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

Proxy vs. VPN Fișă de lucru

Compararea serverelor proxy cu rețelele private virtuale, diferențele de criptare și rutarea la nivel de aplicație față de cea la nivelul întregului sistem

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

- Compară proxy-urile la nivel de aplicație cu criptarea VPN la nivelul întregului sistem.
- Identifică capabilitățile SOCKS5 în comparație cu proxy-urile HTTP de bază.
- Analizează modul în care proxy-urile bazate pe browser lasă expuse aplicațiile din fundal.
- Înțelege cum înregistrează ISP-urile traficul necriptat din tunelurile proxy.
- Selectează instrumentul de rutare potrivit în funcție de nevoile de viteză și de securitate.

INSTRUCȚIUNI PENTRU FIȘA DE COMPARARE A PROXY-URILOR

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 compararea proxy-urilor și a VPN-urilor. Încheie cu activitatea bonus Gândește repede.

PROXY VS VPN (INTRODUCERE)

Proxy-urile și VPN-urile au funcții diferite în protejarea confidențialității digitale. Un server proxy funcționează ca o redirecționare la nivel de aplicație, mascând adresa ta IP pentru anumite programe, fără a cripta datele. Un VPN funcționează la nivel de rețea, securizând cu criptare tot traficul sistemului. Alegerea instrumentului potrivit depinde de cerințele tale de securitate.

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

Punct de control 1: Provocare cu alegere multiplă

1. La ce strat al modelului OSI funcționează un proxy HTTP standard?

- A. Nivelul fizic
- B. Stratul rețea
- C. Stratul aplicație
- D. Stratul legătură de date

2. Care este un avantaj cheie de protocol al SOCKS5 față de proxy-urile HTTP standard?

- A. Impune criptarea completă a conținutului transmis
- B. Acceptă rutarea oricărui trafic TCP/UDP
- C. Este imun la scurgerile DNS
- D. Funcționează direct în spațiul kernelului

3. De ce este un VPN, în general, mai sigur decât un server proxy?

- A. Rulează pe hardware la distanță mai rapid
- B. Criptează tot traficul de rețea la nivelul întregului sistem
- C. Nu necesită tabele de rutare locale
- D. Elimină complet latența rețelei

4. Ce tip de proxy redirecționează traficul fără nicio criptare implicit?

- A. Un proxy HTTP de bază
- B. Un proxy HTTPS criptat
- C. Un client WireGuard sigur
- D. Un server VPN ofuscat

5. Ce se întâmplă cu traficul aplicațiilor care rulează în fundal atunci când folosești un proxy de browser?

- A. Este criptat automat
- B. Este blocat de serverul proxy
- C. Este direcționat prin tunelul proxy
- D. Ocolește proxy-ul și îți expune IP-ul

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Un proxy SOCKS5 criptează toate conținuturile pachetelor care trec prin server.

- ◯ Adevărat
- ◯ Fals

7 Întrebare 7

7. Un VPN funcționează la nivelul rețelei pentru a securiza tot traficul sistemului.

- ◯ Adevărat
- ◯ Fals

8 Întrebare 8

8. Proxy-urile sunt, în general, mai rapide decât VPN-urile deoarece efectuează o criptare profundă a pachetelor.

- ◯ Adevărat
- ◯ Fals

9 Întrebare 9

9. Configurarea unui proxy necesită stabilirea redirecționărilor de trafic în interiorul unor aplicații specifice.

- ◯ Adevărat
- ◯ Fals

10 Întrebare 10

10. Folosirea unui proxy nu îți securizează traficul de date împotriva urmăririi de către ISP-ul local.

- ◯ 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. Un _____ la nivel de aplicație redirecționează traficul specific browserului fără a securiza alte aplicații.

