Nume: _____ **Data:** _____ **Punctaj:** _____

Cum să alegi un VPN
Fișă de lucru

Evaluarea furnizorilor de VPN, a standardelor de securitate, a auditurilor și a politicilor de înregistrare

PREZENTARE GENERALĂ DE ÎNVĂȚARE DESPRE VPN

CURSANT

STATUT DE STUDENT

Parcursul apărătorului de rețea

SIGUR

STAREA CONEXIUNII

Protejarea pachetelor de date

ACTIV

PROTECȚIE LA SCURGERI

Protecție împotriva scurgerilor DNS și IPv6

Bun venit! Acest pachet de activități te ghidează prin principiile fundamentale ale rețelelor private virtuale (VPN). Vei explora modul în care tunelurile criptate îți securizează datele, modul în care funcționează protocoalele de rețea și modul în care poți identifica și reduce scurgerile de confidențialitate.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește conceptele și protocoalele VPN.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com despre VPN

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

Harta ta de învățare despre VPN

- Evaluează jurisdicția furnizorului și politicile zero-logs din perspectiva confidențialității.
- Compară protocoale de tunelare precum WireGuard și OpenVPN din punct de vedere al vitezei.
- Analizează funcții de securitate precum kill switch-urile și nodurile de server doar cu RAM.
- Identifică auditurile independente de securitate și planurile de preț atunci când alegi.
- Selectează locațiile serverelor în funcție de viteza ta și de nevoile de deblocare geografică.

INSTRUCȚIUNI PENTRU FIȘA DE SELECȚIE

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre alegerea unei infrastructuri VPN sigure. Încheie cu activitatea bonus Gândește repede.

ALEGEREA UNUI VPN (INTRODUCERE)

Alegerea VPN-ului potrivit presupune să privești dincolo de agitația publicitară. Un furnizor de încredere trebuie să aibă o politică zero-logs dovedită, protocoale de criptare sigure și clienți open source. Evaluând funcțiile de securitate, jurisdicțiile și performanța vitezei, poți alege un VPN care se potrivește nevoilor tale de protecție digitală.

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT.

Punct de control 1: Provocare cu alegere multiplă

1. Care este factorul-cheie atunci când alegi un furnizor VPN sigur?

- A. Numărul de țări cu servere
- B. O politică fără jurnale (no-logs) auditată independent
- C. Cel mai mic nivel de preț lunar
- D. Sponsorizări publicitare spectaculoase

2. Ce protocol VPN oferă cel mai bun echilibru între viteză și auditabilitate?

- A. PPTP (vechi)
- B. L2TP/IPSec
- C. OpenVPN numai prin TCP
- D. WireGuard

3. De ce ar trebui utilizatorii să evite VPN-urile gratuite pentru activități sensibile?

- A. Sunt interzise în Statele Unite
- B. Îți vând adesea istoricul de navigare web
- C. Nu acceptă navigarea web de bază
- D. Necesită hardware special pentru conectare

4. Ce determină jurisdicția legală de origine a unui furnizor?

- A. Viteza conexiunii la server
- B. Tipurile de dispozitive acceptate
- C. Legile locale privind păstrarea datelor și mandatele de percheziție
- D. Tema vizuală a aplicației client

5. Care este scopul principal al funcției „kill switch” a unui client VPN?

- A. Pentru a bloca accesul la internet dacă conexiunea VPN cade
- B. Pentru a șterge toate aplicațiile instalate pe dispozitiv
- C. Pentru a dubla viteza conexiunii la server
- D. Pentru a reporni sistemul de operare atunci când este inactiv

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Un VPN îți protejează dispozitivul împotriva descărcărilor de malware și a fișierelor cu viruși.

