Nom : _____ Date : _____ Note : _____

Comment configurer un VPN Fiche de travail

Configurer un VPN sous Windows, macOS, Android, iOS, Linux et sur les routeurs

APERÇU DE L'APPRENTISSAGE : VPN

APPRENANT
STATUT D'ÉTUDIANT
Parcours Défenseur du réseau

SÉCURISÉ
ÉTAT DE LA CONNEXION
Protéger les paquets de données

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

Bienvenue ! Ce dossier d'activités vous guide à travers les principes fondamentaux des réseaux privés virtuels (VPN). Vous étudierez comment les tunnels chiffrés sécurisent vos données, comment fonctionnent les protocoles réseau et comment repérer et limiter les fuites de données personnelles.

POINTS DE CONTRÔLE DE LA FICHE

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

Ouvrir le guide VPN.com des VPN

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

Votre parcours d'apprentissage : VPN

- Comparez les applications VPN commerciales avec la configuration de clients natifs.
- Configurez des connexions VPN sur les routeurs pour protéger toute la maison.
- Configurer et gérer des fichiers de configuration tels que les fichiers OVPN ou les clés WireGuard.
- Ouvrir et sécuriser des ports précis du routeur pour le trafic du tunnel.
- Vérifiez la configuration des clients au moyen de tests de fuite DNS et de tests de connexion.

INSTRUCTIONS DE LA FICHE DE CONFIGURATION

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 la configuration et au test des clients VPN. Terminez par l'activité bonus Réflexion rapide.

CONFIGURATION DU VPN (INTRODUCTION)

Configurer un VPN manuellement vous donne un contrôle total sur vos clés de chiffrement et le routage de votre réseau. Que vous configuriez un client natif sur votre appareil mobile ou que vous installiez un tunnel VPN directement sur votre routeur, une configuration correcte est essentielle pour éviter les fuites DNS et sécuriser tout le trafic réseau.

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

Point de contrôle 1 : Défi QCM

1. Quelle est la façon la plus simple de configurer un VPN sur un appareil mobile ?

- A. Télécharger l'application VPN officielle depuis la boutique d'applications
- B. Modifier manuellement les fichiers du noyau du système d'exploitation
- C. Flasher un firmware personnalisé sur le matériel de l'appareil
- D. Connecter le téléphone à un ordinateur de bureau par USB

2. Quel est l'un des avantages d'installer un VPN directement sur votre routeur ?

- A. Il augmente la vitesse de connexion de tous les appareils locaux
- B. Il sécurise automatiquement tous les appareils connectés au réseau
- C. Il évite d'avoir à payer un abonnement auprès d'un FAI local
- D. Il supprime totalement le besoin de routeurs matériels

3. À quoi fait référence une configuration VPN « native » ?

- A. Configurer la connexion avec les paramètres natifs intégrés au système d'exploitation
- B. Utiliser un VPN uniquement dans votre ville
- C. Se connecter uniquement à des serveurs situés dans le pays
- D. Écrire un protocole personnalisé en langage assembleur

4. Que faut-il pour une configuration externe manuelle d'OpenVPN ?

- A. Concevoir un logo personnalisé pour la connexion au serveur
- B. Importer le profil .ovpn contenant les clés de certificat
- C. Déplacer physiquement le routeur domestique
- D. Désactiver complètement le pare-feu du système d'exploitation

5. Pourquoi un administrateur utiliserait-il le split tunneling dans une configuration ?

- A. Bloquer complètement tout le trafic Internet
- B. Permettre à certaines applications sûres de contourner le tunnel sécurisé
- C. Pour diviser le routeur physique en deux appareils distincts
- D. Pour désactiver le chiffrement à des fins de surveillance administrative

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Configurer un VPN sur un routeur est une opération simple qui ne demande aucune compétence technique.

