookies.
☐	4. CAMOUFLAGE	D	Matériel serveur à mémoire volatile qui efface toutes les données à chaque cycle d'alimentation.
☐	5. OUTIL DE CONTOURNEMENT	E	Une fonction qui change régulièrement votre adresse IP externe sans interrompre les tunnels.
☐	6. KILL SWITCH	F	Technologie d'obfuscation qui masque les signatures VPN pour imiter le trafic HTTPS ordinaire.
☐	7. RÉSEAU NEXUS	G	Une fonction de routage double VPN qui chiffre le trafic à travers deux nœuds de serveurs distincts.
☐	8. ROTATION	H	Un réseau propriétaire défini par logiciel qui relie tous les serveurs en un maillage unifié.

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. Filtre avancé qui bloque les publicités, les malwares et les bannières de consentement aux cookies (8)

7. Matériel serveur à mémoire volatile qui efface toutes les données à chaque redémarrage (13)

8. Fonction qui change régulièrement votre adresse IP externe sans interrompre les tunnels (10)

VERTICALEMENT

1. Fonction de sécurité automatique qui bloque le trafic réseau en cas de coupure du VPN (10)

3. Fonction de split tunneling permettant à certaines applications de contourner le VPN (8)

4. Réseau défini par logiciel propriétaire qui relie tous les serveurs en un maillage unifié (5)

5. Technologie d'obscurcissement qui masque les signatures VPN pour imiter le trafic HTTPS ordinaire (10)

6. Fonction de routage double VPN qui chiffre le trafic via deux nœuds serveurs distincts (8)

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: Filtre avancé qui bloque les publicités, les malwares et les bannières de consentement aux cookies (8 lettres):

7 horizontal: Matériel serveur à mémoire volatile qui efface toutes les données à chaque redémarrage (13 lettres):

8 horizontal: Fonction qui change régulièrement votre adresse IP externe sans interrompre les tunnels (10 lettres):

VERTICALEMENT

1 vertical: Fonction de sécurité automatique qui bloque le trafic réseau en cas de coupure du VPN (10 lettres):

3 vertical: Fonction de split tunneling permettant à certaines applications de contourner le VPN (8 lettres):

4 vertical: Réseau défini par logiciel propriétaire qui relie tous les serveurs en un maillage unifié (5 lettres):

5 vertical: Technologie d'obscurcissement qui masque les signatures VPN pour imiter le trafic HTTPS ordinaire (10 lettres):

6 vertical: Fonction de routage double VPN qui chiffre le trafic via deux nœuds serveurs distincts (8 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.

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

LISTE DE MOTS DE VOCABULAIRE

CLEANWEB RAMUNIQUEMENT MULTIHOP CAMOUFLAGE BYPASSER
KILLSWITCH NEXUS IPROTATIVE

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. CLEANWEB
B. RAMUNIQUEMENT
C. MULTIHOP
D. CAMOUFLAGE
E. BYPASSER
F. KILLSWITCH
G. NEXUS
H. IPROTATIVE

	DÉFINITIONS ET CHAMPS D'ASSOCIATION
	1. Technologie d'obscurcissement qui masque les signatures VPN pour imiter le trafic HTTPS ordinaire.
	2. Fonction de sécurité automatique qui bloque le trafic réseau en cas de coupure du VPN.
	3. Filtre avancé qui bloque les publicités, les malwares et les bannières de consentement aux cookies.
	4. Fonction de split tunneling permettant à certaines applications de contourner le VPN.
	5. Matériel serveur à mémoire volatile qui efface toutes les données à chaque redémarrage.
	6. Fonction qui change régulièrement votre adresse IP externe sans interrompre les tunnels.
	7. Fonction de routage double VPN qui chiffre le trafic via deux nœuds serveurs distincts.
	8. Réseau défini par logiciel propriétaire qui relie tous les serveurs en un maillage unifié.