Adevărat Fals

7 Întrebare 7

7. Auditurile independente realizate de firme precum Deloitte verifică afirmațiile privind lipsa jurnalelor.

Adevărat Fals

8 Întrebare 8

8. Legile țării de origine a unui furnizor nu afectează confidențialitatea datelor utilizatorilor.

Adevărat Fals

9 Întrebare 9

9. Baza de cod compactă a WireGuard este mai ușor de auditat decât cea a OpenVPN.

Adevărat Fals

10 Întrebare 10

10. VPN-urile gratuite vând adesea reclame sau urmăresc utilizatorii pentru a acoperi costurile serverelor.

Adevărat Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. O politică verificată independent, de tip _____ , obligă un furnizor de VPN să nu îți înregistreze istoricul online.

2. Protocolul modern _____ oferă viteză mare și folosește un cod foarte mic.

3. O funcție de siguranță numită _____ oprește tot traficul dacă VPN-ul cade brusc.

4. Pentru a stabili dacă un furnizor este supus tratatelor de supraveghere, evaluezi un element legal al său: _____ .

5. Utilizarea serverelor în regim _____ ajută la împiedicarea păstrării datelor utilizatorilor după o repornire.

6. Verificarea unei politici de tip zero-knowledge necesită un _____ de securitate efectuat de firme de renume.

BANCĂ DE CUVINTE DIN VOCABULAR

AUDIT DOAR RAM FIVE EYES JURISDICȚIE KILL SWITCH NO-LOGS VPN GRATUIT WIREGUARD

Scrie răspunsurile aici:

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

Punct de control 4: Asocierea conceptelor despre rețele

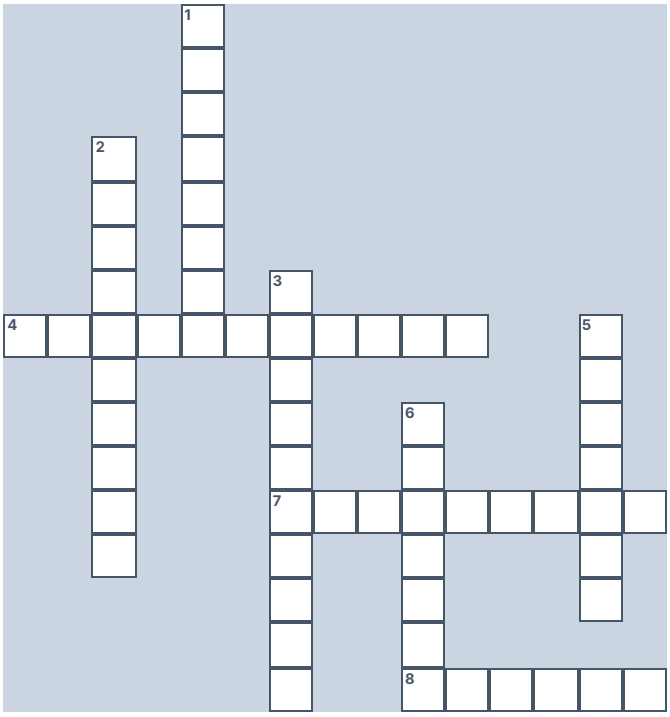
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. WireGuard	A	Serviciu de conectare cu risc ridicat, care își monetizează adesea activitatea prin înregistrarea și vânzarea datelor de navigare.
☐	2. Jurnale auditate	B	Mecanism de siguranță care blochează rutarea internetului dacă tunelul securizat se deconectează.
☐	3. Jurisdicție	C	Alianță internațională de partajare a informațiilor între SUA, Regatul Unit, Canada, Australia și Noua Zeelandă.
☐	4. Kill Switch	D	Infrastructură hardware care rulează pe memorie volatilă, astfel încât datele nu sunt stocate pe disc.
☐	5. Five Eyes	E	Regiunea geografică ce reglementează obligațiile legale ale furnizorului de VPN.
☐	6. VPN gratuit	F	Protocol modern și rapid care folosește aproximativ 4.000 de linii de cod ușor de auditat.
☐	7. Servere doar cu RAM	G	Protocol matur, auditat pe scară largă, open source, cu un cod sursă mult mai mare decât WireGuard.
☐	8. OpenVPN	H	Afirmație privind confidențialitatea, verificată de firme independente de securitate cibernetică.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