- ◯ Vrai
- ◯ Faux

7 Question 7

7. Windows et macOS disposent de clients natifs compatibles avec IKEv2 et L2TP.

- ◯ Vrai
- ◯ Faux

8 Question 8

8. La configuration de WireGuard nécessite de générer des clés publiques et privées.

- ◯ Vrai
- ◯ Faux

9 Question 9

9. Un tunnel VPN sécurise les imprimantes de votre réseau local et vos travaux d'impression.

- ◯ Vrai
- ◯ Faux

10 Question 10

10. Les serrures connectées qui ne peuvent pas exécuter d'applications VPN ont besoin d'un VPN au niveau du routeur pour être couvertes.

- ◯ 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. Installer un VPN au niveau du _____ , la passerelle, protège les téléviseurs connectés et les consoles de jeu.

2. Les configurations OpenVPN manuelles exigent d'importer un _____ de serveur.

3. Les configurations intégrées au système d'exploitation utilisent les paramètres du _____ système.

4. L'authentification WireGuard repose sur une _____ cryptographique, publique et privée.

5. Une installation conviviale passe par l' _____ officielle du fournisseur.

6. Acheminer les requêtes via les serveurs _____ du VPN évite les fuites de suivi lors de la résolution de noms.

BANQUE DE MOTS DE VOCABULAIRE

APPLICATION VPN | CLIENT NATIF | DNS | LOGS DE CONNEXION | PAIRE DE CLÉS
PROFIL OVPN | ROUTEUR | SPLIT TUNNELING

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions sur les réseaux

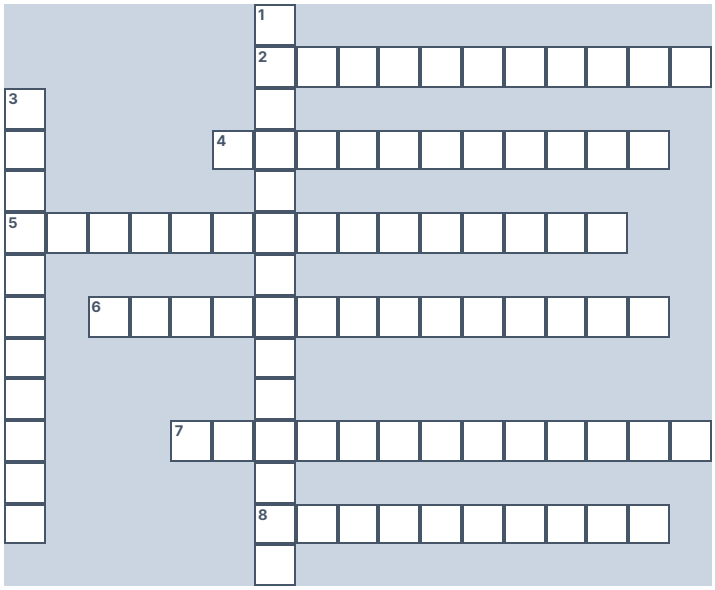
ASSOCIATION DE DÉFINITIONS

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

☐	1. Application VPN	A	Chiffrement au niveau de la passerelle protégeant tous les appareils connectés d'un réseau local.
☐	2. VPN sur routeur	B	Logiciel fourni par le service d'abonnement pour une installation simple en un clic.
☐	3. Client natif	C	Consulter les messages d'erreur et les journaux d'état du client pour déboguer une configuration qui a échoué.
☐	4. Profil .ovpn	D	Différencier les routes du trafic pour permettre à certaines applications de contourner le tunnel chiffré.
☐	5. Paire de clés	E	Sécuriser le trafic dans les paramètres natifs du système d'exploitation sans installer d'applications.
☐	6. Tunnel fractionné (split tunneling)	F	Configurer les adresses des résolveurs réseau pour éviter les fuites de requêtes de domaines.
☐	7. Configuration du serveur DNS	G	Clés cryptographiques (publique/privée) nécessaires pour établir les négociations WireGuard.
☐	8. Journaux de connexion	H	Format de fichier OpenVPN contenant les serveurs, les paramètres de port et les clés de certificat.

