Nom : _____ Date : _____ Note : _____

Proxy ou VPN Fiche de travail

Comparaison des serveurs proxy et des réseaux privés virtuels : différences de chiffrement, et routage par application ou pour tout le système

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 proxys d'application avec le chiffrement VPN pour tout le système.
- Identifier les capacités de SOCKS5 par rapport aux proxys HTTP de base.
- Analysez comment les proxys basés sur le navigateur laissent les applications d'arrière-plan exposées.
- Comprendre comment les FAI enregistrent le trafic non chiffré dans les tunnels de proxy.
- Choisissez le bon outil de routage en fonction de vos besoins de vitesse et de sécurité.

CONSIGNES DE LA FICHE DE COMPARAISON DES PROXYS

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 comparaison des proxys et des VPN. Terminez par l'activité bonus Réflexion rapide.

PROXY OU VPN (INTRODUCTION)

Les proxys et les VPN remplissent des fonctions différentes en matière de vie privée numérique. Un serveur proxy agit comme une redirection au niveau de la couche application : il masque votre adresse IP pour certains programmes sans chiffrer les données. Un VPN agit au niveau du réseau et sécurise tout le trafic du système par le chiffrement. Le bon outil dépend de vos besoins de sécurité.

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

Point de contrôle 1 : Défi QCM

1. À quelle couche du modèle OSI un proxy HTTP standard fonctionne-t-il ?

- A. Couche physique
- B. Couche réseau
- C. Couche application
- D. Couche liaison de données

2. Quel est l'un des principaux avantages du protocole SOCKS5 par rapport aux proxys HTTP standard ?

- A. Il impose le chiffrement intégral des données
- B. Il prend en charge l'acheminement de tout trafic TCP/UDP
- C. Il est insensible aux fuites DNS
- D. Il fonctionne directement dans l'espace noyau

3. Pourquoi un VPN est-il généralement plus sûr qu'un serveur proxy ?

- A. Il fonctionne sur du matériel distant plus rapide
- B. Il chiffre tout le trafic réseau à l'échelle du système
- C. Il ne nécessite pas de tables de routage locales
- D. Il supprime complètement la latence du réseau

4. Quel type de proxy redirige le trafic sans aucun chiffrement par défaut ?

- A. Un proxy HTTP basique
- B. Un proxy HTTPS chiffré
- C. Un client WireGuard sécurisé
- D. Un serveur VPN obfusqué

5. Qu'advient-il du trafic des applications en arrière-plan lorsque vous utilisez un proxy de navigateur ?

- A. Il est chiffré automatiquement
- B. Il est bloqué par le serveur proxy
- C. Il passe par le tunnel du proxy
- D. Il contourne le proxy et expose votre IP

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Un proxy SOCKS5 chiffre le contenu de tous les paquets qui transitent par le serveur.

- ○ Vrai
- ○ Faux

7 Question 7

7. Un VPN fonctionne au niveau de la couche réseau pour sécuriser tout le trafic du système.

- ○ Vrai
- ○ Faux

8 Question 8

8. Les proxys sont généralement plus rapides que les VPN parce qu'ils effectuent un chiffrement approfondi des paquets.

- ○ Vrai
- ○ Faux

9 Question 9

9. Configurer un proxy nécessite de mettre en place des redirections de trafic dans certaines applications.

- ○ Vrai
- ○ Faux

10 Question 10

10. Utiliser un proxy ne protège pas votre trafic de données contre le pistage par le FAI local.

- ○ 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. Un _____ de couche application redirige le trafic de certains navigateurs sans sécuriser les autres applications.