4. Regiunea geografică ce guvernează obligațiile legale ale furnizorului de VPN (11)

7. Protocol modern și rapid, care folosește aproximativ 4.000 de linii de cod foarte ușor de auditat (9)

8. Afirmație de confidențialitate verificată de firme independente de securitate cibernetică (6)

VERTICAL

1. Alianță internațională de schimb de informații între SUA, Regatul Unit, Canada, Australia și Noua Zeelandă (8)

2. Serviciu de conectare cu risc ridicat, care se monetizează adesea prin înregistrarea și vânzarea datelor de navigare (10)

3. Mecanism de siguranță care blochează rutarea internetului dacă tunelul securizat se deconectează (10)

5. Infrastructură hardware care rulează în întregime pe memorie volatilă, împiedicând stocarea datelor (7)

6. Protocol open-source matur, auditat pe scară largă, cu un cod mult mai mare decât WireGuard (7)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

4 orizontal: Regiunea geografică ce guvernează obligațiile legale ale furnizorului de VPN (11 litere):

7 orizontal: Protocol modern și rapid, care folosește aproximativ 4.000 de linii de cod foarte ușor de auditat (9 litere):

8 orizontal: Afirmație de confidențialitate verificată de firme independente de securitate cibernetică (6 litere):

VERTICAL

1 vertical: Alianță internațională de schimb de informații între SUA, Regatul Unit, Canada, Australia și Noua Zeelandă (8 litere):

2 vertical: Serviciu de conectare cu risc ridicat, care se monetizează adesea prin înregistrarea și vânzarea datelor de navigare (10 litere):

3 vertical: Mecanism de siguranță care blochează rutarea internetului dacă tunelul securizat se deconectează (10 litere):

5 vertical: Infrastructură hardware care rulează în întregime pe memorie volatilă, împiedicând stocarea datelor (7 litere):

6 vertical: Protocol open-source matur, auditat pe scară largă, cu un cod mult mai mare decât WireGuard (7 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

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

LISTĂ DE CUVINTE DIN VOCABULAR

WIREGUARD NOLOGS JURISDICȚIE KILLSWITCH FIVEEYES VPNGRATUIT
DOARRAM OPENVPN

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR

- **A. WIREGUARD**
- **B. NOLOGS**
- **C. JURISDICȚIE**
- **D. KILLSWITCH**
- **E. FIVEEYES**
- **F. VPNGRATUIT**
- **G. DOARRAM**
- **H. OPENVPN**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Alianță internațională de schimb de informații între SUA, Regatul Unit, Canada, Australia și Noua Zeelandă.
2. Protocol modern și rapid, care folosește aproximativ 4.000 de linii de cod foarte ușor de auditat.
3. Protocol open-source matur, auditat pe scară largă, cu un cod mult mai mare decât WireGuard.
4. Serviciu de conectare cu risc ridicat, care se monetizează adesea prin înregistrarea și vânzarea datelor de navigare.
5. Mecanism de siguranță care blochează rutarea internetului dacă tunelul securizat se deconectează.
6. Infrastructură hardware care rulează în întregime pe memorie volatilă, împiedicând stocarea datelor.
7. Regiunea geografică ce guvernează obligațiile legale ale furnizorului de VPN.
8. Afirmație de confidențialitate verificată de firme independente de securitate cibernetică.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie despre VPN. Scrie răspunsurile în casetele completabile.

1. UGEIWARDR
2. SEUJIDRȚCII
3. EIFEYSEV
4. MORRADA
5. OLSNGO
6. CSLITKIWHL
7. PGVTAUITRN
8. PNNOPVE

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Lucruri pe care le poate ascunde un VPN			
2	Lucruri care contează mai mult decât prețul			
3	Locuri în care poți citi recenzii despre VPN-uri			
4	Lucruri de care un VPN nu te poate proteja			
5	Întrebări pentru echipa de vânzări a unui VPN			
6	Lucruri pe care le poate vedea furnizorul tău de internet			
7	Elemente de pe lista ta de verificare când alegi un VPN			
8	Locuri în care ai folosi un VPN			
9	Semne de avertizare la un furnizor VPN			
10	Cuvinte legate de confidențialitate			
11	Lucruri pe care le-ai testa mai întâi			
12	Promisiuni pe care le face un furnizor VPN bun			
13	Motive pentru care ai folosi un VPN în călătorii			
14	Dispozitive care pot folosi un VPN			
15	Mituri despre VPN-uri			

Punct de control 8: Studii de caz despre VPN

Aplică conceptele pe care le-ai învățat pentru a rezolva scenariile reale de mai jos.

