Nom : _____ Date : _____ Note : _____

WireGuard ou OpenVPN Fiche de travail

Comparaison des protocoles WireGuard et OpenVPN : taille du code, vitesse et normes cryptographiques

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 la complexité du code et la rapidité d'audit des protocoles.
- Analysez les gains de performance liés à l'exécution dans l'espace noyau.
- Comparez les algorithmes de chiffrement d'OpenSSL avec la cryptographie moderne de WireGuard.
- Générer des paires de clés publique et privée pour les négociations entre pairs.
- Acheminez le trafic VPN par les ports TCP et UDP du pare-feu.

CONSIGNES DE LA FICHE DE COMPARAISON DES PROTOCOLES

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'audit des protocoles modernes. Terminez par l'activité bonus Réflexion rapide.

WIREGUARD OU OPENVPN (INTRODUCTION)

Choisir un protocole VPN exige de trouver un équilibre entre vitesse et options de configuration. OpenVPN est la norme depuis des décennies et offre la flexibilité d'une configuration TCP/UDP. WireGuard est un remplaçant moderne qui s'exécute directement dans l'espace noyau avec seulement 4,000 lignes de code. Comprendre les différences entre protocoles est essentiel pour optimiser vos réseaux sécurisés.

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

Point de contrôle 1 : Défi QCM

1 **1. Quelle est la taille approximative du code du protocole WireGuard ?**

- A. Environ 70 000 lignes
- B. Plus de 100,000 lignes
- C. Moins de 1 000 lignes
- D. Environ 4 000 lignes

2 **2. Dans quel espace du système d'exploitation WireGuard s'exécute-t-il ?**

- A. Espace utilisateur
- B. Espace noyau
- C. Espace applicatif
- D. Espace virtuel

3 **3. Sur quelle bibliothèque cryptographique OpenVPN s'appuie-t-il principalement ?**

- A. ChaCha20-Poly1305
- B. Bibliothèque cryptographique OpenSSL
- C. Framework de protocole Noise
- D. Encodage DES en clair

4 **4. Quel est l'un des principaux avantages de WireGuard sur OpenVPN en matière de performances ?**

- A. Établissement de connexion plus rapide et latence plus faible
- B. En se passant d'adresses IP publiques
- C. Prise en charge native intégrée des anciennes connexions par ligne commutée
- D. Aucune consommation de batterie sur les appareils mobiles

5 **5. Comment WireGuard authentifie-t-il les connexions entre pairs ?**

- A. En échangeant les mots de passe standard des utilisateurs
- B. En vérifiant les certificats d'enregistrement du domaine
- C. En utilisant des paires de clés publiques et privées statiques
- D. En vérifiant les numéros de série du matériel

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Le code compact de WireGuard le rend nettement plus facile à auditer.

- ◯ Vrai
- ◯ Faux

7 Question 7

7. OpenVPN est généralement plus rapide que WireGuard parce qu'il s'exécute dans l'espace noyau.

- ◯ Vrai
- ◯ Faux

8 Question 8

8. OpenVPN est très configurable et prend en charge les protocoles UDP et TCP.

- ◯ Vrai
- ◯ Faux

9 Question 9

9. WireGuard utilise une cryptographie moderne comme ChaCha20 pour un chiffrement rapide des paquets.

- ◯ Vrai
- ◯ Faux

10 Question 10

10. WireGuard nécessite des configurations complexes d'autorité de certification pour l'authentification.

- ◯ 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 protocole moderne _____ fonctionne directement dans le noyau du système d'exploitation.