2. Un _____ robuste encapsule et chiffre tous les paquets de données de l'appareil.

3. Le protocole _____ se situe entre les couches application et transport.

4. Les proxys HTTP fonctionnent au niveau de la couche _____ du modèle OSI.

5. Les serveurs proxy standard n'assurent pas le _____ des données utiles, ce qui les laisse vulnérables.

6. Un VPN offre une protection couvrant _____ pour toutes les cartes réseau.

BANQUE DE MOTS DE VOCABULAIRE

APPLICATION CHIFFREMENT COMPATIBLE UDP PROXY SOCKS5
TOUT LE SYSTÈME TUNNEL VPN VISIBILITÉ DU FAI

Écrivez vos réponses ici :

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

Point de contrôle 4 : Association de notions sur les réseaux

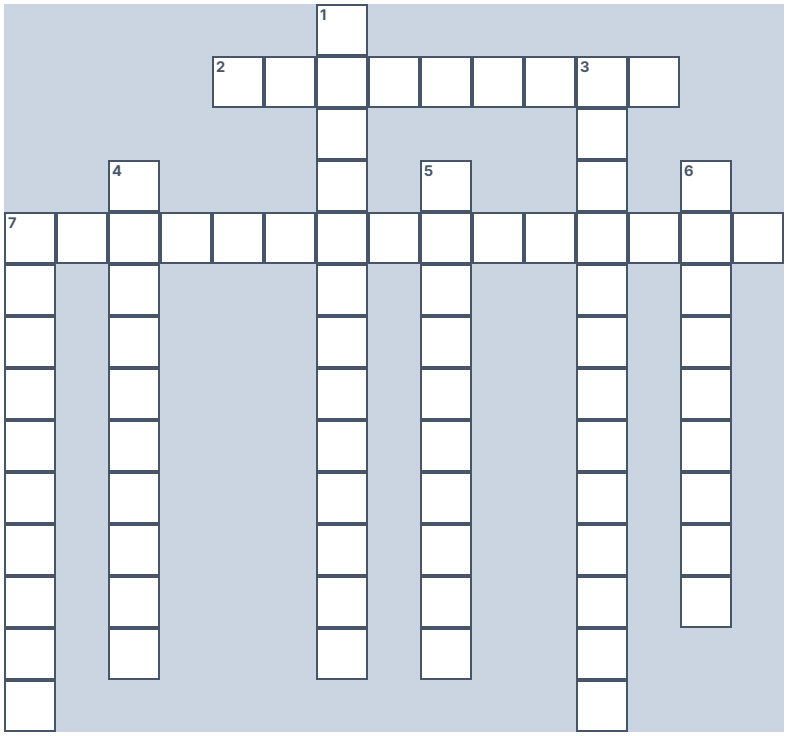
ASSOCIATION DE DÉFINITIONS

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. Proxy HTTP	A	Routage au niveau du système d'exploitation qui chiffre le trafic de toutes les applications.
☐	2. Proxy SOCKS5	B	La couche Application, où fonctionnent les protocoles de proxy web standard.
☐	3. Tunnel VPN	C	La capacité de SOCKS5 à relayer l'UDP comme le TCP, contrairement aux simples proxys HTTP.
☐	4. À l'échelle du système :	D	Extension cliente qui ne masque que le trafic à l'intérieur du bac à sable du navigateur.
☐	5. Couche OSI 7	E	Chiffrement et encapsulation enveloppant tout le trafic de l'appareil en arrière-plan.
☐	6. Prise en charge d'UDP	F	État du trafic dans lequel les données de proxy non chiffrées restent visibles pour les FAI.
☐	7. Proxy de navigateur	G	Proxy de la couche application qui redirige le trafic d'un navigateur web précis.
☐	8. Visibilité du FAI	H	Protocole de proxy situé entre la couche application et la couche transport, sans chiffrement.

