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

Cum să-ți ascunzi adresa IP
Fișă de lucru

Ascunderea adreselor IP, mascarea locației, proxy, Tor și prevenirea scurgerilor DNS/WebRTC

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

- Explică cum funcționează adresele IP și cum dezvăluie ele locațiile.
- Compară proxy-urile, Tor și VPN-urile pentru mascarea adreselor de rețea.
- Identifică metode de detectare și prevenire a scurgerilor DNS și WebRTC.
- Înțelege cum urmăresc site-urile web utilizatorii prin IP-ul lor public.
- Evaluează rutarea multi-hop și tunelurile criptate pentru protecția IP-ului.

INSTRUCȚIUNI PENTRU FIȘA DE LUCRU DESPRE PROTECȚIA IP

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 ascunderea adresei tale IP și prevenirea scurgerilor. Încheie cu activitatea bonus Gândește repede.

ASCUNDEREA IP-ULUI TĂU (INTRODUCERE)

Adresa ta IP este o adresă poștală digitală care îți expune locația fizică și obiceiurile de rețea. Ascunderea IP-ului tău este prima linie de apărare împotriva urmăririi online, a creării de profiluri țintite și a blocării în funcție de geolocalizare. Înțelegerea modului în care îți poți masca adresa în siguranță ajută la protejarea confidențialității tale online.

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

Punct de control 1: Provocare cu alegere multiplă

1. Ce dezvăluie adresa IP publică a unui dispozitiv site-urilor pe care le vizitezi?

- A. Numărul cardului de credit al utilizatorului
- B. Locația ta aproximativă și numele furnizorului tău de internet
- C. Directorul complet de fișiere locale
- D. Setările de limbă ale tastaturii

2. Ce metodă îți ascunde adresa IP și criptează tot traficul la nivelul întregului sistem?

- A. Un proxy web standard
- B. Ștergerea cookie-urilor din browser
- C. O rețea privată virtuală (VPN)
- D. Dezactivarea firewall-ului nativ

3. Care este o limitare majoră de confidențialitate a folosirii unui proxy web gratuit?

- A. Nu criptează traficul de date din rețelele publice
- B. Necesită instalarea unui sistem de operare extern
- C. Este complet ilegal în Statele Unite
- D. Necesită o conexiune dedicată de linie telefonică

4. Cum oferă rețeaua Tor un anonimat ridicat utilizatorilor?

- A. Accelerând vitezele de conectare
- B. Direcționând traficul prin trei relee gestionate de voluntari
- C. Înregistrându-ți numele într-o bază de date globală
- D. Restricționând accesul doar la agențiile guvernamentale

5. Ce este o scurgere DNS?

- A. O eroare la trimiterea unui e-mail către adresa greșită
- B. Când interogările DNS ocolesc tunelul VPN și ajung la ISP
- C. O defecțiune hardware a sursei de alimentare a routerului local
- D. O actualizare a driverului adaptorului de rețea local

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Un server proxy criptează traficul de fundal al sistemului de operare exact ca un VPN.

Adevărat Fals

7 Întrebare 7

7. Rutarea Tor este foarte sigură, dar reduce viteza de navigare în rețea.

Adevărat Fals

8 Întrebare 8

8. Scurgerile WebRTC pot expune IP-ul tău real în timpul unei sesiuni VPN active.

Adevărat Fals

9 Întrebare 9

9. Cu un VPN activ și fără scurgeri, furnizorul tău de internet nu poate vedea ce site-uri vizitezi.

Adevărat Fals

10 Întrebare 10

10. Ascunderea adresei tale IP blochează urmărirea prin amprentarea browserului.

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. Situația în care interogările tale de domeniu ies din tunelul securizat și sunt expuse se numește _____ .