SARAH (STUDENTA DIN CAFENEA)

👩‍💻 „Salut! Sunt la Coffee & Bytes. Există o rețea publică nesecurizată numită «Free_Wi-Fi_No_Password». Vreau să mă conectez la e-mailul școlii și să îmi încarc tema, dar mă tem de hackeri. Care sunt riscurile folosirii acestei rețele fără VPN și cum îmi securizează datele un VPN?”

ALEX (STUDENT CĂLĂTOR)

👩‍💻 „Vai! Călătoresc în străinătate pentru un proiect și încerc să urmăresc un documentar de biologie găzduit pe un server din țara mea. Dar site-ul spune «Acest videoclip nu este disponibil în locația ta actuală.» De ce sunt blocat și cum mă poate ajuta un VPN să îl urmăresc?”

Punct de control 9: Descifrează codul

Pentru a-ți finaliza instruirea privind ghidul de selecție, descifrează acest mesaj ascuns despre alegerea unei infrastructuri securizate.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11
Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22
Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

5 18 16 19 1 21 2 21 1 19 18 1 21 24 7 15 7

24 1 15 7 5 26 26 17 22 11 22 24 7 16

22 11 9 26 21

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre VPN (Partea A)

Parcurge cele mai frecvente întrebări și răspunsuri pe care le au potențialii clienți despre utilizarea rețelelor private virtuale.

Q1: Ce este un VPN și cum funcționează?

O rețea privată virtuală (VPN) îți criptează conexiunea la internet și îți direcționează traficul printr-un server securizat la distanță. Aceasta maschează adresa ta IP publică și limitează ce pot vedea observatorii din rețeaua locală și ISP-ul tău despre traficul direcționat prin tunelul VPN.

Q2: De ce ar trebui să folosesc un VPN?

Un VPN îți protejează confidențialitatea digitală, îți securizează conexiunea în rețelele Wi-Fi publice (precum cafenelele sau aeroporturile), poate reduce limitarea vitezei bazată pe activitate atunci când ISP-ul nu poate identifica tipul de trafic criptat, ocolește restricțiile geografice pentru a accesa conținut global și ajută la securizarea resurselor de lucru la distanță.

Q3: Mă face un VPN complet anonim online?

Nu. Deși un VPN îți ascunde adresa IP și criptează traficul, poți fi totuși urmărit prin cookie-urile browserului, conturile active (precum Google sau Facebook), fingerprintingul browserului sau dacă furnizorul tău VPN îți înregistrează datele.

Q4: Îmi va încetini un VPN viteza internetului?

Da, ușor. Procesul de criptare și distanța fizică față de serverul VPN adaugă latență și suprasarcină. Impactul variază în funcție de furnizor, protocol, distanța până la server, dispozitiv și condițiile de rețea.

Q5: Cum câștigă bani?

Verifică modelul de afaceri. Abonamentele, nivelurile freemium și vânzarea de date influențează cât de mult poți avea încredere într-un VPN, iar un serviciu care nu îți colectează niciodată datele nu le poate vinde. Citește mai întâi politica de confidențialitate. [1]

Punct de control 10: Întrebări frecvente de bază despre VPN (Partea B)

Parcurge cele mai frecvente întrebări și răspunsuri pe care le au potențialii clienți despre utilizarea rețelelor private virtuale.

Q6: Pot folosi un VPN gratuit?

VPN-urile gratuite se pot baza pe publicitate, funcții limitate, analize de utilizare, limite de date sau alte modele de monetizare. Utilizatorii ar trebui să consulte politica de confidențialitate, proprietatea, auditurile și modelul de afaceri ale furnizorului înainte de utilizare.