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. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. EEAMUNTIMQ RNU
6. GUOLACAFEM
7. ILKIWTCHSL
8. VOAEITPTIR

Activité bonus : Réflexion rapide

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

1	Fonctionnalités de sécurité de Surfshark			
2	Signes que votre connexion VPN est lente			
3	Protocoles VPN que vous connaissez			
4	Choses que le chiffrement protège			
5	Menaces sur les Wi-Fi publics			
6	Pays connus pour leurs lois strictes sur la vie privée			
7	Façons de créer un mot de passe robuste			
8	Appareils sur lesquels vous installeriez Surfshark			
9	Questions à poser au service client de Surfshark			
10	Paramètres à activer pour plus de sécurité			
11	Choses que Surfshark peut cacher à votre réseau			
12	Types de fuites VPN			
13	Données qu'un VPN ne devrait jamais stocker			
14	Mots qui décrivent une bonne application VPN			
15	Choses qu'un audit peut vérifier			

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 FILTRES DU CAMPUS ET DU TRAVAIL

👷

Scénario : Un étudiant constate que le Wi-Fi de son campus universitaire bloque tous les ports OpenVPN et WireGuard standard.

Question de discussion : Quelle fonctionnalité de Surfshark permet à l'étudiant de se connecter sans être détecté par les administrateurs réseau ?

ÉTUDE DE CAS 2 : ENQUÊTE JOURNALISTIQUE À HAUT RISQUE

👷

Scénario : Un journaliste d'investigation a besoin d'une protection supplémentaire contre la surveillance pendant qu'il examine des dossiers d'entreprise sensibles.

Question de discussion : Comment Dynamic MultiHop offre-t-il une meilleure confidentialité qu'un routage par un seul serveur ?

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

9	16		18	15	20	1	20	9	22	5		14	5	24	21	19
18	5	14	6	15	18	3	5		12	1		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 sur les réseaux privés virtuels (VPN) et le tunneling.

Q1: Qu'est-ce que Surfshark CleanWeb ?

CleanWeb est une fonction de sécurité intégrée qui bloque les publicités, les traceurs, les logiciels malveillants et les sites d'hameçonnage.

Q2: Que sont les serveurs RAM uniquement ?

Les serveurs fonctionnant uniquement en RAM utilisent une mémoire volatile : les données conservées en mémoire sont effacées à chaque redémarrage des serveurs.

Q3: Qu'est-ce que Surfshark MultiHop ?

MultiHop (Double VPN) achemine et chiffre votre connexion Internet via deux emplacements de serveurs différents.

Q4: Comment fonctionne le Camouflage Mode ?

Le mode Camouflage brouille le trafic VPN pour que votre FAI ne puisse pas savoir que vous utilisez un VPN.

Q5: Qu'est-ce que la fonction Bypasser ?

Bypasser est l'outil de split tunneling de Surfshark qui permet à certaines applications ou à certains sites web de contourner le VPN.

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: Surfshark dispose-t-il d'un Kill Switch ?

Oui, le Kill Switch vous déconnecte d'Internet si le VPN se coupe de manière inattendue.

Q7: Quelle norme de chiffrement Surfshark utilise-t-il ?

Surfshark utilise AES-256-GCM et ChaCha20, ainsi qu'AEGIS-256X2 sur son nouveau protocole Dausos.

Q8: La politique de non-conservation des journaux de Surfshark a-t-elle été auditée ?

Oui, Deloitte a vérifié la politique sans journaux de Surfshark en 2023, puis de nouveau en 2025.

Q9: Qu'est-ce que Surfshark Nexus ?

Nexus est une architecture SDN avancée qui relie tous les serveurs en un réseau unifié pour un routage plus fluide.

Q10: Qu'est-ce que la fonction IP Rotator ?

IP Rotator change automatiquement votre adresse IP toutes les quelques minutes sans déconnecter votre session VPN.

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 Dynamic MultiHop diffère-t-il du double VPN classique ?

Dynamic MultiHop vous permet de personnaliser n'importe quelle combinaison de serveurs d'entrée et de sortie dans le monde.