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. Proxy de couche application qui redirige le trafic d'un navigateur web donné (9)

7. Extension client qui ne masque que le trafic à l'intérieur du bac à sable du navigateur (15)

VERTICALEMENT

1. Capacité de SOCKS5 à relayer l'UDP aussi bien que le TCP, contrairement aux simples proxys HTTP (13)

3. Routage au niveau du système d'exploitation qui chiffre le trafic de toutes les applications (13)

4. Couche application, où fonctionnent les protocoles de proxy web standard (10)

5. État du trafic dans lequel les données de proxy non chiffrées restent visibles pour les FAI (10)

6. Chiffrement et encapsulation enveloppant tout le trafic d'arrière-plan de l'appareil (9)

7. Protocole de proxy situé entre les couches application et transport, sans chiffrement (10)

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: Proxy de couche application qui redirige le trafic d'un navigateur web donné (9 lettres):

7 horizontal: Extension client qui ne masque que le trafic à l'intérieur du bac à sable du navigateur (15 lettres):

VERTICALEMENT

1 vertical: Capacité de SOCKS5 à relayer l'UDP aussi bien que le TCP, contrairement aux simples proxys HTTP (13 lettres):

3 vertical: Routage au niveau du système d'exploitation qui chiffre le trafic de toutes les applications (13 lettres):

4 vertical: Couche application, où fonctionnent les protocoles de proxy web standard (10 lettres):

5 vertical: État du trafic dans lequel les données de proxy non chiffrées restent visibles pour les FAI (10 lettres):

6 vertical: Chiffrement et encapsulation enveloppant tout le trafic d'arrière-plan de l'appareil (9 lettres):

7 vertical: Protocole de proxy situé entre les couches application et transport, sans chiffrement (10 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.

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

LISTE DE MOTS DE VOCABULAIRE

PROXYHTTP PROXYSOCKS TUNNELVPN TOUTLESYSTEME COUCHESEPT
COMPATIBLEUDP PROXYNAVIGATEUR VISIBILITE

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. PROXYHTTP
B. PROXYSOCKS
C. TUNNELVPN
D. TOUTLESYSTEME
E. COUCHESEPT
F. COMPATIBLEUDP
G. PROXYNAVIGATEUR
H. VISIBILITE

DÉFINITIONS ET CHAMPS D'ASSOCIATION

_____ 1. Couche application, où fonctionnent les protocoles de proxy web standard.

_____ 2. Capacité de SOCKS5 à relayer l'UDP aussi bien que le TCP, contrairement aux simples proxys HTTP.

_____ 3. Proxy de couche application qui redirige le trafic d'un navigateur web donné.

_____ 4. Extension client qui ne masque que le trafic à l'intérieur du bac à sable du navigateur.

_____ 5. Chiffrement et encapsulation enveloppant tout le trafic d'arrière-plan de l'appareil.

_____ 6. Routage au niveau du système d'exploitation qui chiffre le trafic de toutes les applications.

_____ 7. État du trafic dans lequel les données de proxy non chiffrées restent visibles pour les FAI.

_____ 8. Protocole de proxy situé entre les couches application et transport, sans chiffrement.

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. HYXRPTTPO
2. NTPNULVEN
3. CEPSOHTCEU
4. AUAXRIGNRV ETPOY
5. CSSRXOYPKO
6. LTSEEUMSTO YET
7. EUBTCOLAPD MIP
8. TIIEVBILIS

Activité bonus : Réflexion rapide

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

1	Différences entre un proxy et un VPN			
2	Choses qui restent non chiffrées sans VPN			
3	Façons de repérer un faux réseau Wi-Fi			
4	Choses que fait un intermédiaire dans la vie quotidienne			
5	Situations où un proxy suffit			
6	Appareils pouvant utiliser un VPN			
7	Types de proxys que vous connaissez			
8	Choses qu'un VPN peut cacher			
9	Idées reçues sur les VPN			
10	Engagements d'un bon fournisseur de VPN			
11	Choses contre lesquelles un VPN ne peut pas vous protéger			
12	Mots de cette fiche que vous voulez retenir			
13	Raisons d'utiliser un VPN en voyage			
14	Situations où vous voulez un VPN			
15	Endroits où vous utiliseriez un VPN			

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 sur un réseau ouvert appelé 'Free_Wi-Fi_No_Password'. Je dois me connecter à ma messagerie scolaire, et un ami dit qu'un proxy de navigateur gratuit suffit pour rester en sécurité. Un proxy protégerait-il mes identifiants et mes fichiers, ou ai-je besoin d'un VPN ?"