2. Interfețele API de comunicare din browser, precum _____ , pot dezvălui accidental adresa ta IP nativă.

3. Un _____ redirecționează traficul din browser, dar nu criptează conținutul pachetelor.

4. Criptarea pe mai multe straturi oferită de o _____ asigură un nivel ridicat de anonimat.

5. Un identificator public numit _____ este atribuit de furnizorul tău de telecomunicații și îți dezvăluie zona.

6. Ocolirea blocajelor regionale ale conținutului media se realizează prin _____ a locației.

BANCĂ DE CUVINTE DIN VOCABULAR

ADRESĂ IP | MASCARE | PROXY WEB | REȚEA TOR | SCURGERE DNS | TUNEL VPN | URMĂRIRE ISP | WEBRTC

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre rețele

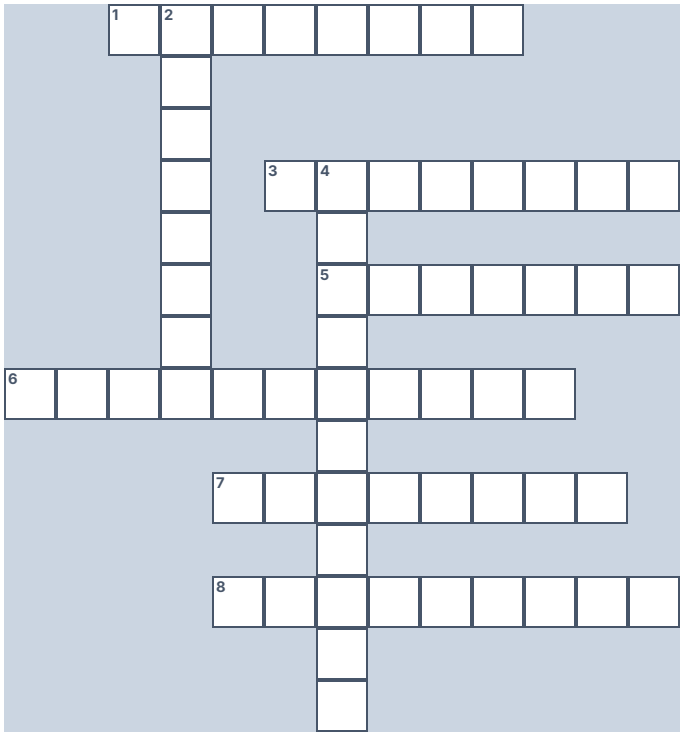
ASOCIEREA DEFINIȚIILOR

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

☐	1. Adresă IP	A	Criptează tot traficul unui dispozitiv și îl direcționează printr-un server VPN.
☐	2. Tunel VPN	B	Direcționează datele prin trei servere de voluntari, criptând straturile la fiecare pas.
☐	3. Rețeaua Tor	C	Direcționarea conexiunii printr-un server dintr-o altă țară pentru a ocoli blocările geografice.
☐	4. Proxy web	D	Etichetă numerică unică ce identifică interfața unui dispozitiv pe internet.
☐	5. Scurgere DNS	E	Redirecționează traficul browserului la nivelul aplicației, fără criptare la nivel de sistem.
☐	6. API-ul WebRTC	F	Înregistrarea de către operatorul tău de telecomunicații a destinațiilor traficului de internet necriptat.
☐	7. Mascarea locației	G	Interogări rezolvate în afara tunelului VPN, care expun domeniile vizitate furnizorului de internet.
☐	8. Urmărirea de către ISP	H	Funcție de browser pentru voce/video care poate ocoli tunelurile și poate expune adresele IP reale.

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

1. Redirecționează traficul browserului la nivelul aplicației, fără criptare la nivel de sistem (8)

3. Criptează tot traficul unui dispozitiv și îl rutează printr-un server VPN (8)

5. Rutarea conexiunii printr-un server din altă țară pentru a ocoli blocările geografice (7)

6. Interogări rezolvate în afara tunelului VPN, care expun domeniile vizitate furnizorului de internet (11)

7. Etichetă numerică unică ce identifică o interfață a unui dispozitiv în internet (8)

8. Funcție a browserului pentru voce/video care poate ocoli tunelurile și poate expune adresele IP reale (9)

VERTICAL

2. Rutează datele prin trei servere de voluntari, criptând straturile la fiecare pas (8)

4. Înregistrarea de către operatorul tău de telecomunicații a destinațiilor traficului necriptat (11)