2. Le protocole historique _____ repose sur la bibliothèque cryptographique OpenSSL.

3. Exécuter le code en _____ réduit la surcharge liée aux changements de contexte.

4. OpenVPN s'exécute en _____ et achemine les paquets via des interfaces virtuelles.

5. WireGuard utilise des _____ , publiques et privées, pour identifier les pairs de connexion.

6. Une base de code réduite améliore l' _____ de sécurité du logiciel.

BANQUE DE MOTS DE VOCABULAIRE

AUDITABILITÉ CODE COMPACT MODE NOYAU MODE UTILISATEUR OPENSSL
OPENVPN PAIRES DE CLÉS WIREGUARD

Écrivez vos réponses ici :

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

Point de contrôle 4 : Association de notions sur les réseaux

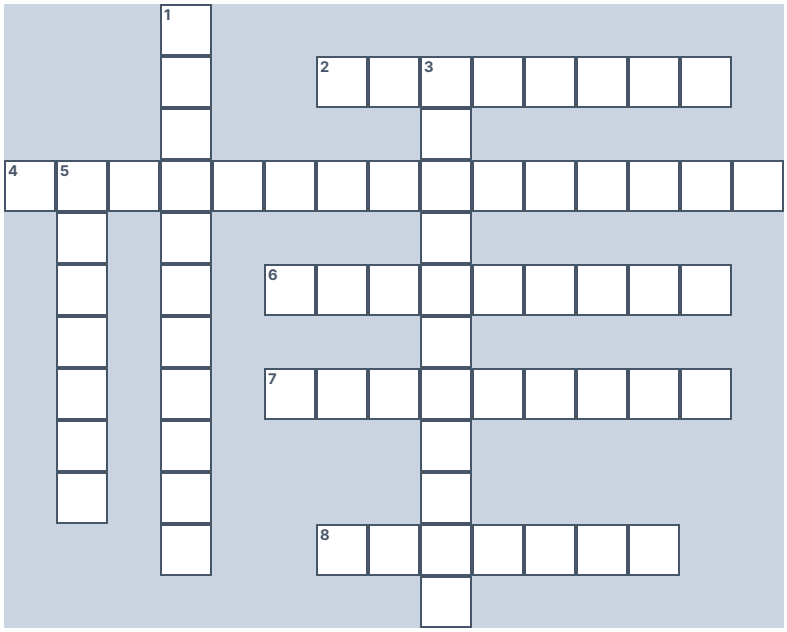
ASSOCIATION DE DÉFINITIONS

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. WireGuard	A	Espace d'exécution où fonctionne OpenVPN, ce qui entraîne une surcharge due aux changements de contexte.
☐	2. OpenVPN	B	La taille compacte du code de WireGuard, qui le rend beaucoup plus facile à auditer.
☐	3. Espace noyau	C	Bibliothèque cryptographique sur laquelle OpenVPN s'appuie pour ses algorithmes de chiffrement.
☐	4. Espace utilisateur	D	Protocoles de transport pris en charge par OpenVPN ; WireGuard fonctionne uniquement sur UDP.
☐	5. 4 000 LIGNES	E	Zone d'exécution du système d'exploitation où WireGuard s'exécute pour la vitesse.
☐	6. OpenSSL	F	Jetons asymétriques utilisés par WireGuard pour vérifier les connexions entre pairs.
☐	7. Paire de clés	G	Protocole VPN moderne conçu pour la vitesse et un audit simple du code.
☐	8. TCP/UDP	H	Protocole historique robuste reposant sur une base de code de configuration volumineuse et complexe.

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. Protocoles de transport pris en charge par OpenVPN ; WireGuard lui-même fonctionne uniquement sur UDP (8)

4. Zone d'exécution où s'exécute OpenVPN, ce qui entraîne une surcharge due aux changements de contexte (15)

6. Zone d'exécution du système d'exploitation où WireGuard s'exécute pour plus de rapidité (9)

7. Protocole VPN moderne conçu pour la vitesse et un audit simple du code (9)

8. Bibliothèque cryptographique sur laquelle OpenVPN s'appuie pour ses algorithmes de chiffrement (7)

VERTICALEMENT

1. Taille réduite de la base de code de WireGuard, qui la rend beaucoup plus facile à auditer (11)

3. Jetons asymétriques utilisés par WireGuard pour vérifier les connexions entre pairs (11)

5. Protocole historique robuste reposant sur une base de code de configuration vaste et complexe (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

2 horizontal: Protocoles de transport pris en charge par OpenVPN ; WireGuard lui-même fonctionne uniquement sur UDP (8 lettres):

