Nom : _____ Date : _____ Note : _____

Guide du VPN le plus sûr

Analyse technique de la conception d'un VPN hautement sécurisé : serveurs à mémoire volatile fonctionnant uniquement en RAM, sécurité d'accès Zero Trust, défenses contre les fuites grâce à un DNS privé chiffré et configurations WireGuard auditées.

GUIDE DU VPN LE PLUS SÛR : PRÉSENTATION

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 normes techniques des VPN hautement sécurisés. Vous étudierez le matériel des serveurs fonctionnant uniquement en RAM, la sécurité d'accès Zero Trust, les résolveurs DNS privés et chiffrés et les configurations WireGuard auditées.

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/vpn-le-plus-securise/

Votre parcours d'apprentissage : VPN les plus sécurisés

- Analysez l'architecture technique et les normes de chiffrement abordées dans le guide des VPN les plus sûrs.
- 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.

GUIDE DU VPN LE PLUS SÛR : 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 au matériel de serveurs RAM uniquement et aux systèmes Zero Trust. Terminez par l'activité bonus Réflexion rapide.

INFRASTRUCTURES FONCTIONNANT UNIQUEMENT EN RAM ET RÉSEAUX ZERO TRUST (INTRODUCTION)

Un VPN réellement sûr repose sur un cadre Zero Trust, des serveurs RAM uniquement pour éviter que la saisie de disques n'expose des journaux, des résolveurs DNS privés et chiffrés, et des protocoles audités comme WireGuard. Ces contrôles combinés protègent les actifs numériques de grande valeur contre les menaces d'interception.

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

Point de contrôle 1 : Défi QCM

1. Quelle architecture est essentielle pour garantir le plus haut niveau de sécurité des serveurs VPN modernes ?

- A) Infrastructure de serveurs RAM uniquement
- B) Stockage sur disque
- C) Routage DNS dynamique
- D) Activation de la redirection de port

2. Quel protocole est largement recommandé pour les configurations VPN les plus sûres et les plus modernes ?

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3. Quel cadre de sécurité exige de vérifier chaque connexion en continu, sans exception ?

- A) Architecture Zero Trust
- B) Pare-feu périmétriques
- C) Routage dynamique
- D) Clés secrètes partagées

4. Quel est le rôle principal de la protection contre les fuites DNS d'un client VPN ?

- A) Acheminer toutes les requêtes DNS par des résolveurs privés et chiffrés
- B) Obfusquer les paquets IP
- C) Mettre en cache les requêtes DNS en local
- D) Désactiver les serveurs de noms

5. Comment le routage Multi-Hop renforce-t-il la sécurité globale d'un tunnel VPN ?

- A) Fait passer les données successivement par deux serveurs distincts
- B) Augmente la vitesse de compression
- C) Chiffre les données avec des algorithmes peu sûrs
- D) Contourne les pare-feu

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Les serveurs fonctionnant uniquement en RAM stockent les fichiers journaux dans une mémoire éphémère, effacée au redémarrage.

- ○ Vrai
- ○ Faux

7 Question 7

7. WireGuard utilise des algorithmes cryptographiques modernes moins sujets aux goulets d'étranglement de vitesse.

- ○ Vrai
- ○ Faux

8 Question 8

8. Le kill switch d'un VPN fonctionne en bloquant tout le trafic réseau si le tunnel tombe.

- ○ Vrai
- ○ Faux

9 Question 9

9. Les audits indépendants réalisés par des tiers n'ont aucune utilité pour vérifier les engagements de sécurité.

- ○ Vrai
- ○ Faux

10 Question 10

10. Les modèles Zero Trust considèrent toutes les connexions au réseau interne comme sûres par défaut.

- ○ 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 administrateurs renforcent la sécurité en déployant un cadre strict de _____ .

2. Acheminer les paquets via plusieurs points d'entrée nécessite une configuration _____ sécurisée.

3. Pour éviter les fuites de données en cas de vol de disques, nous utilisons une conception de type _____ .

4. Le détournement par le FAI est atténué en configurant les fonctions natives de _____ .

5. Pour bloquer le trafic lors des pannes de connexion, activez le mécanisme de _____ .

6. Pour réduire au minimum les journaux stockés en base de données, choisissez un fournisseur doté d'un _____ dans son intégralité.