Q2: CleanWeb 2.0 fonctionne-t-il dans les extensions de navigateur ?

Oui, CleanWeb 2.0 bloque les publicités vidéo, les fenêtres de consentement aux cookies et les bannières d'alerte dans Chrome/ Firefox.

Q3: Qu'est-ce qu'Alternative ID dans la suite de sécurité ?

Alternative ID génère des pseudonymes, des adresses e-mail et des numéros de téléphone masqués uniques.

Q4: Comment Surfshark empêche-t-il les fuites DNS ?

Surfshark fait passer toutes les requêtes de domaine par ses propres serveurs DNS privés sur chaque nœud.

Q5: Surfshark prend-il en charge le chiffrement ChaCha20 sur mobile ?

Oui, WireGuard sur Android et iOS utilise ChaCha20-Poly1305 pour une meilleure efficacité sur mobile.

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: Qu'est-ce que le mode NoBorders dans Surfshark ?

NoBorders détecte automatiquement les environnements réseau restrictifs et fournit des serveurs spécialisés.

Q7: Qui a réalisé les audits de sécurité des extensions de navigateur de Surfshark ?

Le cabinet indépendant de cybersécurité Cure53 a réalisé des audits des extensions de navigateur et des systèmes de serveurs.

Q8: Comment Surfshark protège-t-il contre les fuites IPv6 ?

Surfshark achemine le trafic IPv6 de manière sécurisée ou le restreint de façon sûre pour éviter toute fuite non chiffrée.

Q9: De quelle juridiction légale Surfshark relève-t-il ?

Surfshark relève du droit néerlandais et respecte les normes européennes strictes du RGPD (GDPR) en matière de vie privée.

Q10: Surfshark prend-il en charge l'authentification à deux facteurs (2FA) ?

Oui, et Surfshark One ajoute un verrouillage par 2FA afin que vous seul puissiez modifier les paramètres des fonctionnalités.

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. Surfshark affirme que l'ensemble de son réseau de plus de 4 500 serveurs fonctionne sur du matériel sans disque, en RAM volatile uniquement.

2. APERÇU VPN

2. Deloitte, l'un des « Big Four », a vérifié la politique sans journaux de Surfshark en 2023, puis de nouveau en novembre 2025.

3. APERÇU VPN

3. L'architecture propriétaire Nexus relie tous les serveurs mondiaux en un réseau dynamique défini par logiciel.

4. APERÇU VPN

4. Rotating IP change votre adresse IP environ toutes les cinq minutes sans couper la connexion VPN.

5. APERÇU VPN

5. CleanWeb 2.0 bloque directement dans les navigateurs les fenêtres intrusives de consentement aux cookies et les publicités vidéo.

6. APERÇU VPN

6. Dynamic MultiHop permet aux utilisateurs de créer des chemins de chiffrement personnalisés à deux serveurs dans 100 pays.

7. ZOOM SUR LES VPN

7. Le mode Camouflage supprime les signatures d'en-tête VPN, ce qui rend le trafic impossible à distinguer du HTTPS ordinaire.

8. ZOOM SUR LES VPN

8. Alternative ID génère des pseudonymes jetables et des alias d'e-mail pour protéger les utilisateurs contre les fuites de bases de données.

9. ZOOM SUR LES VPN

9. Surfshark applique le chiffrement symétrique AES-256-GCM ainsi que ChaCha20 sur les protocoles WireGuard.

10. APERÇU VPN

10. Le mode NoBorders s'active automatiquement sur les réseaux restreints pour offrir un accès par tunnel résilient.

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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Corrigé : Point de contrôle 1 – Choix multiple

1 **Bloqueur de contenu intégré** DÉFENSE CONTRE LES PUBLICITÉS ET LES LOGICIELS MALVEILLANTS — **Bonne réponse : B**

NOTE PÉDAGOGIQUE

CleanWeb est le filtre de sécurité intégré de Surfshark qui bloque, au niveau du réseau, les publicités, les domaines de traceurs, les sites d'hameçonnage et les scripts d'URL malveillants. Source : CleanWeb Security Specs.