4 horizontal: Zone d'exécution où s'exécute OpenVPN, ce qui entraîne une surcharge due aux changements de contexte (15 lettres):

6 horizontal: Zone d'exécution du système d'exploitation où WireGuard s'exécute pour plus de rapidité (9 lettres):

7 horizontal: Protocole VPN moderne conçu pour la vitesse et un audit simple du code (9 lettres):

8 horizontal: Bibliothèque cryptographique sur laquelle OpenVPN s'appuie pour ses algorithmes de chiffrement (7 lettres):

VERTICALEMENT

1 vertical: Taille réduite de la base de code de WireGuard, qui la rend beaucoup plus facile à auditer (11 lettres):

3 vertical: Jetons asymétriques utilisés par WireGuard pour vérifier les connexions entre pairs (11 lettres):

5 vertical: Protocole historique robuste reposant sur une base de code de configuration vaste et complexe (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.

I D R Z S F Q M V F A A Q O N

P R L T X Q K O R U C S D N Y

S A S B F S X D W J O A R Z Y

E U S Y L G I E M R D J M L T

L G N O H Q Q U H Z E A O V G

C E E U B Y R T Y B C H L Z G

E R P J O M O I P N O W C M Z

D I O Y P O G L Y O M W P U K

E W V P E D B I N V P T D M G

R V D Y N E U S K R A B U X Z

I Y M R V N Q A X I C P T D A

A D J Q P O V T W W T L E J H

P T H G N Y B E E I K T P S V

R Z E H E A S U C A L Q C C Z

M K V R U U A R S W J M T M H

LISTE DE MOTS DE VOCABULAIRE

WIREGUARD OPENVPN MODENOYAU MODEUTILISATEUR CODECOMPACT
OPENSSL PAIREDECLES TCPETUDP

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. WIREGUARD
B. OPENVPN
C. MODENOYAU
D. MODEUTILISATEUR
E. CODECOMPACT
F. OPENSSL
G. PAIREDECLES
H. TCPETUDP

DÉFINITIONS ET CHAMPS D'ASSOCIATION
_____ 1. Bibliothèque cryptographique sur laquelle OpenVPN s'appuie pour ses algorithmes de chiffrement.
_____ 2. Zone d'exécution du système d'exploitation où WireGuard s'exécute pour plus de rapidité.
_____ 3. Protocole historique robuste reposant sur une base de code de configuration vaste et complexe.
_____ 4. Jetons asymétriques utilisés par WireGuard pour vérifier les connexions entre pairs.
_____ 5. Protocoles de transport pris en charge par OpenVPN ; WireGuard lui-même fonctionne uniquement sur UDP.
_____ 6. Taille réduite de la base de code de WireGuard, qui la rend beaucoup plus facile à auditer.
_____ 7. Protocole VPN moderne conçu pour la vitesse et un audit simple du code.
_____ 8. Zone d'exécution où s'exécute OpenVPN, ce qui entraîne une surcharge due aux changements de contexte.

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. UGEIWARDR
2. UMAEOOYND
3. CMOPDOCTCAE
4. EESDIELCPAR
5. VNNEOPP
6. TIEDTLSURAMOIEU
7. OSSLPNE
8. ECTPTDUP

Activité bonus : Réflexion rapide

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

1	Raisons de choisir WireGuard			
2	Engagements d'un bon fournisseur de VPN			
3	Raisons de choisir OpenVPN			
4	Raisons d'utiliser un VPN en voyage			
5	Choses que votre fournisseur d'accès à Internet peut voir			
6	Façons de repérer un faux réseau Wi-Fi			
7	Idées reçues sur les VPN			
8	Endroits où vous utiliseriez un VPN			
9	Choses rapides de la vie quotidienne			
10	Choses contre lesquelles un VPN ne peut pas vous protéger			
11	Choses qui rendent le code plus facile à vérifier			
12	Choses qu'un VPN peut cacher			
13	Différences entre WireGuard et OpenVPN			
14	Mots liés à la vie privée			
15	Noms d'algorithmes de chiffrement que vous connaissez			

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 sur le Wi-Fi du café et mon application VPN me permet de choisir WireGuard ou OpenVPN. Mes appels vidéo n'arrêtent pas de se couper quand je passe du réseau du café au partage de connexion de mon téléphone. Quel protocole dois-je choisir, et pourquoi gérerait-il mieux ce changement ?"