2. Un _____ robust încapsulează și criptează toate pachetele de date ale dispozitivului.

3. Protocolul _____ se află între stratul de aplicație și cel de transport.

4. Serverele proxy HTTP funcționează la stratul de _____ al modelului OSI.

5. Serverele proxy standard nu au _____ a conținutului, lăsând datele vulnerabile.

6. Un VPN oferă protecție _____ pentru toate adaptoarele de rețea.

BANCĂ DE CUVINTE DIN VOCABULAR

APLICAȚIE CRIPTARE LA NIVEL DE SISTEM PROXY SOCKS5 SUPORT UDP TUNEL VPN VIZIBILITATE

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre rețele

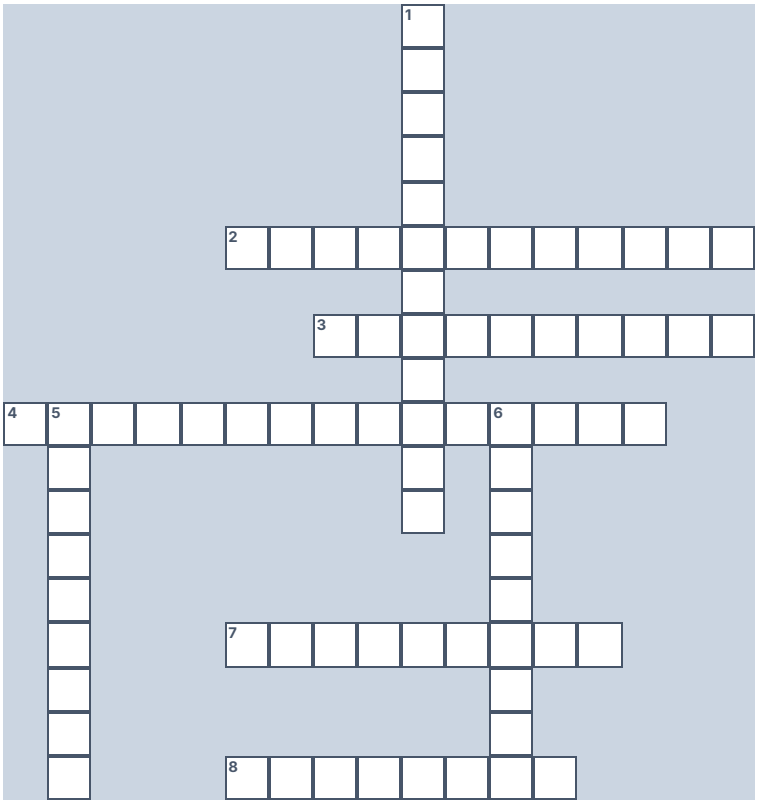
ASOCIEREA DEFINIȚIILOR

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

☐	1. Proxy HTTP	A	Rutare la nivel de sistem de operare care criptează tot traficul aplicațiilor.
☐	2. Proxy SOCKS5	B	Stratul de aplicație, în care funcționează protocoalele standard de proxy web.
☐	3. Tunel VPN	C	Capacitatea SOCKS5 de a retransmite atât UDP, cât și TCP, spre deosebire de proxy-urile HTTP simple.
☐	4. La nivelul întregului sistem	D	Extensie client care ascunde traficul doar în interiorul sandbox-ului browserului.
☐	5. Stratul OSI 7	E	Criptare și încapsulare care învelesc tot traficul de fundal al dispozitivului.
☐	6. Suport UDP	F	Starea traficului în care datele proxy necriptate rămân vizibile pentru ISP-uri.
☐	7. Proxy de browser	G	Proxy la nivelul aplicației care redirecționează traficul anumitor browsere web.
☐	8. Vizibilitatea pentru ISP	H	Protocol proxy între straturile de aplicație și de transport, fără criptare.