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

1 orizontal: Redirecționează traficul browserului la nivelul aplicației, fără criptare la nivel de sistem (8 litere):

3 orizontal: Criptează tot traficul unui dispozitiv și îl rutează printr-un server VPN (8 litere):

5 orizontal: Rutarea conexiunii printr-un server din altă țară pentru a ocoli blocările geografice (7 litere):

6 orizontal: Interogări rezolvate în afara tunelului VPN, care expun domeniile vizitate furnizorului de internet (11 litere):

7 orizontal: Etichetă numerică unică ce identifică o interfață a unui dispozitiv în internet (8 litere):

8 orizontal: Funcție a browserului pentru voce/video care poate ocoli tunelurile și poate expune adresele IP reale (9 litere):

VERTICAL

2 vertical: Rutează datele prin trei servere de voluntari, criptând straturile la fiecare pas (8 litere):

4 vertical: Înregistrarea de către operatorul tău de telecomunicații a destinațiilor traficului necriptat (11 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	T	A	Ă	Â	O	X	K	Î
X	J	X	T	J	C	R	U	M	Î	P	C	I	M	M
J	E	Q	P	G	M	M	N	Q	R	R	S	T	T	F
C	R	O	T	A	E	Ț	E	R	Â	O	Ș	Q	O	H
T	A	S	Â	V	S	C	L	Ș	Y	X	U	Â	A	Z
R	C	V	F	J	C	G	V	Z	C	Y	M	C	D	R
B	S	W	P	Â	U	Ț	P	Ă	A	W	Z	N	R	C
E	A	J	A	C	R	O	N	C	E	E	G	I	E	C
W	M	R	Q	L	G	D	I	S	Z	B	Ș	E	S	R
I	U	D	A	A	E	R	O	M	P	T	X	Q	Ă	Î
P	U	R	M	Ă	R	I	R	E	I	S	P	S	I	T
A	S	B	M	Y	E	Ă	F	S	W	W	Î	A	P	R
Z	Y	Y	K	F	D	I	M	R	Î	L	L	T	O	G
Q	Q	G	Z	A	N	O	U	F	Ț	Â	Y	S	Y	Ă
G	L	Z	F	Î	S	N	P	N	W	Â	L	Z	Y	F

LISTĂ DE CUVINTE DIN VOCABULAR

ADRESĂIP TUNELVPN REȚEATOR PROXYWEB SCURGEREDNS APIWEBRTC MASCARE URMĂRIREISP

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. ADRESĂIP**
- **B. TUNELVPN**
- **C. REȚEATOR**
- **D. PROXYWEB**
- **E. SCURGEREDNS**
- **F. APIWEBRTC**
- **G. MASCARE**
- **H. URMĂRIREISP**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

_____ 1. Redirecționează traficul browserului la nivelul aplicației, fără criptare la nivel de sistem.

_____ 2. Rutarea conexiunii printr-un server din altă țară pentru a ocoli blocările geografice.

_____ 3. Funcție a browserului pentru voce/video care poate ocoli tunelurile și poate expune adresele IP reale.

_____ 4. Etichetă numerică unică ce identifică o interfață a unui dispozitiv în internet.

_____ 5. Rutează datele prin trei servere de voluntari, criptând straturile la fiecare pas.

_____ 6. Înregistrarea de către operatorul tău de telecomunicații a destinațiilor traficului necriptat.

_____ 7. Interogări rezolvate în afara tunelului VPN, care expun domeniile vizitate furnizorului de internet.

_____ 8. Criptează tot traficul unui dispozitiv și îl rutează printr-un server VPN.

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. IESAĂDPR
2. ERREOTAȚ
3. SREEUCNSGDR
4. EAACRMS
5. LVUNETPN
6. EBXWPYRO
7. BATCRWPEI
8. IRPIMURRSEĂ