BANQUE DE MOTS DE VOCABULAIRE

CHIFFREMENT | CONFIANCE ZÉRO | KILL SWITCH | MULTI-HOP | PROTECTION DNS | PROTOCOLE | SERVEUR RAM | SYSTÈME AUDITÉ

Écrivez vos réponses ici :

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

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

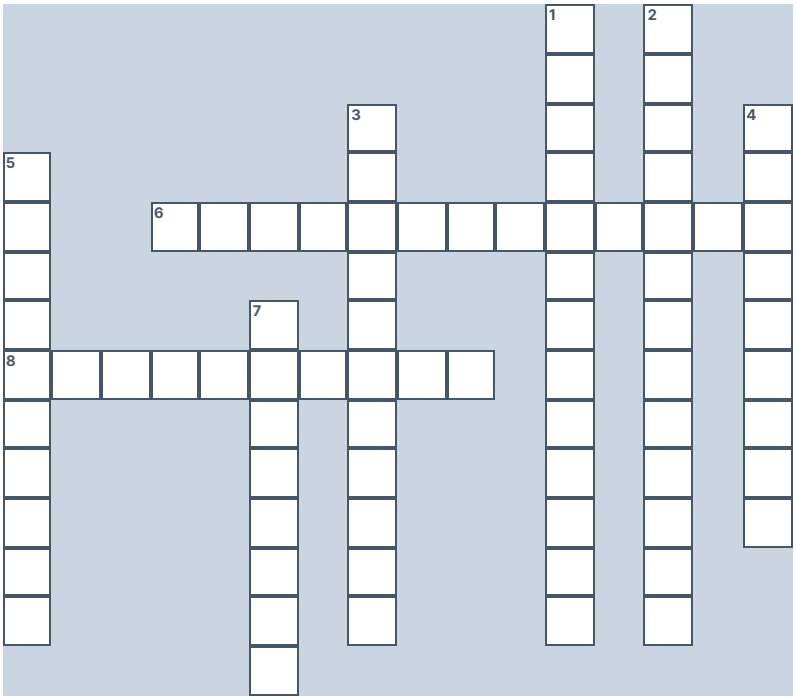
ASSOCIATION DE DÉFINITIONS

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. Zero Trust	A	Configuration inspectée de façon indépendante confirmant qu'aucun journal n'est conservé.
☐	2. Multi-saut	B	Brouillage cryptographique des données utiles pour sécuriser le transit.
☐	3. Serveur fonctionnant uniquement en RAM	C	Cadre de sécurité exigeant une authentification continue de tous les utilisateurs.
☐	4. Protection DNS	D	Ensemble de règles techniques qui déterminent comment les données sont empaquetées et envoyées.
☐	5. Kill switch	E	Routage VPN en cascade qui enchaîne deux nœuds de serveur.
☐	6. Système audité	F	Architecture de serveur utilisant la mémoire volatile pour stocker les données utiles.
☐	7. Chiffrement	G	Imposer des requêtes DNS privées pour protéger les recherches auprès des serveurs de noms.
☐	8. Protocole	H	Mécanisme de sécurité qui bloque le trafic si le VPN tombe en panne.

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

6. Cadre de sécurité exigeant l'authentification continue de tous les utilisateurs (13)

8. Architecture de serveur utilisant la mémoire volatile pour stocker les données utiles (10)

VERTICALEMENT

1. Application de requêtes DNS privées pour protéger les résolutions de serveurs de noms (13)

2. Configuration inspectée de manière indépendante, confirmant qu'aucun journal n'est stocké (13)

3. Brouillage cryptographique des données utiles pour sécuriser leur transit (11)

4. Ensemble de règles techniques qui définissent comment les données sont empaquetées et envoyées (9)

5. Mécanisme de sécurité qui bloque le trafic en cas de défaillance du VPN (10)

7. Routage VPN en cascade qui enchaîne deux nœuds serveurs (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

6 horizontal: Cadre de sécurité exigeant l'authentification continue de tous les utilisateurs (13 lettres):