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

2. Starea traficului în care datele proxy necriptate rămân vizibile pentru furnizorii de internet (12)

3. Protocol proxy situat între stratul de aplicație și cel de transport, fără criptare (10)

4. Rutare la nivelul sistemului de operare, care criptează tot traficul aplicațiilor (15)

7. Proxy la nivel de aplicație, care redirecționează traficul specific al browserului (9)

8. Criptare și încapsulare care învelesc tot traficul de fundal al dispozitivului (8)

VERTICAL

1. Extensie client care ascunde traficul doar în interiorul sandbox-ului browserului (12)

5. Stratul de aplicație, în care funcționează protocoalele proxy web standard (9)

6. Capacitatea SOCKS5 de a retransmite UDP, nu doar TCP, spre deosebire de proxy-urile HTTP simple (9)

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

2 orizontal: Starea traficului în care datele proxy necriptate rămân vizibile pentru furnizorii de internet (12 litere):

3 orizontal: Protocol proxy situat între stratul de aplicație și cel de transport, fără criptare (10 litere):

4 orizontal: Rutare la nivelul sistemului de operare, care criptează tot traficul aplicațiilor (15 litere):

7 orizontal: Proxy la nivel de aplicație, care redirecționează traficul specific al browserului (9 litere):

8 orizontal: Criptare și încapsulare care învelesc tot traficul de fundal al dispozitivului (8 litere):

VERTICAL

1 vertical: Extensie client care ascunde traficul doar în interiorul sandbox-ului browserului (12 litere):

5 vertical: Stratul de aplicație, în care funcționează protocoalele proxy web standard (9 litere):

6 vertical: Capacitatea SOCKS5 de a retransmite UDP, nu doar TCP, spre deosebire de proxy-urile HTTP simple (9 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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

PROXYHTTP PROXYSOCKS TUNELVPN LANIVELDESISTEM APLICAȚIE
SUPORTUDP PROXYBROWSER VIZIBILITATE

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. PROXYHTTP**
- **B. PROXYSOCKS**
- **C. TUNELVPN**
- **D. LANIVELDESISTEM**
- **E. APLICAȚIE**
- **F. SUPORTUDP**
- **G. PROXYBROWSER**
- **H. VIZIBILITATE**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Stratul de aplicație, în care funcționează protocoalele proxy web standard.
2. Capacitatea SOCKS5 de a retransmite UDP, nu doar TCP, spre deosebire de proxy-urile HTTP simple.
3. Proxy la nivel de aplicație, care redirecționează traficul specific al browserului.
4. Extensie client care ascunde traficul doar în interiorul sandbox-ului browserului.
5. Criptare și încapsulare care învelesc tot traficul de fundal al dispozitivului.
6. Rutare la nivelul sistemului de operare, care criptează tot traficul aplicațiilor.
7. Starea traficului în care datele proxy necriptate rămân vizibile pentru furnizorii de internet.
8. Protocol proxy situat între stratul de aplicație și cel de transport, fără criptare.

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. HYXRPTTPO
2. ETNUPVLN
3. AACPȚEIIL
4. EOYORRBSWPRX
5. CSSRXOYPKO
6. SLTNEDSEMILAEIV
7. TSDPUOURP
8. IZBALEVIITTI

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Deosebiri dintre un proxy și un VPN			
2	Lucruri rămase necriptate fără un VPN			
3	Moduri de a recunoaște o rețea Wi-Fi falsă			
4	Lucruri pe care le face un intermediar în viața de zi cu zi			
5	Situații în care un proxy este suficient			
6	Dispozitive care pot folosi un VPN			
7	Tipuri de proxy pe care le cunoști			
8	Lucruri pe care le poate ascunde un VPN			
9	Mituri despre VPN-uri			
10	Promisiuni pe care le face un furnizor VPN bun			
11	Lucruri de care un VPN nu te poate proteja			
12	Cuvinte din această fișă de lucru pe care vrei să le ții minte			
13	Motive pentru care ai folosi un VPN în călătorii			
14	Situații în care ai vrea un VPN			
15	Locuri în care ai 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, într-o rețea deschisă numită «Free_Wi-Fi_No_Password». Trebuie să mă conectez la e-mailul școlii, iar un prieten spune că un proxy gratuit de browser e suficient ca să fiu în siguranță. Mi-ar proteja un proxy autentificarea și fișierele sau am nevoie de un VPN?”