Q7: Ce este o politică „no-logs” (fără jurnale)?

O politică no-logs descrie ce date despre activitate și conexiune spune un furnizor că nu păstrează. Sfera exactă variază, așa că cititorii ar trebui să analizeze politica și constatările auditurilor independente.

Q8: Cum aleg cel mai bun VPN?

Caută politici no-logs auditate, protocoale puternice (WireGuard, OpenVPN), locații de server sigure, viteze mari, servere doar în RAM, o funcție kill switch și o jurisdicție din afara alianțelor de partajare a informațiilor (precum 5/9/14 Eyes).

Q9: Pot folosi un VPN pe telefon și pe smart TV?

Da. Furnizorii VPN moderni oferă aplicații dedicate pentru iOS, Android, macOS, Windows, Linux și televizoare inteligente, precum și configurări pe router pentru a proteja toate dispozitivele din rețeaua ta de acasă.

Q10: Ce este un Kill Switch?

Kill Switch-ul este o funcție de securitate care deconectează automat dispozitivul tău de la internet dacă conexiunea VPN cade. Astfel se previne scurgerea datelor tale necriptate sau a adresei tale IP reale.

Punct de control 10: Întrebări frecvente avansate despre VPN (Partea C)

Explorează aspecte tehnice și structurale ale rețelelor private virtuale și ale protocoalelor de tunelare securizată.

Q1: Care este diferența dintre WireGuard, OpenVPN și IKEv2?

WireGuard este un protocol modern și ușor (doar aproximativ 4.000 de linii de cod), care oferă viteze mari și timpi de conectare rapizi. OpenVPN este un protocol open-source foarte sigur și verificat în practică. IKEv2 este excelent pentru dispozitivele mobile datorită capacității sale de a se reconecta rapid la schimbarea rețelei.

Q2: Ce este rutarea dublu VPN sau Multi-Hop?

Multi-Hop direcționează traficul tău prin două sau mai multe servere VPN, în secvență. Aceasta adaugă un al doilea strat de criptare și ajută la menținerea ascunsă a adresei tale IP reale față de al doilea hop dacă un server este compromis.

Q3: Ce este scurgerea WebRTC și cum o previne un VPN?

WebRTC este un protocol de browser care îți poate dezvălui adresele IP locală și publică reale chiar și când un VPN este activ. VPN-urile premium blochează sau falsifică cererile WebRTC în aplicațiile lor desktop/mobile și în extensiile de browser.

Q4: Ce sunt serverele care rulează doar în RAM și de ce contează?

Serverele tradiționale scriu datele pe hard disk-uri, care pot fi confiscate sau compromise. Serverele doar RAM (fără disc) rulează integral în memorie volatilă (RAM). Când serverul este repornit sau oprit, datele din memorie se șterg.

Q5: Cum ocolește ofuscarea blocările VPN?

Ofuscarea (sau „Stealth VPN") deghizează pachetele de trafic VPN astfel încât să arate ca trafic web HTTPS obișnuit (portul 443). Aceasta ajută la ocolirea inspecției profunde a pachetelor (DPI) folosite de guverne sau de rețelele școlare/de birou pentru a bloca VPN-urile.

Punct de control 10: Întrebări frecvente avansate despre VPN (Partea D)

Explorează aspecte tehnice și structurale ale rețelelor private virtuale și ale protocoalelor de tunelare securizată.

Q6: Ce este Split Tunneling și când ar trebui să îl folosesc?

Split Tunneling îți permite să alegi ce aplicații sunt direcționate prin tunelul VPN criptat și care se conectează direct la internet. Folosește-l pentru a direcționa prin VPN aplicațiile bancare sensibile, în timp ce jocurile locale se conectează direct, evitând latența adăugată de VPN.

Q7: Cum funcționează confidențialitatea directă (Forward Secrecy / Perfect Forward Secrecy)?

PFS asigură generarea unei chei de criptare unice și temporare pentru fiecare sesiune în parte. Chiar dacă o cheie privată este compromisă în viitor, ea nu poate fi folosită pentru a decripta sesiunile trecute sau viitoare, deoarece acestea au folosit chei independente.