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Motive pentru care ai folosi un VPN în călătorii			
2	Browsere pe care le cunoști			
3	Lucruri pe care le poate ascunde un VPN			
4	Cuvinte legate de confidențialitate			
5	Cuvinte din această fișă de lucru pe care vrei să le ții minte			
6	Lucruri pe care un site web le poate deduce din IP-ul tău			
7	Numere sau simboluri dintr-o adresă IP			
8	Mituri despre VPN-uri			
9	Servicii VPN pe care le cunoști			
10	Lucruri pe care le poate vedea furnizorul tău de internet			
11	Promisiuni pe care le face un furnizor VPN bun			
12	Lucruri care îți pot dezvălui adresa IP reală			
13	Motive pentru care ți-ai ascunde locația			
14	Moduri de a-ți ascunde adresa IP			
15	Dispozitive care pot folosi un VPN			

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 mascarea IP-ului, descifrează acest mesaj secret despre ascunderea urmelor tale digitale.

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

1	22	5	26	17	6	7		1	6	21	7	22	1		24	1		5	26

26	17		22	11	22	24	7	16		6	11	22	5	21	7	24

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: Ascunde un proxy web adresa mea IP?

Da, dar doar pentru traficul trimis prin el, de obicei cel din browser. Majoritatea proxy-urilor web nu îți criptează datele, așa că furnizorul tău de internet sau operatorul rețelei poate vedea în continuare ce trimiți și ce primești.

Q5: Este legal să îmi ascund IP-ul?

În multe țări, da, dar unele restricționează sau interzic VPN-urile și alte instrumente folosite pentru a ascunde o adresă IP. Ascunderea IP-ului tău nu face niciodată legală o faptă ilegală, așa că verifică legile locale înainte de a folosi unul.

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: Îmi ascunde Tor adresa IP?

Da. Tor îți trimite traficul prin trei relee de voluntari (de intrare, intermediar și de ieșire), astfel că site-urile văd adresa releului de ieșire, iar niciun releu nu știe atât cine ești, cât și unde navighezi. [1]

Q7: Ce dezvăluie adresa mea IP?

IP-ul tău public îți dezvăluie, de obicei, furnizorul de internet și o locație aproximativă, precum țara sau orașul. Site-urile îl pot folosi și pentru a-ți corela vizitele și pentru a aplica blocări geografice.

Q8: Cum verific dacă este ascuns?

Conectează-te la VPN, apoi accesează un site de verificare a IP-ului și rulează teste de scurgeri DNS și WebRTC. IP-ul și serverele DNS afișate ar trebui să aparțină VPN-ului, nu ISP-ului tău. Dacă apare adresa ta IP reală, activează protecția împotriva scurgerilor.

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: De ce mă mai pot urmări site-urile după ce îmi ascund adresa IP?

Ascunderea IP-ului nu oprește amprentarea browserului. Trackerele pot combina detalii precum rezoluția ecranului, fonturile instalate și setările browserului într-un identificator, iar cookie-urile sau conturile conectate te pot identifica și ele, așa că folosește și un browser orientat spre confidențialitate. [3]

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: Poate traficul IPv6 să îmi dezvăluie adresa IP reală?

Da, dacă VPN-ul tău tunelează doar IPv4. Atunci dispozitivul tău poate trimite trafic IPv6 în afara tunelului, expunând o adresă atribuită de furnizorul tău de internet. Folosește un VPN care tunelează sau blochează IPv6 și confirmă acest lucru cu un test de scurgeri IPv6.

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: Îmi expune split tunneling adresa IP reală?

Da, pentru aplicațiile pe care le excluzi. Traficul trimis în afara tunelului folosește adresa ta IP reală, iar RFC 8828 notează că WebRTC poate dezvălui adresa furnizorului de internet de sub un VPN cu split tunneling, dacă browserul nu o limitează. [2]

Q7: Ce este o adresă IP partajată și cum ajută confidențialitatea?

Cu un IP partajat, mulți utilizatori VPN apar online în același timp cu aceeași adresă. Asta face mult mai greu pentru un site web să asocieze o singură vizită cu tine, față de un IP dedicat folosit doar de tine.

Q8: Poate furnizorul meu de internet să vadă că folosesc un VPN pentru a-mi ascunde IP-ul?