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. Jetons cryptographiques (public/privé) nécessaires pour établir les échanges de clés WireGuard (11)

4. Sécurisation du trafic dans les paramètres natifs du système d'exploitation, sans installer d'application (11)

5. Consultation des messages d'erreur et des journaux d'état du client pour déboguer une configuration qui échoue (15)

6. Différenciation des routes de trafic pour laisser certaines applications contourner le tunnel chiffré (14)

7. Chiffrement au niveau de la passerelle, qui protège tous les appareils connectés d'un réseau local (13)

8. Format de fichier OpenVPN contenant les serveurs, les réglages de port et les clés de certificat (10)

VERTICALEMENT

1. Logiciel fourni par le service d'abonnement pour une installation simple en un clic (14)

3. Configuration des adresses des résolveurs réseau pour éviter les fuites de résolution de noms de domaine (11)

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: Jetons cryptographiques (public/privé) nécessaires pour établir les échanges de clés WireGuard (11 lettres):

4 horizontal: Sécurisation du trafic dans les paramètres natifs du système d'exploitation, sans installer d'application (11 lettres):

5 horizontal: Consultation des messages d'erreur et des journaux d'état du client pour déboguer une configuration qui échoue (15 lettres):

6 horizontal: Différenciation des routes de trafic pour laisser certaines applications contourner le tunnel chiffré (14 lettres):

7 horizontal: Chiffrement au niveau de la passerelle, qui protège tous les appareils connectés d'un réseau local (13 lettres):

8 horizontal: Format de fichier OpenVPN contenant les serveurs, les réglages de port et les clés de certificat (10 lettres):

VERTICALEMENT

1 vertical: Logiciel fourni par le service d'abonnement pour une installation simple en un clic (14 lettres):

3 vertical: Configuration des adresses des résolveurs réseau pour éviter les fuites de résolution de noms de domaine (11 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.

T U K X E J R L Z X I K M X E

M R M X U P V O C T A S G P V

R P F S Z I I G J U P Q N A D

U R Z N F N N S D B P R I W F

E O P D I R J D M V L K L X M

T F A S T Q W E J K I L E O F

U I I E A G N C U V C F N D X

O L R G N L V O O O A R N P W

R O E A T G L N G M T M U V W

R V D L N N E N H J I Q T K H

U P E G E P J E L I O W T T L

S N C E I N C X N C N X I E T

N W L R L N T I N K V D L D J

P S E O C B W O P X P P P H C

V H S N T K W N O W N O S R Q

LISTE DE MOTS DE VOCABULAIRE

APPLICATIONVPN VPNSURROUTEUR CLIENTNATIF PROFILOVPN PAIREDECLES SPLITTUNNELING REGLAGESDNS LOGSDECONNEXION

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. APPLICATIONVPN**
- **B. VPNSURROUTEUR**
- **C. CLIENTNATIF**
- **D. PROFILOVPN**
- **E. PAIREDECLES**
- **F. SPLITTUNNELING**
- **G. REGLAGESDNS**
- **H. LOGSDECONNEXION**

DÉFINITIONS ET CHAMPS D'ASSOCIATION

_____ 1. Configuration des adresses des résolveurs réseau pour éviter les fuites de résolution de noms de domaine.

_____ 2. Différenciation des routes de trafic pour laisser certaines applications contourner le tunnel chiffré.

_____ 3. Chiffrement au niveau de la passerelle, qui protège tous les appareils connectés d'un réseau local.

_____ 4. Jetons cryptographiques (public/privé) nécessaires pour établir les échanges de clés WireGuard.

_____ 5. Sécurisation du trafic dans les paramètres natifs du système d'exploitation, sans installer d'application.

_____ 6. Consultation des messages d'erreur et des journaux d'état du client pour déboguer une configuration qui échoue.

_____ 7. Format de fichier OpenVPN contenant les serveurs, les réglages de port et les clés de certificat.

_____ 8. Logiciel fourni par le service d'abonnement pour une installation simple en un clic.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés sur les VPN. Écrivez vos réponses dans les champs à remplir.