2 **Infrastructure 100 % RAM** ARCHITECTURE RAM — **Bonne réponse : B**

NOTE PÉDAGOGIQUE

Surfshark utilise des serveurs fonctionnant uniquement en RAM : les données conservées dans la mémoire d'un serveur sont donc effacées lorsqu'il est éteint ou redémarré. Source : Cure53 Infrastructure Audit.

3 **Double tunnel MultiHop** VPN MULTI-SAUT — **Bonne réponse : B**

NOTE PÉDAGOGIQUE

MultiHop (Double VPN) chiffre le trafic à travers deux nœuds serveurs distincts situés dans des pays différents afin d'empêcher les attaques par corrélation de trafic. Source : Surfshark MultiHop Guide.

4 **Obfuscation par le mode Camouflage** OBFUSCATION — **Bonne réponse : B**

NOTE PÉDAGOGIQUE

Le mode Camouflage modifie les en-têtes des paquets OpenVPN pour faire passer le trafic VPN pour du trafic HTTPS standard, ce qui permet de contourner les blocages de pare-feu restrictifs. Source : Surfshark Stealth Whitepaper.

5 **Split tunneling Bypasser** SPLIT TUNNELING — **Bonne réponse : B**

NOTE PÉDAGOGIQUE

Bypasser est l'outil de split tunneling de Surfshark qui permet aux utilisateurs de choisir des applications ou des sites web à acheminer directement par leur connexion habituelle au FAI. Source : Surfshark Client Features.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Effacement des données de la mémoire volatile** SÉCURITÉ DES SERVEURS **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les serveurs fonctionnant uniquement en RAM ne stockent aucune donnée sur des disques durs permanents; le redémarrage du matériel purge immédiatement toute la mémoire de fonctionnement. Source : RAM Server Architecture.

7 **Dissimulation au FAI par le mode Camouflage** DISSIMULATION DU TRAFIC **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Le mode Camouflage supprime les signatures du protocole OpenVPN, ce qui empêche les FAI de détecter que l'utilisateur est connecté à un tunnel VPN. Source : Deep Packet Inspection Guide.

8 **Extensions de navigateur CleanWeb 2.0** EXTENSION DE NAVIGATEUR **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

CleanWeb 2.0 fonctionne dans les extensions de navigateur pour bloquer en temps réel les fenêtres de consentement aux cookies, les publicités vidéo et les scripts de redirection malveillants. Source : CleanWeb 2.0 Release Notes.

9 **Aucune conservation des journaux de connexion** POLITIQUE D'ABSENCE DE JOURNAUX **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Surfshark applique une politique stricte de non-journalisation vérifiée par un audit indépendant : il n'enregistre ni adresses IP, ni horodatages de connexion, ni journaux de bande passante. Source : Deloitte No-Logs Audit.

10 **Rotation dynamique des IP Nexus** RÉSEAU NEXUS **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Le réseau défini par logiciel Surfshark Nexus fait tourner dynamiquement les adresses IP des utilisateurs toutes les quelques minutes sans interrompre la connexion VPN active. Citation : Surfshark Nexus Architecture.

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

C 1. CLEANWEB	D 2. RAM UNIQUEMENT	G 3. MULTI-SAUT	F 4. CAMOUFLAGE
B 5. OUTIL DE CONTOURNEMENT	A 6. KILL SWITCH	H 7. RÉSEAU NEXUS	E 8. ROTATION

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 CLEANWEB	2 RAM UNIQUEMENT	3 MULTI-HOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

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

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – RAMUNIQUEMENT	6 H – IPROTATIVE	7 C – MULTIHOP	8 G – NEXUS

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer CLEANWEB, RAM UNIQUEMENT et MULTI-SAUT 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.