ALEX (STUDENT CĂLĂTOR)

👩‍💻 „Sunt în străinătate, iar un documentar de biologie găzduit în țara mea spune «Acest videoclip nu este disponibil în locația ta actuală.» Un coleg folosește un proxy, iar eu am un VPN. De ce sunt blocat și care instrument ar funcționa mai bine?”

Punct de control 9: Descifrează codul

Pentru a-ți finaliza instruirea privind compararea proxy-urilor, descifrează acest mesaj secret despre tunelarea securizată.

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

21 7 6 11 21 7 5 25 11 18 17 7 1 31 2

24 21 1 8 11 5 26 15 5 26 1 13 26 24 18 21 26 15

26 17 26 11 19 21 18 29 30

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: Ce este un server proxy?

Un server proxy este un intermediar care transmite cererile între aplicația ta și serverul de destinație. Site-ul vede adresa IP a proxy-ului în loc de a ta, dar este redirecționat doar traficul aplicațiilor configurate să folosească proxy-ul, iar un proxy de bază nu criptează acel trafic.

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: Este un proxy un VPN?

Nu. Un proxy retransmite traficul pentru anumite aplicații, de obicei fără criptare. Un VPN creează un tunel criptat la nivelul rețelei, care transportă tot traficul dispozitivului, inclusiv aplicațiile din fundal.

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 proxy gratuit?

Poți, dar proxy-urile gratuite sunt adesea administrate de operatori necunoscuți. Deoarece un proxy de bază nu criptează traficul, operatorul său poate vedea și chiar modifica paginile necriptate. Verifică cine administrează serviciul înainte de utilizare.

Q7: Păstrează un proxy jurnale?

Se poate. Un proxy gestionează fiecare cerere pe care o redirecționează, așa că operatorul său îți poate înregistra adresa IP, site-urile pe care le vizitezi și momentul accesării. Verifică cine îl administrează și ce spune politica sa de confidențialitate.

Q8: Când este suficient un proxy?

Un proxy poate fi suficient pentru sarcini cu risc scăzut, precum schimbarea locației aparente a unui singur browser. Pentru operațiuni bancare, Wi-Fi public sau protejarea fiecărei aplicații de pe un dispozitiv, un VPN este alegerea mai sigură, deoarece criptează tot traficul.

Q9: Poate un proxy să protejeze toate aplicațiile telefonului meu?

Nu. Doar aplicațiile care respectă setarea proxy o folosesc; celelalte se conectează direct. O aplicație VPN direcționează în schimb toate aplicațiile telefonului prin tunelul său criptat.

Q10: Ce este un proxy SOCKS5?

SOCKS5, definit în RFC 1928, este un protocol proxy aflat între nivelul aplicației și cel de transport. Poate retransmite conexiuni TCP și datagrame UDP și acceptă autentificarea, dar nu are criptare încorporată. [1]

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: La ce niveluri de rețea funcționează proxy-urile și VPN-urile?

Un proxy HTTP funcționează la nivelul aplicației (Layer 7) și înțelege cererile web. SOCKS5 se află între nivelul aplicației și cel de transport. Protocoalele VPN, precum IPsec sau WireGuard, funcționează la nivelul rețelei, deci pot transporta tot traficul IP al dispozitivului.

Q2: Rămâne criptat un site HTTPS printr-un proxy?

Da. Când deschizi un site HTTPS printr-un proxy, criptarea TLS funcționează cap-coadă între browserul tău și site, astfel că proxy-ul vede domeniul, dar nu și conținutul paginii. Paginile HTTP simple rămân lizibile.

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 este un proxy transparent și cine îl folosește?