1. NCTOAPPIVAPNIL
2. NFLCITITANE
3. PEDCIAESELR
4. ENSGGADSREL
5. UEPNOURRTRVUS
6. PIFOVPRLNO
7. LNESNPLGTINIUT
8. NINSCNOOELOGEXD

Activité bonus : Réflexion rapide

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

1	Choses à vérifier une fois la configuration terminée			
2	Appareils pouvant utiliser un VPN			
3	Services VPN que vous connaissez			
4	Raisons d'utiliser un VPN en voyage			
5	Erreurs courantes lors de la configuration			
6	Mots de cette fiche que vous voulez retenir			
7	Paramètres que vous activez en premier			
8	Engagements d'un bon fournisseur de VPN			
9	Étapes de la configuration d'un VPN			
10	Endroits où vous utiliseriez un VPN			
11	Façons de repérer un faux réseau Wi-Fi			
12	Choses qu'un VPN peut cacher			
13	Choses que votre fournisseur d'accès à Internet peut voir			
14	Endroits où trouver de l'aide			
15	Choses dont vous avez besoin pour commencer			

Point de contrôle 8 : Études de cas sur les VPN

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

SARAH (ÉTUDIANTE AU CAFÉ)

👩‍💻 "Salut ! Je suis au Coffee & Bytes. Il y a un réseau public non sécurisé appelé 'Free_Wi-Fi_No_Password'. Je veux me connecter à ma messagerie scolaire et envoyer mon devoir, mais j'ai peur des pirates. Quels sont les risques si j'utilise ce réseau sans VPN, et comment un VPN sécurise-t-il mes données ?"

ALEX (ÉTUDIANT VOYAGEUR)

👩‍💻 "Oh non ! Je voyage à l'étranger pour un projet et j'essaie de regarder un documentaire de biologie hébergé sur un serveur de mon pays d'origine. Mais le site affiche : 'Cette vidéo n'est pas disponible dans votre pays.' Pourquoi suis-je bloqué, et comment un VPN peut-il m'aider à le regarder ?"

Point de contrôle 9 : Déchiffrer le code

Pour terminer votre formation sur la configuration des serveurs, déchiffrez ce message caché sur la mise en place de tunnels sécurisés.

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 14 19 20 1 12 12 5 26 12 1

16 1 19 19 5 18 5 12 12 5 1 22 5 3 21 14

4 5 13 15 14 19 5 3 21 18 9 19 5

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

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

Passez en revue les questions et réponses les plus courantes que se posent les clients potentiels sur l'utilisation des réseaux privés virtuels.

Q1: Qu'est-ce qu'un VPN et comment fonctionne-t-il ?

Un réseau privé virtuel (VPN) chiffre votre connexion Internet et fait passer votre trafic par un serveur distant sécurisé. Cela masque votre adresse IP publique et limite ce que les observateurs du réseau local et votre FAI peuvent voir du trafic acheminé par le tunnel VPN.

Q2: De quoi ai-je besoin pour commencer ?

Il vous faut un abonnement VPN actif ou votre propre serveur VPN, un appareil compatible, et soit l'application du fournisseur, soit les informations de configuration manuelle : adresse du serveur, protocole et vos identifiants, clés ou certificats. La plupart des gens installent simplement l'application officielle, se connectent à leur compte et appuient sur le bouton de connexion.

Q3: Comment configurer un VPN sur Windows sans application ?

Ouvrez Paramètres > Réseau et Internet > VPN, choisissez Ajouter un VPN, puis saisissez le nom du serveur du fournisseur, le type de VPN (comme IKEv2 ou L2TP/IPsec) et vos identifiants de connexion. Sélectionnez ensuite Se connecter.

Q4: Un VPN va-t-il ralentir ma connexion Internet ?

Oui, légèrement. Le processus de chiffrement et la distance physique jusqu'au serveur VPN ajoutent de la latence et une surcharge. L'impact varie selon le fournisseur, le protocole, la distance du serveur, l'appareil et les conditions du réseau.

Q5: Comment configurer macOS ?

Installez l'application macOS du fournisseur, ou ouvrez Réglages Système > VPN, ajoutez une configuration VPN, choisissez IKEv2, L2TP sur IPSec ou Cisco IPSec, puis saisissez l'adresse du serveur et les identifiants fournis par votre fournisseur.