ALEX (ÉTUDIANT VOYAGEUR)

👩‍💻 "Je suis à l'étranger, sur le réseau d'un hôtel qui semble bloquer la plupart du trafic VPN. WireGuard ne se connecte pas du tout, mais je dois accéder aux ressources de mon école restées au pays. Qu'est-ce qui est probablement bloqué, et comment OpenVPN pourrait-il m'aider à passer ?"

Point de contrôle 9 : Déchiffrer le code

Pour terminer votre formation sur l'audit des protocoles, déchiffrez ce message caché sur l'exécution dans l'espace noyau.

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

13	15	4	5	18	14	9	19	5	26		15	16	5	14	22	16	14
1	22	5	3		21	14		20	21	14	14	5	12		16	12	21	19
							18	1	16	9	4	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: Pourquoi les protocoles sont-ils importants ?

Le protocole détermine comment votre VPN construit son tunnel, quelle cryptographie protège vos données et à quelle vitesse il se connecte et se reconnecte. WireGuard et OpenVPN sont les deux protocoles open source que proposent la plupart des applications VPN, et ils font des compromis différents entre simplicité, vitesse et possibilités de configuration.

Q3: L'un est-il plus confidentiel que l'autre ?

Aucun des deux protocoles ne vous rend anonyme. Tous deux chiffrent le trafic du tunnel avec des algorithmes robustes ; votre confidentialité dépend surtout de ce que le fournisseur de VPN journalise et de la manière dont il gère les clés, les comptes et les serveurs.

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: Les deux sont-ils open source ?

Oui. WireGuard et l'édition communautaire d'OpenVPN publient tous deux leur code source, ce qui permet à des chercheurs indépendants de les examiner. La petite base de code de WireGuard rend un examen complet beaucoup plus rapide.

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: Lequel est le plus rapide ?

WireGuard est généralement plus rapide : il s'exécute dans le noyau, utilise le chiffrement léger ChaCha20-Poly1305 et réalise ses poignées de main rapidement. OpenVPN a plus de surcharge, mais les vitesses réelles dépendent aussi de la charge du serveur et de la distance.

Q7: Les deux peuvent-ils fonctionner en TCP et en UDP ?

Non. OpenVPN peut fonctionner sur UDP ou TCP, et le mode TCP aide sur les réseaux qui bloquent UDP. WireGuard envoie ses paquets uniquement en UDP : il peut donc échouer sur les réseaux qui n'autorisent que TCP. [4]

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 WireGuard et OpenVPN sur mon téléphone ?

Oui. WireGuard est multiplateforme, avec des applications pour Windows, macOS, Linux, iOS et Android, et des clients OpenVPN existent pour les mêmes systèmes. La plupart des applications VPN vous permettent de choisir l'un ou l'autre. [1]

Q10: Pourquoi WireGuard est-il si compact ?

WireGuard prend en charge un seul ensemble fixe d'algorithmes de chiffrement modernes au lieu de nombreuses options. Son implémentation Linux nécessite moins de 4 000 lignes de code, ce qui la rend plus facile à auditer que des bases de code VPN plus volumineuses. [3]

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: Quels algorithmes de chiffrement WireGuard utilise-t-il ?

WireGuard utilise ChaCha20 avec Poly1305 pour le chiffrement, Curve25519 pour l'échange de clés, BLAKE2s pour le hachage et le cadre Noise pour sa poignée de main. Il n'y a pas de négociation d'algorithme de chiffrement : les utilisateurs ne peuvent donc pas choisir une option faible. [2]

Q3: Quels algorithmes de chiffrement et bibliothèques OpenVPN peut-il utiliser ?

OpenVPN est étroitement intégré à la bibliothèque OpenSSL et utilise TLS pour échanger les clés. Les administrateurs peuvent choisir des algorithmes de chiffrement du canal de données comme AES-256-GCM, ce qui apporte de la souplesse mais laisse aussi place à des réglages faibles. [4]

Q4: Comment chaque protocole authentifie-t-il les pairs ?