Un proxy transparent interceptează traficul fără nicio configurare pe dispozitivul utilizatorului. Școlile, companiile și ISP-urile le folosesc pentru caching sau filtrarea conținutului. Utilizatorii adesea nu știu că există unul și nu primesc nicio confidențialitate de la el.

Q5: Cum ocolește ofuscarea blocările VPN?

Ofuscarea (sau „Stealth VPN") deghizează traficul VPN astfel încât să arate ca trafic HTTPS obișnuit (portul 443). Aceasta poate ajuta 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: De ce poate părea un proxy mai rapid decât o conexiune VPN?

Un proxy de bază omite criptarea și gestionează doar traficul unei singure aplicații, deci adaugă mai puțină procesare. Un VPN criptează fiecare pachet de pe dispozitiv. Cu protocoalele moderne, diferența este adesea mică, iar proxy-ul oferă mult mai puțină protecție.

Q8: Pot site-urile să își dea seama că folosesc un proxy sau un VPN?

Adesea, da. Multe site-uri compară adresele IP cu liste de servere proxy și VPN cunoscute, iar proxy-urile HTTP pot adăuga anteturi precum Via sau X-Forwarded-For. Serviciile de streaming blochează frecvent ambele.

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: Poate un proxy opri limitarea vitezei de către furnizorul de internet (ISP)?

Rareori. Un proxy simplu nu criptează traficul, astfel încât furnizorul de internet poate vedea în continuare ce fel de activitate este. Un VPN ascunde tipurile de trafic, dar niciunul dintre instrumente nu rezolvă congestia sau plafoanele de date.

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. STANDARDUL SOCKS

Versiunea 5 a protocolului SOCKS a fost publicată de IETF ca RFC 1928 în martie 1996 și rămâne specificația de referință pentru proxy-urile SOCKS5 folosite astăzi de browsere și aplicații. [1]

2. STRAT SHIM

RFC 1928 descrie SOCKS ca pe un strat intermediar între straturile de aplicație și de transport, astfel încât nu poate retransmite trafic de nivel rețea, cum ar fi ICMP. [1]

3. RELEU UDP

SOCKS5 a adăugat comanda UDP ASSOCIATE, permițând unui proxy să retransmită datagrame UDP, nu doar conexiuni TCP, lucru pe care proxy-urile HTTP simple nu îl gestionează. [1]

4. PORTUL SOCKS IMPLICIT

Clienții SOCKS5 se conectează implicit la serverul proxy pe portul TCP 1080, conform RFC 1928; multe servicii proxy le permit utilizatorilor să aleagă alte porturi. [1]

5. INTERMEDIARI HTTP

Standardul HTTP (RFC 9110) definește un proxy ca pe un agent de redirecționare a mesajelor ales de client, care transmite cererile către serverul de origine.

6. INSPECȚIA PROFUNDĂ A PACHETELOR

Inspecția aprofundată a pachetelor (DPI) examinează conținutul pachetelor și tiparele de trafic; traficul proxy necriptat îi este complet vizibil, în timp ce traficul VPN dezvăluie mult mai puțin.

7. VPN-URI DE NIVEL REȚEA

IPsec, descris în NIST SP 800-77, protejează traficul la nivelul rețelei, astfel încât pachetele IP ale fiecărei aplicații pot fi securizate fără configurare separată pentru fiecare aplicație. [2]

8. DOAR ÎN BROWSER

Un proxy setat într-un browser afectează doar acel browser; clienții de e-mail, jocurile și actualizările de sistem continuă să folosească conexiunea normală a dispozitivului.

9. TOR VS. PROXY-URI

Tor trimite traficul prin trei relee de voluntari (guard, middle și exit) și este de obicei accesat printr-un proxy SOCKS local, adăugând straturi pe care un singur proxy nu le poate oferi.

10. COMPROMISUL DE VITEZĂ

Proxy-urile pot părea mai rapide deoarece omit criptarea, dar protocoalele VPN moderne, precum WireGuard, adaugă o suprasarcină mică, protejând în același timp tot traficul dispozitivului.