8 horizontal: Architecture de serveur utilisant la mémoire volatile pour stocker les données utiles (10 lettres):

VERTICALEMENT

1 vertical: Application de requêtes DNS privées pour protéger les résolutions de serveurs de noms (13 lettres):

2 vertical: Configuration inspectée de manière indépendante, confirmant qu'aucun journal n'est stocké (13 lettres):

3 vertical: Brouillage cryptographique des données utiles pour sécuriser leur transit (11 lettres):

4 vertical: Ensemble de règles techniques qui définissent comment les données sont empaquetées et envoyées (9 lettres):

5 vertical: Mécanisme de sécurité qui bloque le trafic en cas de défaillance du VPN (10 lettres):

7 vertical: Routage VPN en cascade qui enchaîne deux nœuds serveurs (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.

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

LISTE DE MOTS DE VOCABULAIRE

CONFIANCEZERO MULTIHOP SERVEURRAM PROTECTIONDNS KILLSWITCH
SYSTEMEAUDITE CHIFFREMENT PROTOCOLE

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. CONFIANCEZERO
B. MULTIHOP
C. SERVEURRAM
D. PROTECTIONDNS
E. KILLSWITCH
F. SYSTEMEAUDITE
G. CHIFFREMENT
H. PROTOCOLE

DÉFINITIONS ET CHAMPS D'ASSOCIATION
1. Mécanisme de sécurité qui bloque le trafic en cas de défaillance du VPN.
2. Application de requêtes DNS privées pour protéger les résolutions de serveurs de noms.
3. Routage VPN en cascade qui enchaîne deux nœuds serveurs.
4. Ensemble de règles techniques qui définissent comment les données sont empaquetées et envoyées.
5. Brouillage cryptographique des données utiles pour sécuriser leur transit.
6. Architecture de serveur utilisant la mémoire volatile pour stocker les données utiles.
7. Configuration inspectée de manière indépendante, confirmant qu'aucun journal n'est stocké.
8. Cadre de sécurité exigeant l'authentification continue de tous les utilisateurs.

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. NNERAOCZCE OIF
2. AVSEEMRRUR
3. KWCIISHLTL
4. ENTRIFEMCH F
5. IHUPTMOL
6. ENTCDONOPR IST
7. DIAMSYUEET SET
8. EOLPTRCOO

Activité bonus : Réflexion rapide

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

1	Serrures ou clés que vous utilisez chaque jour			
2	Choses qu'un VPN peut cacher			
3	Choses qui rendent un VPN sûr			
4	Idées reçues sur les VPN			
5	Raisons d'utiliser un VPN en voyage			
6	Endroits sûrs dans le monde réel			
7	Mots qui signifient 'protégé'			
8	Engagements d'un bon fournisseur de VPN			
9	Mots liés à la vie privée			
10	Types d'audits ou d'inspections			
11	Mots de cette fiche que vous voulez retenir			
12	Choses qu'un pirate veut voler			
13	Façons de repérer un faux réseau Wi-Fi			
14	Endroits où vous utiliseriez un VPN			
15	Choses que votre fournisseur d'accès à Internet peut voir			

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 : RENFORCER L'INFRASTRUCTURE D'ENTREPRISE

👷

Scénario : Une banque d'entreprise repense la topologie de son accès à distance. Elle exige une architecture Zero Trust reliant tous les appareils clients à des serveurs sécurisés.

Question de discussion : Quel est le principal avantage de la micro-segmentation du réseau dans un modèle de VPN Zero Trust ?

ÉTUDE DE CAS 2 : PROTECTIONS DES SERVEURS RAM UNIQUEMENT

👷

Scénario : Un fournisseur de VPN axé sur la sécurité met à niveau ses serveurs afin d'éviter qu'une saisie physique d'un serveur n'expose l'historique des journaux des utilisateurs.