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

Passez en revue les questions et réponses les plus courantes que se posent les clients potentiels sur l'utilisation des réseaux privés virtuels.

Q6: Puis-je utiliser un VPN gratuit ?

Les VPN gratuits peuvent reposer sur la publicité, des fonctionnalités limitées, l'analyse d'utilisation, des plafonds de données ou d'autres modèles de monétisation. Les utilisateurs devraient examiner la politique de confidentialité, la structure de propriété, les audits et le modèle économique du fournisseur avant de l'utiliser.

Q7: Comment utiliser un fichier .ovpn ?

Installez un client OpenVPN, importez le profil .ovpn fourni par votre fournisseur ou votre administrateur, puis connectez-vous. Le fichier contient l'adresse du serveur, le port, le choix UDP ou TCP et souvent les certificats et les clés.

Q8: Comment choisir le meilleur VPN ?

Recherchez des politiques d'absence de journaux auditées, des protocoles robustes (WireGuard, OpenVPN), des emplacements de serveurs sûrs, des vitesses élevées, des serveurs fonctionnant uniquement en RAM, une fonction kill switch et une juridiction en dehors des alliances de partage de renseignements (comme les 5/9/14 Eyes).

Q9: Puis-je utiliser un VPN sur mon téléphone et ma smart TV ?

Oui. Les fournisseurs de VPN modernes proposent des applications dédiées pour iOS, Android, macOS, Windows, Linux et les téléviseurs connectés, ainsi que des configurations pour routeur afin de protéger tous les appareils de votre réseau domestique.

Q10: Qu'est-ce qu'un kill switch ?

Un kill switch est une fonction de sécurité qui déconnecte automatiquement votre appareil d'Internet si la connexion VPN tombe. Cela empêche la fuite de vos données non chiffrées ou de votre véritable adresse IP.

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

Découvrez les aspects techniques et structurels des réseaux privés virtuels et des protocoles de tunnel sécurisés.

Q1: Quelle est la différence entre WireGuard, OpenVPN et IKEv2 ?

WireGuard est un protocole moderne et léger (environ 4 000 lignes de code seulement) qui offre des vitesses élevées et des temps de connexion courts. OpenVPN est un protocole open source très sûr et éprouvé. IKEv2 est excellent pour les appareils mobiles grâce à sa capacité à se reconnecter rapidement lors d'un changement de réseau.

Q2: Comment configurer WireGuard manuellement ?

Générez une paire de clés avec wg genkey et wg pubkey, communiquez votre clé publique au serveur, puis rédigez une configuration indiquant votre clé privée, la clé publique du pair, les IP autorisées et le point de terminaison. L'outil wg-quick active ensuite le tunnel. [2]

Q3: Qu'est-ce qu'une fuite WebRTC et comment un VPN l'empêche-t-il ?

WebRTC est un protocole de navigateur qui peut révéler vos véritables adresses IP locale et publique même lorsqu'un VPN est actif. Les VPN premium bloquent ou falsifient les requêtes WebRTC dans leurs applications pour ordinateur et mobile et dans leurs extensions de navigateur.

Q4: Comment configurer un VPN en toute sécurité sur mon routeur domestique ?

Vérifiez que votre routeur prend en charge le mode client VPN, connectez-vous à sa page d'administration et importez le fichier OpenVPN ou WireGuard du fournisseur. Certains routeurs nécessitent d'abord une mise à jour du firmware ; ensuite, chaque appareil du réseau utilise le tunnel.

Q5: Comment l'obfuscation contourne-t-elle les blocages de VPN ?

L'obfuscation (ou « VPN furtif ») déguise le trafic VPN pour qu'il ressemble à du trafic HTTPS ordinaire (port 443). Cela peut l'aider à passer l'inspection approfondie des paquets (DPI) utilisée par les gouvernements ou les réseaux scolaires et professionnels pour bloquer les VPN.