De obicei, da. ISP-ul tău poate vedea că te conectezi la adresa IP a unui server VPN, când te conectezi și cât de multe date trimiți, dar nu site-urile pe care le vizitezi și nici conținutul din tunelul criptat.

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: Este mai bun un proxy sau un VPN pentru a-mi ascunde IP-ul?

De obicei, un VPN este mai bun. Îți ascunde IP-ul pentru fiecare aplicație de pe dispozitiv și criptează traficul, în timp ce un proxy web acoperă de obicei doar browserul și adesea nu adaugă nicio criptare.

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.

2. AMPRENTARE

Ascunderea IP-ului nu oprește amprentarea browserului, care te poate identifica pe baza unor detalii precum rezoluția ecranului și fonturile instalate. [3]

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.

4. EXPUNEREA ADRESEI PRIN WEBRTC

RFC 8828 avertizează că WebRTC poate descoperi atât adresa publică a unui VPN, cât și adresa furnizorului de internet peste care rulează VPN-ul, cu excepția cazului în care browserul o limitează. [2]

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. REUTILIZAREA CIRCUITELOR TOR

Tor refolosește același circuit aproximativ zece minute, apoi construiește unul nou, ceea ce face mai greu de legat între ele activitățile tale de navigare. [1]

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. [1]

10. PROXY VS. TUNELURI VPN

Un proxy web schimbă adresa IP pe care o vede un site pentru traficul browserului tău, dar, spre deosebire de un VPN, de obicei nu criptează acel trafic și nu acoperă alte aplicații de pe dispozitivul tău. [5]

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] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] 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

Barem: Ascunderea adreselor IP, mascarea locației, proxy, Tor și prevenirea scurgerilor DNS/WebRTC

1 Întrebarea 1

Răspuns corect: B

NOTĂ PENTRU PROFESOR

Ce dezvăluie adresa IP publică a unui dispozitiv site-urilor pe care le vizitezi? → Locația ta aproximativă și numele furnizorului tău de internet

2 Criptarea sistemului VPN LATENȚĂ

Răspuns corect: C

NOTĂ PENTRU PROFESOR

Spre deosebire de proxy-urile care redirecționează doar traficul din browser, un VPN creează un tunel criptat la nivel de sistem, securizând aplicațiile de fundal, jocurile și interogările sistemului de operare. Citare: Tor Project Relays, W3C WebRTC API.

3 Lipsa criptării la proxy SECURITATE WI-FI

Răspuns corect: A

NOTĂ PENTRU PROFESOR

Proxy-urile web doar redirecționează traficul browserului, fără a cripta conținutul pachetelor, ceea ce înseamnă că operatorul rețelei sau furnizorul tău de internet îți poate urmări în continuare traficul de conținut. Citat: IETF Proxy Vulnerabilities.

4 Întrebarea 4

Răspuns corect: B

NOTĂ PENTRU PROFESOR

Cum oferă rețeaua Tor un anonimat ridicat utilizatorilor? → Direcționând traficul prin trei relee gestionate de voluntari

5 Scurgeri DNS prin tunel CONFIDENȚIALITATE

Răspuns corect: B

NOTĂ PENTRU PROFESOR

O scurgere DNS apare atunci când cererile de rezolvare a numelor de domeniu ocolesc tunelul VPN și ajung direct la resolverele ISP-ului tău, expunând înregistrările domeniilor vizitate. Citare: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Barem: Punct de control 2 – Adevărat sau fals

6 Detalii despre limitările proxy-ului

MASCARE IP

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Proxy-urile funcționează la nivelul aplicației și nu au integrarea driverului de rețea la nivel de sistem pe care o are un tunel VPN. Citație: IETF Proxy Vulnerabilities.

7 Întrebarea 7

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Releul traficului prin trei relee ale unor voluntari, cu criptare în straturi, adaugă latență, deci Tor este de obicei mai lent decât o conexiune directă.

8 Întrebarea 8

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

WebRTC poate dezvălui adrese locale și, în unele configurații VPN, IP-ul public atribuit de furnizorul de internet aflat sub tunel (RFC 8828).