Les pairs WireGuard s'identifient mutuellement par des clés publiques statiques, un peu comme l'échange de clés SSH, et chaque clé correspond à des IP de tunnel autorisées. OpenVPN repose généralement sur une autorité de certification avec des certificats X.509, souvent combinés à un nom d'utilisateur et un mot de passe.

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: Que se passe-t-il quand je passe du Wi-Fi aux données mobiles ?

WireGuard fonctionne sans connexion : il envoie les paquets depuis la nouvelle adresse et le tunnel continue après une rapide poignée de main. OpenVPN conserve un état de session ; un changement de réseau peut donc nécessiter une reconnexion un peu plus longue.

Q7: Comment fonctionne la confidentialité persistante (Perfect Forward Secrecy) ?

La PFS garantit qu'une clé de chiffrement unique et temporaire est générée pour chaque session. Même si une clé privée est compromise à l'avenir, elle ne peut pas servir à déchiffrer les sessions passées ou futures, car celles-ci utilisaient des clés indépendantes.

Q8: OpenVPN reste-t-il un bon choix si WireGuard est plus rapide ?

Oui. OpenVPN est mature et largement déployé, fonctionne en TCP lorsque l'UDP est bloqué et prend en charge les configurations d'entreprise basées sur des certificats. De nombreux fournisseurs proposent les deux protocoles pour que les utilisateurs puissent changer si l'un est bloqué ou lent.

Q9: Quels ports utilisent-ils ?

Le port standard d'OpenVPN est 1194, mais il peut être déplacé vers n'importe quel port UDP ou TCP, y compris 443. WireGuard écoute sur un port UDP défini dans sa configuration ; 51820 est le port utilisé dans ses exemples officiels.

Q10: Quel protocole est le plus facile à configurer à la main ?

WireGuard est généralement plus simple : générez une paire de clés, échangez les clés publiques et indiquez les IP autorisées. OpenVPN nécessite des certificats, une autorité de certification et davantage d'options, même si les profils .ovpn les regroupent dans un seul fichier.

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. PREMIER PROTOCOLE VPN

PPTP (Point-to-Point Tunneling Protocol) a été développé par un groupe de fournisseurs comprenant Microsoft et publié sous la forme de la RFC 2637 en juillet 1999 pour prendre en charge les VPN d'accès à distance. [6]

2. DEUX TRANSPORTS

OpenVPN peut faire passer son tunnel par UDP ou TCP et, en mode TLS, ses canaux de contrôle et de données partagent un seul port. [4]

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. [3]

4. CRYPTOGRAPHIE MODERNE

WireGuard combine ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 et HKDF dans le cadre du protocole Noise, sans choix d'algorithme de chiffrement sur lequel les utilisateurs pourraient se tromper. [2]

5. OPENSSL AU CŒUR D'OPENVPN

OpenVPN est étroitement intégré à la bibliothèque OpenSSL et en tire une grande partie de ses capacités cryptographiques, y compris le TLS utilisé pour échanger les clés. [4]

6. INSPECTION APPROFONDIE DES PAQUETS

L'inspection approfondie des paquets (DPI) examine le contenu des paquets et les schémas de trafic, pas seulement les en-têtes, et certains pare-feu l'utilisent pour détecter et bloquer les protocoles VPN courants.

7. CLÉS DE TYPE SSH

Les connexions WireGuard s'établissent par un simple échange de clés publiques, un peu comme l'échange de clés SSH, sans besoin d'autorité de certification. [1]

8. MULTIPLATEFORME

WireGuard a d'abord été publié pour le noyau Linux et est désormais disponible pour Windows, macOS, BSD, iOS et Android : le même protocole fonctionne donc sur la plupart des appareils. [1]

9. CONFIDENTIALITÉ PERSISTANTE (FORWARD SECRECY)

WireGuard répète sa poignée de main Noise_IK toutes les quelques minutes pour renouveler les clés de session symétriques, ce qui assure une confidentialité persistante parfaite (perfect forward secrecy) même si une clé à long terme venait à fuiter. [2]