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

Découvrez les aspects techniques et structurels des réseaux privés virtuels et des protocoles de tunnel sécurisés.

Q6: Qu'est-ce que le split tunneling et quand l'utiliser ?

Le tunnel fractionné (split tunneling) vous permet de choisir quelles applications passent par le tunnel VPN chiffré et lesquelles se connectent directement à internet. Utilisez-le pour faire passer les applications bancaires sensibles par le VPN tandis que les jeux locaux se connectent directement, ce qui évite la latence ajoutée par le VPN.

Q7: Comment vérifier que ma nouvelle configuration VPN fonctionne ?

Connectez-vous, puis rendez-vous sur un site de vérification d'IP : il doit afficher l'adresse IP et l'emplacement du serveur VPN. Lancez des tests de fuite DNS et WebRTC, et coupez brièvement la connexion pour vérifier que le kill switch bloque le trafic.

Q8: Que vérifier si mon VPN ne se connecte pas après la configuration ?

Vérifiez vos identifiants ou vos clés, l'adresse du serveur, et que le port et le protocole choisis ne sont pas bloqués. Essayez de passer d'UDP à TCP ou de changer de serveur, et lisez les journaux de connexion de l'application pour repérer les erreurs.

Q9: Qu'est-ce que la protection contre les fuites DNS ?

La protection contre les fuites DNS oblige votre appareil à envoyer les requêtes de recherche de sites web (requêtes DNS) aux serveurs DNS privés et chiffrés du VPN plutôt qu'aux serveurs de votre FAI. Cela empêche votre FAI de suivre les sites que vous visitez.

Q10: Le VPN doit-il démarrer automatiquement ?

Généralement, oui. La plupart des applications peuvent se lancer au démarrage et se connecter automatiquement, ou sur un Wi-Fi non fiable, afin que vous soyez protégé avant que d'autres applications ne commencent à envoyer des données.

Partie 11 : 10 faits intéressants et enseignements concrets sur les VPN

Découvrez ces faits et informations concrets et précieux sur l'histoire, le marché et la technologie des VPN.

1. CLIENTS NATIFS

Windows et macOS incluent tous deux des clients VPN intégrés compatibles avec IKEv2 et L2TP/IPsec, si bien que de nombreuses connexions peuvent être configurées sans application supplémentaire.

2. GÉNÉRATION DE CLÉS

Le démarrage rapide de WireGuard crée une clé privée avec wg genkey et en dérive la clé publique avec wg pubkey. [2]

3. LA RÉVOLUTION WIREGUARD

WireGuard dispose d'un code très épuré, conçu pour l'efficacité, ce qui le rend plus facile à auditer que les protocoles traditionnels pour y rechercher des vulnérabilités. [1]

4. FICHIERS DE PROFIL

Un profil .ovpn regroupe l'adresse du serveur, le port, le protocole et les certificats : une seule importation suffit donc à configurer une connexion OpenVPN.

5. PORTS PAR DÉFAUT

OpenVPN utilise couramment le port 1194, tandis que les exemples officiels de WireGuard utilisent le port UDP 51820 ; il peut être nécessaire d'autoriser ces ports sur les pare-feu et les routeurs pour que le tunnel se connecte.

6. INSPECTION APPROFONDIE DES PAQUETS

L'inspection approfondie des paquets (DPI) peut repérer et bloquer les protocoles VPN courants ; passer à OpenVPN sur TCP port 443 ou à un mode obscurci peut aider.

7. COUVERTURE DES ROUTEURS

Un VPN installé sur le routeur protège tous les appareils qui y sont connectés, y compris les consoles et les téléviseurs connectés qui ne peuvent pas exécuter d'application VPN, sans rien installer sur chaque appareil.

8. KEEPALIVES

Derrière un NAT ou un pare-feu, le paramètre PersistentKeepalive de WireGuard, souvent réglé sur 25 secondes, maintient le tunnel joignable. [2]

9. PILOTES TUN/TAP

OpenVPN est conçu pour fonctionner avec l'interface réseau virtuelle TUN/TAP, disponible sur la plupart des plateformes et configurée lors de l'installation du client. [3]

10. TUNNEL FRACTIONNÉ (SPLIT TUNNELING)

Lors de la configuration, le split tunneling vous permet d'exclure du VPN certaines applications ou adresses, ce qui aide pour les imprimantes locales ou les applications qui bloquent les adresses IP de VPN.