Q8: Ce sunt alianțele 5/9/14 Eyes și de ce ar trebui să-mi pese?

Jurisdicția poate afecta procedura legală cu care se poate confrunta un furnizor, dar riscul practic pentru confidențialitate depinde și de datele pe care le păstrează furnizorul, de arhitectura sa tehnică, de proprietate, de rapoartele de transparență și de istoricul auditurilor.

Q9: Ce este protecția împotriva scurgerilor DNS?

Protecția împotriva scurgerilor DNS obligă dispozitivul tău să trimită interogările de căutare ale site-urilor (interogări DNS) prin serverele DNS private și criptate ale VPN-ului, în loc de serverele furnizorului tău de internet. Astfel, furnizorul tău de internet nu poate urmări ce site-uri vizitezi.

Q10: De ce să verifici cine administrează și susține un VPN?

Reputația contează. Cercetează proprietarii și conducerea companiei, caută audituri publice realizate de terți și verifică ce spun experții independenți în securitate și presa înainte să ai încredere în ea. [1]

Partea 11: 10 fapte interesante despre VPN și perspective din lumea reală

Parcurge aceste fapte și informații valoroase din lumea reală despre istoria, piața și tehnologia VPN-urilor.

1. PRIMUL PROTOCOL VPN

PPTP (Point-to-Point Tunneling Protocol), un protocol VPN timpuriu, creat în anii 1990 de un grup condus de Microsoft, este considerat acum nesigur, așa că VPN-urile moderne folosesc WireGuard sau OpenVPN. [1]

2. EVALUAREA PIEȚEI

Piața globală a VPN-urilor a cunoscut o creștere rapidă, determinată de cerințele tot mai mari ale muncii la distanță și de nevoile de securitate ale întreprinderilor.

3. REVOLUȚIA WIREGUARD

WireGuard are o bază de cod foarte simplificată, concepută pentru eficiență, ceea ce o face mai ușor de auditat pentru vulnerabilități de securitate decât protocoalele tradiționale. [3]

4. STANDARDE STRICTE DE AUDIT

Furnizorii VPN de top angajează firme precum Deloitte, KPMG sau PwC pentru a verifica afirmațiile de non-înregistrare și firme de securitate precum Cure53 pentru a-și testa aplicațiile și serverele. [4]

5. ORIGINILE ALIANȚEI 5-EYES

Parteneriatul de informații Five Eyes dintre SUA, Regatul Unit, Canada, Australia și Noua Zeelandă a apărut din cooperarea Aliaților în domeniul informațiilor de semnale din perioada celui de-al Doilea Război Mondial.

6. INSPECȚIA PROFUNDĂ A PACHETELOR

Firewall-urile avansate folosesc Deep Packet Inspection (DPI) pentru a analiza metadatele pachetelor de rețea și a bloca caracteristicile standard ale conexiunilor VPN.

7. UTILIZARE CORPORATIVĂ

Multe organizații oferă angajaților la distanță un VPN pentru a accesa sisteme interne, precum bazele de date, ceea ce face din VPN-uri un instrument de securitate frecvent la locul de muncă.

8. VPN-URI DESCENTRALIZATE

VPN-urile descentralizate (dVPN) distribuie traficul într-o rețea de noduri administrate de utilizatori, reducând dependența de un singur furnizor centralizat.

9. ANONIMITATEA TOR VS. VPN

Un VPN trece traficul printr-un singur furnizor, în timp ce Tor (The Onion Router) trimite traficul prin trei relee de voluntari (guard, middle, exit) pentru a maximiza confidențialitatea. [5]

10. COSTUL ÎNCĂLCĂRILOR DE DATE

Combinarea unui VPN cu un model de acces zero-trust, care verifică fiecare utilizator și dispozitiv, ajută organizațiile să protejeze datele și să limiteze daunele provocate de brețele de date.