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] 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/

Barem: Compararea serverelor proxy și a rețelelor private virtuale, diferențele de criptare și rutarea la nivel de aplicație față de cea la nivelul întregului sistem

1 **Nivelul OSI al proxy-ului** PROTOCOALE — **Răspuns corect: C**

NOTĂ PENTRU PROFESOR

Proxy-urile HTTP/HTTPS standard funcționează la nivelul Aplicație (Layer 7) și redirecționează traficul specific al browserului. Nu au rutare de rețea la nivelul întregului sistem. Citare: Tor Project Foundation.

2 **Întrebarea 2** — **Răspuns corect: B**

NOTĂ PENTRU PROFESOR

SOCKS5 retransmite trafic TCP și UDP între straturile de aplicație și de transport, dar nu criptează implicit, în timp ce proxy-urile HTTP gestionează cereri web.

3 **Criptarea sistemului VPN** SECURITATE WI-FI — **Răspuns corect: B**

NOTĂ PENTRU PROFESOR

Un VPN încapsulează și criptează tot traficul sistemului de operare la nivelul întregului sistem, în timp ce un proxy redirecționează doar traficul anumitor aplicații configurate. Citare: Deloitte Advisory.

4 **Lipsa criptării la proxy** CONTROALELE RUTĂRII — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Proxy-urile HTTP redirecționează traficul browserului la nivelul aplicației, fără a cripta conținutul pachetelor, ceea ce înseamnă că operatorul rețelei tale sau ISP-ul poate în continuare să urmărească traficul tău de conținut. Citare: IETF Proxy Vulnerabilities.

5 **Vulnerabilitate de ocolire** CONFIDENȚIALITATE — **Răspuns corect: D**

NOTĂ PENTRU PROFESOR

Proxy-urile de browser aplică reguli doar browserului web în sine. Aplicațiile din fundal, actualizările sistemului de operare și clienții de e-mail ocolesc proxy-ul, expunându-ți adresa IP nativă. Citare: W3C Consortium.

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

SOCKS5 retransmite traficul între straturile de aplicație și de transport, dar nu efectuează nicio criptare implicit, așa că conținutul pachetelor rămâne lizibil în tranzit.

7 Tuneluri la nivelul rețelei VITEZE

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Funcționând la nivelul rețea, un VPN direcționează și criptează traficul de ieșire de pe dispozitivul tău, ajutând la protejarea traficului la nivelul întregului sistem. Citare: Deloitte Advisory.

8 Limita de criptare a proxy-ului RISCUL DE SNIFFING

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Proxy-urile pot fi uneori mai rapide, dar acest lucru se întâmplă deoarece NU efectuează criptare. Lipsa criptării lasă datele vulnerabile la inspecție. Citație: IETF Proxy Vulnerabilities.

9 Redirecționare la nivel de aplicație FIREWALLURI

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Spre deosebire de VPN-urile la nivel de sistem, serverele proxy necesită configurare manuală în setările browserului sau în câmpurile de proxy specifice aplicațiilor. Citare: W3C Consortium.

10 Riscul urmăririi de către ISP NO-LOGS

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Deoarece proxy-urile HTTP/SOCKS5 standard nu criptează datele din sarcina utilă, ISP-ul tău local păstrează vizibilitate completă asupra acțiunilor tale online. Citare: 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

G 1. Proxy HTTP	H 2. Proxy SOCKS5	E 3. Tunel VPN	A 4. La nivelul întregului sistem
B 5. Stratul OSI 7	C 6. Suport UDP	D 7. Proxy de browser	F 8. Vizibilitatea pentru ISP

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 PROXY	2 TUNEL VPN	3 SOCKS5	4 APLICAȚIE
5 CRIPTARE	6 LA NIVEL DE SISTEM		

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

1 E – APLICAȚIE	2 F – SUPORTUDP	3 A – PROXYHTTP	4 G – PROXYBROWSER
5 C – TUNELVPN	6 D – LANIVELDESISTEM	7 H – VIZIBILITATE	8 B – PROXYSOCKS

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica Proxy HTTP, Proxy SOCKS5 și Tunel VPN 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.