Question de discussion : Expliquez comment les configurations matérielles fonctionnant uniquement en RAM empêchent l'extraction de données à des fins d'analyse forensique lors de saisies physiques de serveurs.

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 22 16 14 19 5 3 21 18 9 19 5 19

16 18 15 20 5 7 5 14 20 12 5 19 1 3 20 9 6 19

16 18 5 3 9 5 21 24

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 qui fait d'un VPN le « plus sûr » ?

Une combinaison de Zero Trust, de serveurs RAM uniquement et de protocoles audités.

Q2: Que sont les serveurs RAM uniquement ?

Serveurs fonctionnant en mémoire volatile, conçus pour ne stocker aucun journal sur disque.

Q3: Qu'est-ce qu'un VPN Zero Trust ?

Un cadre qui vérifie en permanence chaque demande d'accès et chaque connexion.

Q4: Pourquoi WireGuard est-il considéré comme sûr ?

Sa base de code est petite et facile à auditer, et il utilise des algorithmes de chiffrement modernes.

Q5: Comment les VPN sécurisés empêchent-ils les fuites DNS ?

En faisant passer toutes les requêtes par des résolveurs DNS privés et chiffrés.

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: Un VPN sécurisé nécessite-t-il des audits ?

Oui, des audits indépendants vérifient les affirmations de non-journalisation et la sécurité du code.

Q7: Quel est le rôle d'un kill switch ?

Il coupe immédiatement le trafic réseau si la connexion VPN tombe.

Q8: Quel chiffrement est utilisé dans les VPN sécurisés ?

AES-256 et ChaCha20 sont les normes du secteur en matière de chiffrement.

Q9: Le routage Multi-Hop est-il sûr ?

Oui, il enchaîne deux serveurs ou plus pour empêcher l'analyse du trafic.

Q10: En quoi une juridiction offshore est-elle utile ?

Elle peut limiter les lois applicables, mais n'offre aucune immunité absolue.

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: Comment les serveurs RAM uniquement empêchent-ils les risques de saisie de données ?

Comme ils fonctionnent en RAM, couper l'alimentation efface les données conservées en mémoire.

Q2: Comment le Zero Trust remplace-t-il la sécurité périmétrique classique ?

Il traite chaque client comme hostile et exige une authentification continue.

Q3: Qu'est-ce qui rend le code de WireGuard plus facile à auditer ?

Son code Linux compte moins de 4 000 lignes, bien moins que les piles VPN habituelles. [4]

Q4: Comment DNSSEC protège-t-il les requêtes DNS ?

Il signe les enregistrements DNS afin que les résolveurs puissent détecter les réponses falsifiées ou altérées.

Q5: Comment le Multi-Hop complique-t-il la corrélation du trafic ?

En séparant les adresses IP entrantes et sortantes entre différents hébergeurs.

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: Pourquoi les juridictions des Five Eyes sont-elles risquées pour les VPN ?

Les États membres partagent des renseignements et peuvent recourir à des ordonnances judiciaires pour obtenir des données d'utilisateurs.

Q7: Comment un kill switch est-il mis en œuvre au niveau du noyau ?

Il utilise les règles du pare-feu système (comme iptables ou WFP) pour bloquer le trafic sortant.

Q8: Qu'est-ce que la confidentialité persistante dans les négociations de connexion VPN ?

Il génère des clés de session uniques afin que les sessions passées ne puissent pas être déchiffrées.

Q9: Comment les VPN sécurisés limitent-ils les fuites WebRTC ?

En bloquant les requêtes WebRTC ou en les faisant passer par le tunnel.

Q10: Comment les audits indépendants garantissent-ils le respect de la vie privée ?

Les auditeurs réalisent des tests d'intrusion et inspectent la configuration des serveurs.

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

Les serveurs fonctionnant uniquement en RAM chargent leur système d'exploitation en mémoire au démarrage, si bien que rien ne subsiste sur disque après un redémarrage.