ALEX (ÉTUDIANT VOYAGEUR)

👩‍💻 "Je suis à l'étranger, et un documentaire de biologie hébergé dans mon pays d'origine affiche : 'Cette vidéo n'est pas disponible dans votre pays.' Un camarade utilise un proxy, et moi j'ai un VPN. Pourquoi suis-je bloqué, et quel outil fonctionnerait le mieux ?"

Point de contrôle 9 : Déchiffrer le code

Pour terminer votre formation sur la comparaison des proxys, déchiffrez ce message secret sur les 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

18	5	4	9	18	9	7	5	26		22	15	20	18	5

20	18	1	6	9	3		1	22	5	3		21	14		16	18	15	24	25

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: Qu'est-ce qu'un serveur proxy ?

Un serveur proxy est un intermédiaire qui transmet les requêtes entre votre application et le serveur de destination. Le site web voit l'adresse IP du proxy au lieu de la vôtre, mais seul le trafic des applications configurées pour utiliser le proxy est redirigé, et un proxy basique ne chiffre pas ce trafic.

Q3: Un VPN me rend-il complètement anonyme en ligne ?

Non. Même si un VPN masque votre adresse IP et chiffre votre trafic, vous pouvez toujours être pisté via les cookies du navigateur, les comptes actifs (comme Google ou Facebook), l'empreinte du navigateur, ou si votre fournisseur de VPN journalise vos données.

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: Un proxy est-il un VPN ?

Non. Un proxy relaie le trafic de certaines applications, généralement sans chiffrement. Un VPN crée un tunnel chiffré au niveau de la couche réseau qui transporte tout le trafic de l'appareil, y compris celui des applications en arrière-plan.

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 proxy gratuit ?

Vous le pouvez, mais les proxys gratuits sont souvent gérés par des opérateurs inconnus. Comme un proxy basique ne chiffre pas le trafic, son opérateur peut voir et même modifier les pages non chiffrées. Vérifiez qui gère le service avant de l'utiliser.

Q7: Un proxy conserve-t-il des journaux ?

Oui, c'est possible. Un proxy traite chaque requête qu'il transmet ; son opérateur peut donc enregistrer votre adresse IP, les sites que vous visitez et à quel moment. Vérifiez qui l'exploite et ce que dit sa politique de confidentialité.

Q8: Quand un proxy suffit-il ?

Un proxy peut suffire pour des tâches à faible risque, comme modifier l'emplacement apparent d'un navigateur. Pour les opérations bancaires, le Wi-Fi public ou la protection de toutes les applications d'un appareil, un VPN est le choix le plus sûr, car il chiffre tout le trafic.

Q9: Un proxy peut-il protéger toutes les applications de mon téléphone ?

Non. Seules les applications qui respectent le paramètre de proxy l'utilisent ; les autres se connectent directement. Une application VPN, elle, fait passer toutes les applications du téléphone par son tunnel chiffré.

Q10: Qu'est-ce qu'un proxy SOCKS5 ?

SOCKS5, défini dans la RFC 1928, est un protocole de proxy situé entre la couche application et la couche transport. Il peut relayer des connexions TCP et des datagrammes UDP et prend en charge l'authentification, mais il ne dispose d'aucun chiffrement intégré. [1]

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: À quelles couches réseau les proxys et les VPN fonctionnent-ils ?

Un proxy HTTP fonctionne au niveau de la couche application (couche 7) et comprend les requêtes web. SOCKS5 se situe entre la couche application et la couche transport. Les protocoles VPN comme IPsec ou WireGuard fonctionnent au niveau de la couche réseau : ils peuvent donc transporter tout le trafic IP de l'appareil.