Referințe tehnice și surse

Publicațiile citate, specificațiile criptografice și standardele oficiale ale documentelor utilizate în această fișă de lucru.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

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

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

Barem: Evaluarea furnizorilor de VPN, a standardelor de securitate, a auditurilor și a politicilor de înregistrare a datelor

1 **Politică de jurnale auditată** PROTOCOALE — **Răspuns corect: B**

NOTĂ PENTRU PROFESOR

O politică no-logs auditată independent este cea mai practică modalitate de a verifica afirmațiile unui furnizor privind confidențialitatea zero-knowledge. Marketingul strălucitor sau declarațiile proprii nu sunt suficiente. Citare: Deloitte Advisory, Cure53 Audit.

2 **Superioritatea WireGuard** LATENȚĂ — **Răspuns corect: D**

NOTĂ PENTRU PROFESOR

WireGuard oferă rutare modernă și rapidă a conexiunilor în spațiul nucleului, cu o bază de cod compactă (~4.000 de linii), ceea ce face auditurile foarte eficiente. Citat: IETF Protocol RFC, WireGuard Project.

3 **Întrebarea 3** — **Răspuns corect: B**

NOTĂ PENTRU PROFESOR

VPN-urile gratuite tot plătesc pentru servere, iar FTC avertizează că unele aplicații VPN partajează datele utilizatorilor cu terți, de exemplu pentru a afișa reclame.

4 **Jurisdicții juridice** CONTROALELE RUTĂRII — **Răspuns corect: C**

NOTĂ PENTRU PROFESOR

Jurisdicția stabilește dacă VPN-ul este supus legilor de supraveghere, obligațiilor locale de păstrare a datelor și mandatelor secrete de citare ale guvernului. Citare: Privacy Rights Clearinghouse.

5 **Protecție Kill Switch** CONFIDENȚIALITATE — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Kill switch-ul întrerupe imediat rutarea adaptorului de rețea al sistemului dacă tunelul cade, prevenind expunerea IP-ului real și scurgerile DNS. Citare: IETF Tunnel RFC.

Barem: Punct de control 2 – Adevărat sau fals

6 **Limitările împotriva software-ului rău intenționat** MASCARE IP

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Un VPN oferă o conductă criptată securizată, dar nu scanează conținutul transmis și nici fișierele. Este necesar un software antivirus pentru a bloca malware-ul. Citare: Deloitte Advisory.

7 **Audit independent** VITEZE

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Rapoartele de audit verifică configurațiile software ale serverelor, conformitatea configurației doar cu RAM și lipsa bazelor de date de jurnale. Citare: Deloitte Advisory, Cure53 Audit.

8 **Întrebarea 8**

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Furnizorii trebuie să respecte legile țării lor de origine, care pot include reguli de păstrare a datelor și ordine de a preda datele pe care le dețin.

9 **Dimensiunea bazei de cod a protocolului** FIREWALLURI

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Un cod sursă mai mic reduce suprafața potențială de atac și le este mai ușor echipelor de securitate să verifice integritatea protocolului. Citare: WireGuard Project.

10 **Monetizarea prin reclame** NO-LOGS

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Fără taxe de abonament, VPN-urile gratuite se bazează pe extragerea datelor, profilarea traficului și injectarea de reclame în browser pentru a genera venituri. Citat: EDRi Retention Guidelines.

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

F 1. WireGuard	H 2. Jurnale auditate	E 3. Jurisdicție	B 4. Kill Switch
C 5. Five Eyes	A 6. VPN gratuit	D 7. Servere doar cu RAM	G 8. OpenVPN

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 NO-LOGS	2 WIREGUARD	3 KILL SWITCH	4 JURISDICȚIE
5 DOAR RAM	6 AUDIT		

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – VPNGRATUIT
5 D – KILLSWITCH	6 G – DOARRAM	7 C – JURISDICȚIE	8 B – NOLOGS

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica WireGuard, Jurnale auditate și Jurisdicție cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