2. APERÇU VPN

WireGuard utilise le cadre Noise avec Curve25519, ChaCha20, Poly1305, BLAKE2s et HKDF. [3]

3. APERÇU VPN

Le Zero Trust accorde l'accès ressource par ressource et n'accorde aucune confiance implicite fondée sur l'emplacement réseau (NIST SP 800-207). [1]

4. APERÇU VPN

L'alliance de renseignement des Five Eyes regroupe les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.

5. APERÇU VPN

Les fuites WebRTC se produisent lorsque les navigateurs révèlent la véritable adresse IP publique du client par des requêtes STUN.

6. APERÇU VPN

La confidentialité persistante (PFS) garantit que la compromission d'une clé à long terme n'expose pas les clés des sessions passées. [3]

7. ZOOM SUR LES VPN

Cure53, une société de sécurité basée à Berlin, a publié des audits de plusieurs fournisseurs de VPN.

8. ZOOM SUR LES VPN

Les fuites DNS se produisent lorsque des requêtes DNS contournent le tunnel VPN et sont envoyées aux serveurs de noms du FAI local.

9. ZOOM SUR LES VPN

Les puces de RAM volatile ont besoin d'une alimentation électrique constante pour conserver les données et perdent leur contenu à la mise hors tension.

10. APERÇU VPN

Les systèmes zero trust d'entreprise imposent des vérifications de posture des appareils avant d'autoriser la connexion aux ressources sécurisées. [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Corrigé : Point de contrôle 1 – Choix multiple

1 **Serveur fonctionnant uniquement en RAM** UNIQUEMENT EN RAM — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les serveurs fonctionnant uniquement en RAM ne stockent aucun journal sur disque et effacent les données au redémarrage. Source : Most Secure VPN.

2 **Question 2** — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

WireGuard associe un code compact et auditable à des algorithmes de chiffrement modernes.

3 **Modèle Zero Trust** ZERO TRUST — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les modèles Zero Trust vérifient en continu la conformité des appareils avant l'accès. Source : Most Secure VPN.

4 **Protection DNS** PROTECTION DNS — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

La protection contre les fuites DNS fait passer les requêtes de résolution par des résolveurs privés. Source : Most Secure VPN.

5 **Tunnels multi-saut** MULTI-SAUT — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Le routage multi-saut enchaîne deux nœuds serveurs distincts en série. Source : Most Secure VPN.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Serveur fonctionnant uniquement en RAM** UNIQUEMENT EN RAM — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Le matériel des serveurs fonctionnant uniquement en RAM n'écrit aucune donnée sur disque et s'efface au redémarrage. Source : Most Secure VPN.

7 **Vitesse de WireGuard** WIREGUARD — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

WireGuard utilise une cryptographie moderne qui évite les goulets d'étranglement de traitement. Citation : Most Secure VPN.

8 **Kill switch** COUPURE DE SÉCURITÉ — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Un kill switch bloque tout le trafic si la connexion VPN tombe. Source : Most Secure VPN.

9 **Audits par des tiers** AUDITS ESSENTIELS — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Les audits par des tiers sont essentiels pour vérifier les affirmations des entreprises en matière de confidentialité. Citation : Most Secure VPN.

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

NOTE PÉDAGOGIQUE

Le Zero Trust n'accorde aucune confiance implicite fondée sur l'emplacement réseau. [1]

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. Zero Trust	E 2. Multi-saut	F 3. Serveur fonctionnant uniquement en RAM	G 4. Protection DNS
H 5. Kill switch	A 6. Système audité	B 7. Chiffrement	D 8. Protocole

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 CONFIANCE ZÉRO	2 MULTI-HOP	3 SERVEUR RAM	4 PROTECTION DNS
5 KILL SWITCH	6 SYSTÈME AUDITÉ		

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

1 E – KILLSWITCH	2 D – PROTECTIONDNS	3 B – MULTIHOP	4 H – PROTOCOLE
5 G – CHIFFREMENT	6 C – SERVEURRAM	7 F – SYSTEMEAUDITE	8 A – CONFIANCEZERO

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Zero Trust, Multi-saut et Serveur fonctionnant uniquement en RAM 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.