Références techniques et sources

Publications citées, spécifications cryptographiques et normes documentaires officielles utilisées dans cette fiche.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

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

[2] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

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

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

Corrigé : configuration des VPN sous Windows, macOS, Android, iOS, Linux et sur les routeurs

1 Question 1

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quelle est la façon la plus simple de configurer un VPN sur un appareil mobile ? → Télécharger l'application VPN officielle depuis la boutique d'applications

2 Configuration de la passerelle sur le routeur

LATENCE

Bonne réponse : B

NOTE PÉDAGOGIQUE

Un VPN sur routeur chiffre le trafic au niveau de la passerelle, ce qui protège les objets connectés, les consoles et les appareils intelligents qui ne peuvent pas installer d'application VPN native. Source : DD-WRT OpenVPN Clients, Linksys Router Config.

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

Windows et macOS intègrent des clients pour des protocoles comme IKEv2 et L2TP/IPsec : une connexion peut donc être configurée sans installer de logiciel supplémentaire.

4 Import de profil OpenVPN

CONTRÔLES DU ROUTAGE

Bonne réponse : B

NOTE PÉDAGOGIQUE

Les configurations manuelles nécessitent de télécharger des profils.ovpn contenant les ports du serveur cible, les paramètres de protocole (UDP/TCP) et les certificats cryptographiques. Source : DD-WRT OpenVPN Clients.

5 Routage par tunnel fractionné

CONFIDENTIALITÉ

Bonne réponse : B

NOTE PÉDAGOGIQUE

Le tunnel fractionné permet aux utilisateurs de faire passer les applications de travail sensibles par le tunnel chiffré, tout en laissant le streaming local ou les jeux se connecter directement, sans la surcharge du VPN. Source : IETF IKEv2 RFC.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Configurer un routeur implique de se connecter à la page d'administration, de vérifier la prise en charge des VPN et d'importer des fichiers de configuration.

7 Intégration native au système d'exploitation

VITESSES

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les principaux systèmes d'exploitation intègrent nativement les protocoles afin de garantir une configuration fluide des connexions sécurisées. Source : Microsoft Native Gateway, Apple Support Profiles.

8 Appariement des clés WireGuard

RISQUE D'INTERCEPTION

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

WireGuard utilise des clés asymétriques pour établir des poignées de main P2P sécurisées au lieu de s'appuyer sur des mots de passe ou des chaînes d'autorités de certification. Citation : WireGuard CLI Specifications.

9 Blocages du trafic local

PARE-FEU

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Les VPN acheminent généralement le trafic Internet public et peuvent parfois bloquer l'accès aux imprimantes du réseau local, sauf configuration contraire. Citation : Microsoft Native Gateway.

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les serrures connectées qui ne peuvent pas exécuter d'applications VPN ont besoin d'un VPN au niveau du routeur pour être couvertes.

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

B 1. Application VPN	A 2. VPN sur routeur	E 3. Client natif	H 4. Profil .ovpn
G 5. Paire de clés	D 6. Tunnel fractionné (split tunneling)	F 7. Configuration du serveur DNS	C 8. Journaux de connexion

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 ROUTEUR	2 PROFIL OVPN	3 CLIENT NATIF	4 PAIRE DE CLÉS
5 APPLICATION VPN	6 DNS		

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

1 G – REGLAGESDNS	2 F – SPLITTUNNELING	3 B – VPNSURROUTEUR	4 E – PAIREDECLES
5 C – CLIENTNATIF	6 H – LOGSDECONNEXION	7 D – PROFILOVPN	8 A – APPLICATIONVPN

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Application VPN, VPN sur routeur et Client natif 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.