Q2: Un site HTTPS reste-t-il chiffré lorsqu'on passe par un proxy ?

Oui. Lorsque vous ouvrez un site HTTPS via un proxy, le chiffrement TLS fonctionne de bout en bout entre votre navigateur et le site, de sorte que le proxy voit le domaine mais pas le contenu des pages. Les pages en HTTP simple restent lisibles.

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: Qu'est-ce qu'un proxy transparent et qui l'utilise ?

Un proxy transparent intercepte le trafic sans aucune configuration sur l'appareil de l'utilisateur. Les écoles, les entreprises et les FAI les utilisent pour la mise en cache ou le filtrage de contenus. Les utilisateurs ignorent souvent sa présence, et il ne leur offre aucune confidentialité.

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: Pourquoi un proxy peut-il sembler plus rapide qu'une connexion VPN ?

Un proxy basique ne chiffre rien et ne gère que le trafic d'une seule application : il demande donc moins de traitement. Un VPN chiffre chaque paquet de l'appareil. Avec les protocoles modernes, la différence est souvent faible, et le proxy offre une protection bien moindre.

Q8: Les sites web peuvent-ils savoir que j'utilise un proxy ou un VPN ?

Souvent, oui. De nombreux sites comparent les adresses IP à des listes de serveurs proxy et VPN connus, et les proxys HTTP peuvent ajouter des en-têtes comme Via ou X-Forwarded-For. Les services de streaming bloquent couramment les deux.

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: Un proxy peut-il empêcher le bridage par le FAI ?

Rarement. Un proxy basique ne chiffre pas le trafic, donc le FAI peut toujours voir de quel type d'activité il s'agit. Un VPN masque les types de trafic, mais aucun des deux outils ne règle la congestion ni les plafonds de 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. STANDARD SOCKS

La version 5 du protocole SOCKS a été publiée par l'IETF sous la référence RFC 1928 en mars 1996 et reste aujourd'hui la spécification de référence des proxys SOCKS5 utilisés par les navigateurs et les applications. [1]

2. COUCHE D'INTERCALAGE (SHIM)

La RFC 1928 décrit SOCKS comme une couche intermédiaire entre la couche application et la couche transport ; il ne peut donc pas transmettre le trafic de la couche réseau, comme l'ICMP. [1]

3. RELAIS UDP

SOCKS5 a ajouté la commande UDP ASSOCIATE, qui permet à un proxy de relayer des datagrammes UDP ainsi que des connexions TCP, ce que les simples proxys HTTP ne gèrent pas. [1]

4. PORT SOCKS PAR DÉFAUT

Les clients SOCKS5 se connectent par défaut au serveur proxy sur le port TCP 1080, comme le définit la RFC 1928 ; de nombreux services de proxy permettent aux utilisateurs de choisir d'autres ports. [1]

5. INTERMÉDIAIRES HTTP

La norme HTTP (RFC 9110) définit un proxy comme un agent de transfert de messages choisi par le client, qui relaie les requêtes vers le serveur d'origine.

6. INSPECTION APPROFONDIE DES PAQUETS

L'inspection approfondie des paquets (DPI) examine le contenu des paquets et les schémas de trafic ; le trafic de proxy non chiffré lui est entièrement visible, alors que le trafic VPN en révèle beaucoup moins.

7. VPN DE COUCHE RÉSEAU

IPsec, décrit dans la publication NIST SP 800-77, protège le trafic au niveau de la couche réseau : les paquets IP de toutes les applications peuvent donc être sécurisés sans configuration application par application. [2]

8. PORTÉE LIMITÉE AU NAVIGATEUR

Un proxy configuré dans un navigateur n'affecte que ce navigateur ; les clients de messagerie, les jeux et les mises à jour du système continuent d'utiliser la connexion normale de l'appareil.

9. TOR OU PROXYS

Tor fait passer le trafic par trois relais bénévoles (garde, intermédiaire et sortie) et s'utilise généralement via un proxy SOCKS local, ce qui ajoute des couches qu'un proxy unique ne peut pas offrir.