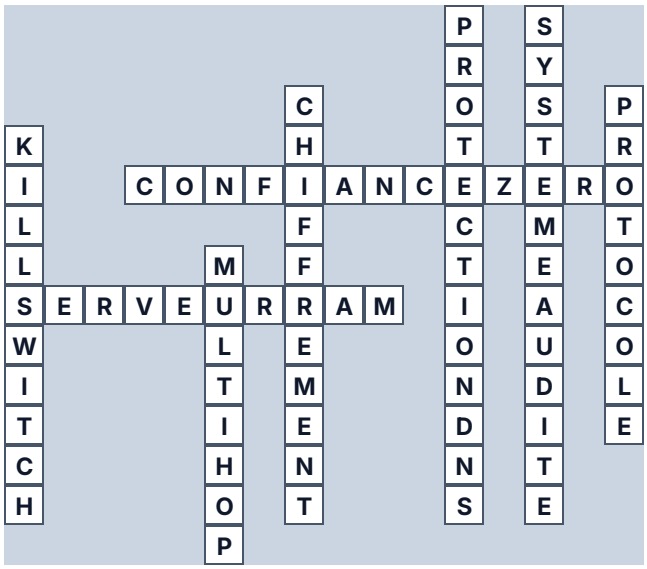
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

6 horizontal: CONFIANCEZERO Cadre de sécurité exigeant l'authentification continue de tous les utilisateurs (13 lettres)

8 horizontal: SERVEURRAM Architecture de serveur utilisant la mémoire volatile pour stocker les données utiles (10 lettres)

VERTICALEMENT

1 vertical: PROTECTIONDNS Application de requêtes DNS privées pour protéger les résolutions de serveurs de noms (13 lettres)

2 vertical: SYSTEMEAUDITE Configuration inspectée de manière indépendante, confirmant qu'aucun journal n'est stocké (13 lettres)

3 vertical: CHIFFREMENT Brouillage cryptographique des données utiles pour sécuriser leur transit (11 lettres)

4 vertical: PROTOCOLE Ensemble de règles techniques qui définissent comment les données sont empaquetées et envoyées (9 lettres)

5 vertical: KILLSWITCH Mécanisme de sécurité qui bloque le trafic en cas de défaillance du VPN (10 lettres)

7 vertical: MULTIHOP Routage VPN en cascade qui enchaîne deux nœuds serveurs (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. NNERAOCZCEOIF — **CONFIANCEZERO**
2. AVSEEMRRUR — **SERVEURRAM**
3. KWCIISHLTL — **KILLSWITCH**
4. ENTRIFEMCHF — **CHIFFREMENT**
5. IHUPTMOL — **MULTIHOP**
6. ENTCDONOPRIST — **PROTECTIONDNS**
7. DIAMSYUEETSET — **SYSTEMEAUDITE**
8. EOLPTRCOO — **PROTOCOLE**

CORRIGÉ DU DÉFI DU CODE SECRET

"LES VPN SECURISES PROTEGENT LES ACTIFS PRECIEUX"

Corrigé des études de cas

A ÉTUDE DE CAS 1 : RENFORCER L'INFRASTRUCTURE D'ENTREPRISE

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : une banque d'entreprise repense la topologie de son accès à distance. Elle exige une architecture zero trust reliant tous les appareils clients à des serveurs sécurisés.
- Stratégie et solution recommandées : Consignes de notation : expliquer que la micro-segmentation limite l'accès à des ressources précises, empêchant le déplacement latéral d'une menace si un appareil est compromis.

B ÉTUDE DE CAS 2 : PROTECTIONS DES SERVEURS RAM UNIQUEMENT

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un fournisseur VPN axé sur la sécurité modernise ses serveurs pour éviter qu'une saisie physique d'un serveur n'expose l'historique des journaux des utilisateurs.
- Stratégie et solution recommandées : Consignes de notation : expliquer en détail que les serveurs RAM-Only n'ont pas de stockage physique sur disque. Une coupure de courant efface automatiquement toutes les données éphémères en mémoire volatile.