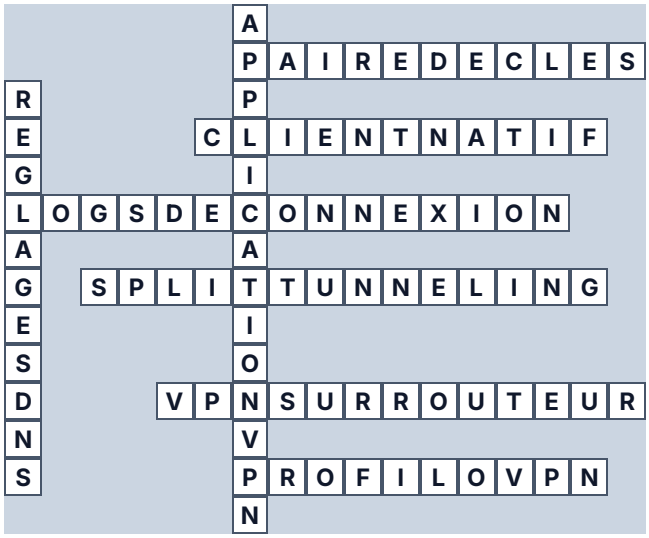
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

2 horizontal: PAIREDECLES Jetons cryptographiques (public/privé) nécessaires pour établir les échanges de clés WireGuard (11 lettres)

4 horizontal: CLIENTNATIF Sécurisation du trafic dans les paramètres natifs du système d'exploitation, sans installer d'application (11 lettres)

5 horizontal: LOGSDECONNEXION Consultation des messages d'erreur et des journaux d'état du client pour déboguer une configuration qui échoue (15 lettres)

6 horizontal: SPLITTUNNELING Différenciation des routes de trafic pour laisser certaines applications contourner le tunnel chiffré (14 lettres)

7 horizontal: VPNSURROUTEUR Chiffrement au niveau de la passerelle, qui protège tous les appareils connectés d'un réseau local (13 lettres)

8 horizontal: PROFILOVPN Format de fichier OpenVPN contenant les serveurs, les réglages de port et les clés de certificat (10 lettres)

VERTICALEMENT

1 vertical: APPLICATIONVPN Logiciel fourni par le service d'abonnement pour une installation simple en un clic (14 lettres)

3 vertical: REGLAGESDNS Configuration des adresses des résolveurs réseau pour éviter les fuites de résolution de noms de domaine (11 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. NCTOAPPIVAPNIL — **APPLICATIONVPN**
2. NFLCITITANE — **CLIENTNATIF**
3. PEDCIAESELR — **PAIREDECLES**
4. ENSGGADSREL — **REGLAGESDNS**
5. UEPNOURRTRVUS — **VPNSURROUTEUR**
6. PIFOVPRLNO — **PROFILOVPN**
7. LNESNPLGTINIUT — **SPLITTUNNELING**
8. NINSCNOOELOGEXD — **LOGSDECONNEXION**

CORRIGÉ DU DÉFI DU CODE SECRET

"INSTALLEZ LA PASSERELLE AVEC UN DEMON SECURISE"

Corrigé des études de cas

A Scénario A : sécurité sur un réseau public

INTERCEPTION ET CHIFFREMENT

Le dilemme de Sarah

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Risques : interception de paquets (packet sniffing), interception de données et attaques de l'homme du milieu. Une personne connectée au même réseau du café pourrait capturer ses identifiants de connexion ou son fichier de devoirs.
- Protection VPN : chiffre le contenu des paquets réseau, ce qui rend le trafic du tunnel intercepté illisible pour les espions passifs du réseau local lorsque le VPN est correctement configuré.

B Scénario B : accéder à des ressources bloquées

GÉOBLOCAGE ET IPS

Le dilemme d'Alex

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Pourquoi c'est bloqué : le service de streaming utilise le géoblocage, qui associe l'adresse IP locale du voyageur à son pays physique et la bloque en fonction des licences territoriales.
- Comment le VPN aide : il masque sa localisation réelle en acheminant le trafic par un serveur situé dans son pays d'origine. Le site voit une IP de ce pays et autorise l'accès.