9 Întrebarea 9

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Fără scurgeri DNS sau WebRTC, furnizorul de internet vede doar trafic criptat către serverul VPN, nu site-urile pe care le vizitezi.

10 Limitele fingerprintingului

NO-LOGS

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fingerprintingul vizează metrici de configurare a dispozitivului (rezoluția ecranului, fonturi, pluginuri) care rămân vizibile chiar și atunci când IP-ul este ascuns. Citare: EFF Tracking Evasion.

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

D 1. Adresă IP	A 2. Tunel VPN	B 3. Rețeaua Tor	E 4. Proxy web
G 5. Scurgere DNS	H 6. API-ul WebRTC	C 7. Mascarea locației	F 8. Urmărirea de către ISP

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 SCURGERE DNS	2 WEBRTC	3 PROXY WEB	4 REȚEA TOR
5 ADRESĂ IP	6 MASCARE		

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

1 D – PROXYWEB	2 G – MASCARE	3 F – APIWEBRTC	4 A – ADRESĂIP
5 C – REȚEATOR	6 H – URMĂRIREISP	7 E – SCURGEREDNS	8 B – TUNELVPN

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica Adresă IP, Tunel VPN și Rețeaua Tor 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.

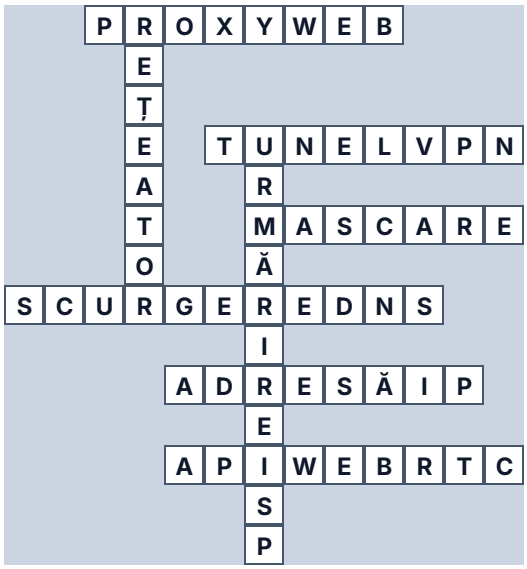
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

1 orizontal: PROXYWEB Redirecționează traficul browserului la nivelul aplicației, fără criptare la nivel de sistem (8 litere)

3 orizontal: TUNELVPN Criptează tot traficul unui dispozitiv și îl rutează printr-un server VPN (8 litere)

5 orizontal: MASCARE Rutarea conexiunii printr-un server din altă țară pentru a ocoli blocările geografice (7 litere)

6 orizontal: SCURGEREDNS Interogări rezolvate în afara tunelului VPN, care expun domeniile vizitate furnizorului de internet (11 litere)

7 orizontal: ADRESĂIP Etichetă numerică unică ce identifică o interfață a unui dispozitiv în internet (8 litere)

8 orizontal: APIWEBRTC Funcție a browserului pentru voce/video care poate ocoli tunelurile și poate expune adresele IP reale (9 litere)

VERTICAL

2 vertical: REȚEATOR Rutează datele prin trei servere de voluntari, criptând straturile la fiecare pas (8 litere)

4 vertical: URMĂRIREISP Înregistrarea de către operatorul tău de telecomunicații a destinațiilor traficului necriptat (11 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. I E S A Ă D P R — **ADRESĂIP**
2. E R R E O T A Ț — **REȚEATOR**
3. S R E E U C N S G D R — **SCURGEREDNS**
4. E A A C R M S — **MASCARE**
5. L V U N E T P N — **TUNELVPN**
6. E B X W P Y R O — **PROXYWEB**
7. B A T C R W P E I — **APIWEBRTC**
8. I R P I M U R R S E Ă — **URMĂRIREISP**

BAREMUL PROVOCĂRII CU CODUL SECRET

"ASCUNDE ADRESA TA CU UN SISTEM DISCRET"

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.