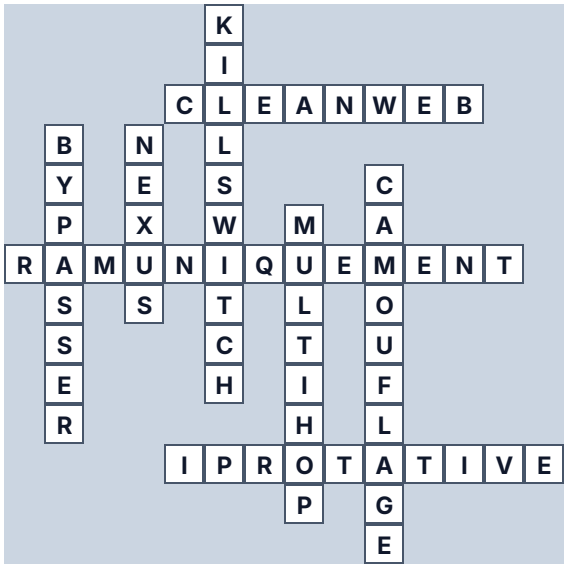
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

2 horizontal: CLEANWEB Filtre avancé qui bloque les publicités, les malwares et les bannières de consentement aux cookies (8 lettres)

7 horizontal: RAMUNIQUEMENT Matériel serveur à mémoire volatile qui efface toutes les données à chaque redémarrage (13 lettres)

8 horizontal: IPROTATIVE Fonction qui change régulièrement votre adresse IP externe sans interrompre les tunnels (10 lettres)

VERTICALEMENT

1 vertical: KILLSWITCH Fonction de sécurité automatique qui bloque le trafic réseau en cas de coupure du VPN (10 lettres)

3 vertical: BYPASSER Fonction de split tunneling permettant à certaines applications de contourner le VPN (8 lettres)

4 vertical: NEXUS Réseau défini par logiciel propriétaire qui relie tous les serveurs en un maillage unifié (5 lettres)

5 vertical: CAMOUFLAGE Technologie d'obscurcissement qui masque les signatures VPN pour imiter le trafic HTTPS ordinaire (10 lettres)

6 vertical: MULTIHOP Fonction de routage double VPN qui chiffre le trafic via deux nœuds serveurs distincts (8 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. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. E E A M U N T I M Q R N U — **RAMUNIQUEMENT**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. V O A E I T P T I R — **IPROTATIVE**

CORRIGÉ DU DÉFI DU CODE SECRET

"IP ROTATIVE NEXUS RENFORCE LA VIE PRIVEE"

Corrigé des études de cas

A ÉTUDE DE CAS 1 : CONTOURNER LES FILTRES DU CAMPUS ET DU TRAVAIL

Corrigé de l'enseignant

GRILLE DE NOTATION ET ÉLÉMENTS DE CORRECTION

- Analyse de scénario : un étudiant constate que le Wi-Fi du campus universitaire bloque tous les ports standard d'OpenVPN et de WireGuard.
- Question clé : quelle fonctionnalité de Surfshark permet à l'élève de se connecter sans être détecté par les administrateurs réseau ?
- Stratégie et solution recommandées : activer le Camouflage Mode (OpenVPN), qui masque les métadonnées du VPN afin que les pare-feu voient une navigation HTTPS normale.

B ÉTUDE DE CAS 2 : ENQUÊTE JOURNALISTIQUE À HAUT RISQUE

Corrigé de l'enseignant

GRILLE DE NOTATION ET ÉLÉMENTS DE CORRECTION

- Analyse de scénario : un journaliste d'investigation a besoin d'une protection supplémentaire contre la surveillance pendant qu'il consulte des documents d'entreprise sensibles.
- Question clé : en quoi Dynamic MultiHop offre-t-il une meilleure confidentialité que le routage par un seul serveur ?
- Stratégie et solution recommandées : le MultiHop dynamique fait transiter le trafic par des serveurs d'entrée et de sortie situés dans deux pays, si bien qu'aucun serveur ne peut à lui seul exposer l'utilisateur.