10. COMPROMIS DE VITESSE

Les proxys peuvent sembler plus rapides parce qu'ils ne chiffrent pas, mais les protocoles VPN modernes comme WireGuard ajoutent peu de surcharge tout en protégeant tout le trafic de l'appareil.

Références techniques et sources

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

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Corrigé : comparaison des serveurs proxy et des réseaux privés virtuels, des différences de chiffrement et du routage par application ou pour tout le système

1 Couche OSI du proxy

PROTOCOLES

Bonne réponse : C

NOTE PÉDAGOGIQUE

Les proxys HTTP/HTTPS standard fonctionnent au niveau de la couche application (couche 7) et redirigent le trafic de navigateurs spécifiques. Ils n'offrent pas de routage réseau à l'échelle du système. Source : Tor Project Foundation.

2 Question 2

Bonne réponse : B

NOTE PÉDAGOGIQUE

SOCKS5 relaie le trafic TCP et UDP entre la couche application et la couche transport mais ne chiffre pas par défaut, tandis que les proxys HTTP traitent les requêtes web.

3 Chiffrement du système VPN

SÉCURITÉ WI-FI

Bonne réponse : B

NOTE PÉDAGOGIQUE

Un VPN encapsule et chiffre l'ensemble du trafic du système d'exploitation, alors qu'un proxy ne redirige que le trafic des applications spécifiquement configurées. Source : Deloitte Advisory.

4 Absence de chiffrement du proxy

CONTRÔLES DU ROUTAGE

Bonne réponse : A

NOTE PÉDAGOGIQUE

Les proxys HTTP transmettent le trafic du navigateur au niveau de la couche application sans chiffrer le contenu des paquets : votre opérateur réseau ou votre FAI peut donc toujours suivre votre trafic. Source : IETF Proxy Vulnerabilities.

5 Vulnérabilité de contournement

CONFIDENTIALITÉ

Bonne réponse : D

NOTE PÉDAGOGIQUE

Les proxys de navigateur n'appliquent leurs règles qu'au navigateur lui-même. Les applications d'arrière-plan, les mises à jour du système d'exploitation et les clients de messagerie contournent le proxy, ce qui expose votre adresse IP réelle. Source : W3C Consortium.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

SOCKS5 relaie le trafic entre la couche application et la couche transport mais n'effectue aucun chiffrement par défaut : le contenu des paquets reste donc lisible en transit.

7 Tunnels de la couche réseau VITESSES

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

En fonctionnant au niveau de la couche réseau, un VPN achemine et chiffre le trafic sortant de votre appareil, ce qui aide à protéger le trafic de tout le système. Source : Deloitte Advisory.

8 Limite de chiffrement du proxy RISQUE D'INTERCEPTION

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Les proxys peuvent parfois être plus rapides, mais c'est parce qu'ils n'effectuent PAS de chiffrement. Cette absence de chiffrement expose les données à l'inspection. Source : IETF Proxy Vulnerabilities.

9 Redirection au niveau des applications PARE-FEU

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Contrairement aux VPN qui couvrent tout le système, les serveurs proxy nécessitent une configuration manuelle dans les réglages du navigateur ou dans les champs proxy propres à chaque application. Citation : W3C Consortium.

10 Risque de pistage par le FAI SANS JOURNAUX

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Comme les proxys HTTP/SOCKS5 standard ne chiffrent pas les données utiles, votre FAI local conserve une visibilité complète sur vos activités en ligne. Source : EDRi Retention Guidelines.