10. INTERFACES TUN/TAP

OpenVPN est conçu pour fonctionner avec l'interface réseau virtuelle TUN/TAP, disponible sur la plupart des plateformes, qui transporte les paquets du tunnel. [4]

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.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[3] 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/

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

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

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Corrigé : comparaison des protocoles WireGuard et OpenVPN, de la taille de leur code, de leur vitesse et de leurs normes cryptographiques

1 Taille du code de WireGuard

PROTOCOLES

Bonne réponse : D

NOTE PÉDAGOGIQUE

WireGuard est extrêmement compact : il tient en environ 4 000 lignes de code. Cela réduit la surface d'attaque et facilite les audits. Citation : WireGuard Project.

2 Vitesse en espace noyau

LATENCE

Bonne réponse : B

NOTE PÉDAGOGIQUE

En s'exécutant directement dans l'espace noyau, WireGuard évite la charge liée aux changements de contexte, ce qui permet un débit élevé. Source : WireGuard Project.

3 Question 3

Bonne réponse : B

NOTE PÉDAGOGIQUE

OpenVPN est étroitement intégré à OpenSSL, qui fournit des algorithmes de chiffrement comme AES-GCM et le rend très configurable mais plus complexe.

4 Performances du protocole

CONTRÔLES DU ROUTAGE

Bonne réponse : A

NOTE PÉDAGOGIQUE

WireGuard établit ses poignées de main en quelques millisecondes et réagit instantanément à l'itinérance réseau (par ex. le passage du Wi-Fi au réseau cellulaire). Citation : Microsoft Native Gateway, Apple Support.

5 Cryptographie asymétrique

CONFIDENTIALITÉ

Bonne réponse : C

NOTE PÉDAGOGIQUE

WireGuard utilise le Cryptokey Routing, qui associe des clés publiques à des adresses IP de tunnel autorisées, de façon semblable aux configurations SSH. Citation : WireGuard Project.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

L'implémentation Linux de WireGuard compte moins de 4,000 lignes : les équipes de sécurité peuvent donc l'examiner bien plus vite que des codes VPN beaucoup plus volumineux comme OpenVPN.

7 Latence en espace utilisateur VITESSES

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

OpenVPN s'exécute dans l'espace utilisateur et fait transiter les paquets dans les deux sens par l'interface virtuelle du noyau, ce qui ajoute une surcharge de changement de contexte (sauf si un déchargement vers le noyau comme OpenVPN DCO est utilisé). Source : DD-WRT custom firmware.

8 Configuration OpenVPN RISQUE D'INTERCEPTION

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

OpenVPN peut fonctionner sur TCP (pour la fiabilité et le contournement des pare-feu) ou sur UDP (pour la vitesse), ce qui le rend compatible avec les pare-feu d'entreprise complexes. Source : IETF Cryptographic Protocols.

9 Cryptographie moderne PARE-FEU

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

WireGuard abandonne les anciens algorithmes de chiffrement au profit de primitives modernes et sûres comme ChaCha20 et Poly1305, qui s'exécutent rapidement sur les processeurs mobiles. Citation : WireGuard Project.

10 Simplification des paires de clés SANS JOURNAUX

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

WireGuard n'utilise ni certificats ni hiérarchies d'autorités de certification complexes; il repose sur de simples paires de clés publique/privée échangées entre pairs. Citation : WireGuard Project.

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. WireGuard	H 2. OpenVPN	E 3. Espace noyau	A 4. Espace utilisateur
B 5. 4 000 LIGNES	C 6. OpenSSL	F 7. Paire de clés	D 8. TCP/UDP

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 WIREGUARD	2 OPENVPN	3 MODE NOYAU	4 MODE UTILISATEUR
5 PAIRES DE CLÉS	6 AUDITABILITÉ		

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

1 F – OPENSSL	2 C – MODENOYAU	3 B – OPENVPN	4 G – PAIREDECLES
5 H – TCPETUDP	6 E – CODECOMPACT	7 A – WIREGUARD	8 D – MODEUTILISATEUR

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer WireGuard, OpenVPN et Espace noyau 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.