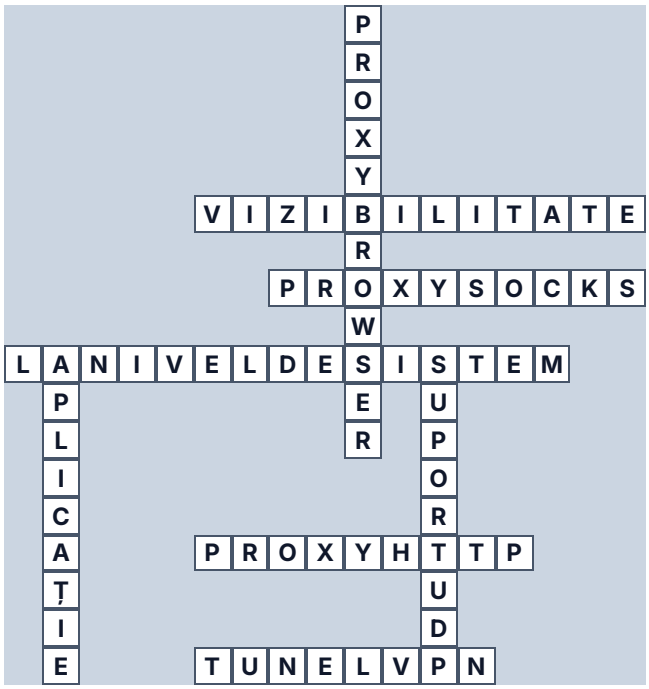
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

2 orizontal: VIZIBILITATE Starea traficului în care datele proxy necriptate rămân vizibile pentru furnizorii de internet (12 litere)

3 orizontal: PROXYSOCKS Protocol proxy situat între stratul de aplicație și cel de transport, fără criptare (10 litere)

4 orizontal: LANIVELDESISTEM Rutare la nivelul sistemului de operare, care criptează tot traficul aplicațiilor (15 litere)

7 orizontal: PROXYHTTP Proxy la nivel de aplicație, care redirecționează traficul specific al browserului (9 litere)

8 orizontal: TUNELVPN Criptare și încapsulare care învelesc tot traficul de fundal al dispozitivului (8 litere)

VERTICAL

1 vertical: PROXYBROWSER Extensie client care ascunde traficul doar în interiorul sandbox-ului browserului (12 litere)

5 vertical: APLICAȚIE Stratul de aplicație, în care funcționează protocoalele proxy web standard (9 litere)

6 vertical: SUPORTUDP Capacitatea SOCKS5 de a retransmite UDP, nu doar TCP, spre deosebire de proxy-urile HTTP simple (9 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. HYXRPTTPO — PROXYHTTP
2. ETNUPVLN — TUNELVPN
3. AACPȚEIIL — APLICAȚIE
4. EOYORRBSWPRX — PROXYBROWSER
5. CSSRXOYPKO — PROXYSOCKS
6. SLTNEDSEMILAEIV — LANIVELDESISTEM
7. TSDPUOURP — SUPORTUDP
8. IZBALEVIITTI — VIZIBILITATE

BAREMUL PROVOCĂRII CU CODUL SECRET

"REDIRECȚIONEAZĂ TRAFICUL CU AJUTORUL UNUI PROXY"

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.
- Proxy vs. VPN: Un proxy de browser simplu nu îi criptează traficul. Un VPN criptează tot ce se află pe dispozitiv, făcând pachetele interceptate ilizibile pentru cei care spionează la nivel local.

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.
- Care funcționează mai bine: ambele îi oferă o adresă IP din țara sa, dar un proxy acoperă doar aplicația configurată, în timp ce un VPN criptează și tot traficul dispozitivului său.