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. Proxy HTTP	H 2. Proxy SOCKS5	E 3. Tunnel VPN	A 4. À l'échelle du système :
B 5. Couche OSI 7	C 6. Prise en charge d'UDP	D 7. Proxy de navigateur	F 8. Visibilité du FAI

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 PROXY	2 TUNNEL VPN	3 SOCKS5	4 APPLICATION
5 CHIFFREMENT	6 TOUT LE SYSTÈME		

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

1 E – COUCHESEPT	2 F – COMPATIBLEUDP	3 A – PROXYHTTP	4 G – PROXYNAVIGATEUR
5 C – TUNNELVPN	6 D – TOUTLESYSTEME	7 H – VISIBILITE	8 B – PROXYSOCKS

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Proxy HTTP, Proxy SOCKS5 et Tunnel VPN 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.

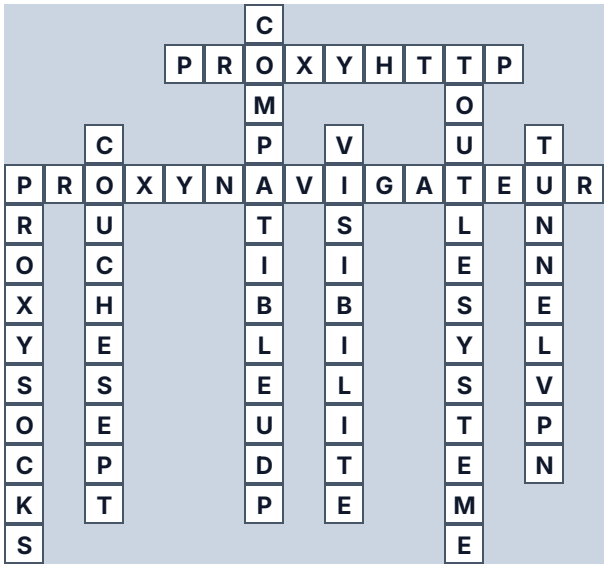
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

2 horizontal: PROXYHTTP Proxy de couche application qui redirige le trafic d'un navigateur web donné (9 lettres)

7 horizontal: PROXYNAVIGATEUR Extension client qui ne masque que le trafic à l'intérieur du bac à sable du navigateur (15 lettres)

VERTICALEMENT

1 vertical: COMPATIBLEUDP Capacité de SOCKS5 à relayer l'UDP aussi bien que le TCP, contrairement aux simples proxys HTTP (13 lettres)

3 vertical: TOUTLESYSTEME Routage au niveau du système d'exploitation qui chiffre le trafic de toutes les applications (13 lettres)

4 vertical: COUCHESEPT Couche application, où fonctionnent les protocoles de proxy web standard (10 lettres)

5 vertical: VISIBILITE État du trafic dans lequel les données de proxy non chiffrées restent visibles pour les FAI (10 lettres)

6 vertical: TUNNELVPN Chiffrement et encapsulation enveloppant tout le trafic d'arrière-plan de l'appareil (9 lettres)

7 vertical: PROXYSOCKS Protocole de proxy situé entre les couches application et transport, sans chiffrement (10 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. HYXRPTTPO — **PROXYHTTP**
2. NTPNULVEN — **TUNNELVPN**
3. CEPSOHTCEU — **COUCHESEPT**
4. AUAXRIGNRVETPOY — **PROXYNAVIGATEUR**
5. CSSRXOYPKO — **PROXYSOCKS**
6. LTSEEUMSTOYET — **TOUTLESYSTEME**
7. EUBTCOLAPDMIP — **COMPATIBLEUDP**
8. TIIEVBILIS — **VISIBILITE**

CORRIGÉ DU DÉFI DU CODE SECRET

"REDIRIGEZ VOTRE TRAFIC AVEC UN PROXY"

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.
- Proxy ou VPN : un simple proxy de navigateur ne chiffre pas son trafic. Un VPN chiffre tout sur l'appareil, ce qui rend les paquets interceptés illisibles pour les espions locaux.

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.
- Quelle solution fonctionne le mieux : les deux lui donnent une IP de son pays d'origine, mais un proxy ne couvre que l'application configurée, tandis qu'un VPN chiffre aussi tout le trafic de son appareil.