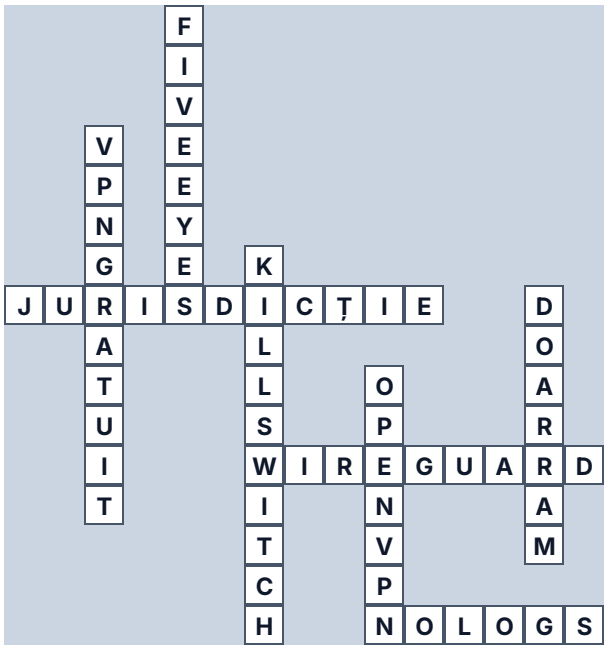
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

4 orizontal: JURISDICȚIE Regiunea geografică ce guvernează obligațiile legale ale furnizorului de VPN (11 litere)

7 orizontal: WIREGUARD Protocol modern și rapid, care folosește aproximativ 4.000 de linii de cod foarte ușor de auditat (9 litere)

8 orizontal: NOLOGS Afirmație de confidențialitate verificată de firme independente de securitate cibernetică (6 litere)

VERTICAL

1 vertical: FIVEEYES Alianță internațională de schimb de informații între SUA, Regatul Unit, Canada, Australia și Noua Zeelandă (8 litere)

2 vertical: VPNGRATUIT Serviciu de conectare cu risc ridicat, care se monetizează adesea prin înregistrarea și vânzarea datelor de navigare (10 litere)

3 vertical: KILLSWITCH Mecanism de siguranță care blochează rutarea internetului dacă tunelul securizat se deconectează (10 litere)

5 vertical: DOARRAM Infrastructură hardware care rulează în întregime pe memorie volatilă, împiedicând stocarea datelor (7 litere)

6 vertical: OPENVPN Protocol open-source matur, auditat pe scară largă, cu un cod mult mai mare decât WireGuard (7 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. UGEIWARDR — **WIREGUARD**
2. SEUJIDRȚCII — **JURISDICȚIE**
3. EIFEYSEV — **FIVEEYES**
4. MORRADA — **DOARRAM**
5. OLSNGO — **NOLOGS**
6. CSLITKIWHL — **KILLSWITCH**
7. PGVTAUITRN — **VPNGRATUIT**
8. PNNOPVE — **OPENVPN**

BAREMUL PROVOCĂRII CU CODUL SECRET

"COMPARĂ RAPOARTELE TALE CU UN SISTEM SIGUR"

Barem pentru studiile de caz

A Scenariul A: securitatea rețelelor publice

SNIFFING ȘI CRIPTARE | Dilema Sarei

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Riscuri: Interceptarea pachetelor, interceptarea datelor și atacurile de tip man-in-the-middle. Cineva aflat în aceeași rețea a cafenelei ar putea captura datele ei de autentificare sau fișierul cu tema.
- Protecție VPN: criptează conținutul pachetelor de rețea, făcând traficul interceptat din tunel ilizibil pentru cei care îl pândesc pasiv în rețeaua locală, atunci când VPN-ul este configurat corect.

B Scenariul B: Accesarea resurselor blocate

GEO-BLOCARE ȘI ADRESE IP | Dilema lui Alex

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- De ce este blocat: gazda de streaming folosește blocarea geografică, care asociază adresa IP locală a călătorului cu țara sa fizică și o blochează pe baza licențierii teritoriale.
- Cum ajută VPN-ul: Mascarea locației sale reale prin direcționarea traficului printr-un server din țara sa de origine. Site-ul vede adresa IP din țara de origine, ceea ce permite accesul.