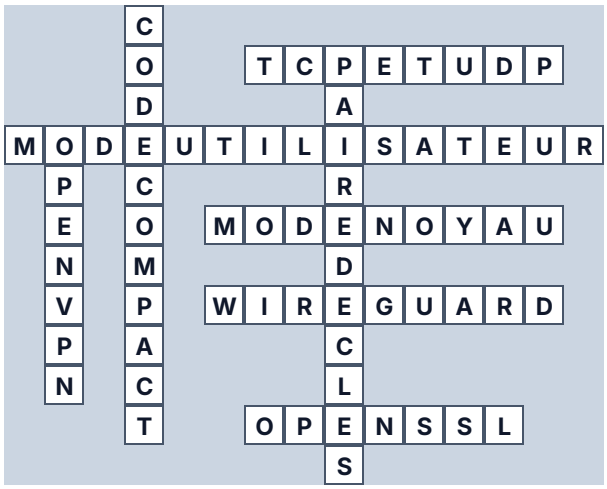
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

2 horizontal: TCPETUDP Protocoles de transport pris en charge par OpenVPN ; WireGuard lui-même fonctionne uniquement sur UDP (8 lettres)

4 horizontal: MODEUTILISATEUR Zone d'exécution où s'exécute OpenVPN, ce qui entraîne une surcharge due aux changements de contexte (15 lettres)

6 horizontal: MODENOYAU Zone d'exécution du système d'exploitation où WireGuard s'exécute pour plus de rapidité (9 lettres)

7 horizontal: WIREGUARD Protocole VPN moderne conçu pour la vitesse et un audit simple du code (9 lettres)

8 horizontal: OPENSSL Bibliothèque cryptographique sur laquelle OpenVPN s'appuie pour ses algorithmes de chiffrement (7 lettres)

VERTICALEMENT

1 vertical: CODECOMPACT Taille réduite de la base de code de WireGuard, qui la rend beaucoup plus facile à auditer (11 lettres)

3 vertical: PAIREDECLES Jetons asymétriques utilisés par WireGuard pour vérifier les connexions entre pairs (11 lettres)

5 vertical: OPENVPN Protocole historique robuste reposant sur une base de code de configuration vaste et complexe (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. UGEIWARDR — **WIREGUARD**
2. UMAEOOYND — **MODENOYAU**
3. CMOPDOCTCAE — **CODECOMPACT**
4. EESDIELCPAR — **PAIREDECLES**
5. VNNEOPP — **OPENVPN**
6. TIEDTLSURAMOIEU — **MODEUTILISATEUR**
7. OSSLPNE — **OPENSSL**
8. ECTPTDUP — **TCPETUDP**

CORRIGÉ DU DÉFI DU CODE SECRET

"MODERNISEZ OPENVPN AVEC UN TUNNEL PLUS RAPIDE"

Corrigé des études de cas

A Scénario A : choisir un protocole

INTERCEPTION ET CHIFFREMENT | Le dilemme de Sarah

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Recommandation : WireGuard. Sa conception légère et sans connexion permet au tunnel de se rétablir rapidement quand son réseau change, et ChaCha20-Poly1305 assure un chiffrement rapide.
- Sécurité : les deux protocoles chiffrent son trafic sur le Wi-Fi du café ; l'un ou l'autre protège donc ses identifiants s'il est correctement configuré ; le choix influe surtout sur la vitesse et la stabilité.

B Scénario B : contourner les blocages de VPN

GÉOBLOCAGE ET IPS | Le dilemme d'Alex

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Pourquoi c'est bloqué : WireGuard utilise uniquement l'UDP, et le pare-feu de l'hôtel bloque probablement l'UDP ou reconnaît les paquets WireGuard par filtrage ou par inspection approfondie des paquets (DPI).
- Comment OpenVPN aide : il peut fonctionner via TCP, notamment sur le port 443 utilisé par HTTPS, que les pare-feu des hôtels bloquent rarement complètement car la navigation web en dépend.