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

Ghidul VPN.com despre VPN
Fișă de lucru

Exerciții practice despre protocoale de rețea, tunelare și controale de securitate.

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 conceptul de tunelare și încapsulare a datelor.
- Identifică configurațiile standard de protocol și cerințele de lățime de bandă.
- Analizează rolurile firewall-urilor și ale geo-blocării în rutarea internetului.
- Înțelege cum urmăresc ISP-urile navigarea necriptată și cum o previne un VPN.
- Face distincția între limitele operaționale ale locației serverului și cele ale jurisdicției.

INSTRUCȚIUNI PENTRU GHIDUL VPN

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 scenariile reale din secțiunea de studii de caz. Încheie cu activitatea bonus Gândește repede.

CE ESTE UN VPN? (INTRODUCERE)

O rețea privată virtuală este mai mult decât un simplu comutator de confidențialitate. Este un tunel criptat care îți direcționează traficul de internet printr-un server la distanță. Acesta îți ascunde adresa IP, împiedică ISP-ul să compileze jurnale ale acțiunilor tale online și îți securizează datele în rețelele publice. Înțelegerea terminologiei este esențială pentru a-ți menține siguranța digitală.

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

Punct de control 1: Provocare cu alegere multiplă

1. Ce este un protocol VPN?

- A. Un dispozitiv hardware folosit pentru conectarea cablurilor.
- B. Un set de reguli care definesc modul în care datele sunt criptate și trimise.
- C. Un plugin de browser care blochează reclamele.
- D. O companie de furnizare de servicii de internet.

2. Dacă conexiunea ta VPN pare lentă, care este cea mai probabilă cauză?

- A. Serverul VPN este prea departe sau suprasolicitat.
- B. Rezoluția monitorului tău este setată prea mare.
- C. Ai dezactivat cookie-urile browserului web.
- D. Aranjamentul tastaturii tale este configurat incorect.

3. De ce este foarte recomandat un VPN atunci când te conectezi la Wi-Fi public?

- A. Face conexiunea Wi-Fi gratuită.
- B. Mărește raza de acoperire a routerului.
- C. Criptează traficul pentru a bloca hackerii aflați în aceeași rețea.
- D. Șterge automat e-mailurile nedorite.

4. Care dintre următoarele descrie o blocare geografică (geoblock)?

- A. Un instrument care măsoară distanța fizică până la un server.
- B. O restricție care blochează accesul la un site în funcție de locație.
- C. Un protocol pentru comprimarea fișierelor locale.
- D. Un mecanism de stocare a copiilor de rezervă.

5. Ce poate vedea furnizorul tău de internet (ISP) când folosești un VPN?

- A. Cuvintele-cheie căutate și conținutul paginilor web pe care le vizualizezi.
- B. Că ești conectat la un VPN, dar nu detaliile traficului.
- C. Nicio informație, nici măcar că ești online.
- D. Fișierele și fotografiile tale de pe hard disk-ul local.

Punct de control 2: Provocare Adevărat sau Fals

6 Mascarea locației

6. Un VPN maschează adresa IP publică a dispozitivului tău, împiedicând site-urile terțe să îți identifice cu ușurință locația fizică.

- ○ Adevărat
- ○ Fals

7 Impactul VPN asupra vitezei

7. Activarea unei conexiuni VPN face ca viteza ta de bază de internet să fie de două ori mai mare decât a conexiunii fără VPN.

- ○ Adevărat
- ○ Fals

8 Interceptarea traficului în Wi-Fi public

8. Dacă folosești o rețea Wi-Fi publică nesecurizată fără VPN, alți utilizatori din aceeași rețea îți pot intercepta potențial traficul necriptat.

- ○ Adevărat
- ○ Fals

9 Firewall-uri și conexiuni blocate

9. Firewall-urile pot fi configurate de administratorii de rețea pentru a detecta și a bloca tunelurile de conexiune VPN de ieșire.

- ○ Adevărat
- ○ Fals

10 Politici stricte de tip no-logs

10. O politică strictă „no-logs” înseamnă că furnizorul VPN este obligat prin lege să îți stocheze interogările de căutare și linkurile vizitate timp de cel puțin 30 de zile.

- ○ 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. Pentru a-ți securiza traficul, VPN-ul împachetează pachetele de date într-un alt protocol, proces numit _____ .

2. Dacă ai viteze mici de descărcare la streaming, poate fi vorba de o _____ limitată a rețelei.

3. Un serviciu de streaming disponibil doar într-o anumită țară folosește o _____ pentru a restricționa utilizatorii din alte state.

4. Regulile de conectare care definesc parametrii de criptare și conectare se numesc, în cazul unui VPN, _____ .

5. Computerul tău folosește un _____ local pentru a monitoriza traficul de rețea și a bloca conexiunile nesigure.

6. Când te conectezi la un VPN, datele sunt rutate printr-un _____ la distanță pentru a-ți ascunde IP-ul public.

BANCĂ DE CUVINTE DIN VOCABULAR

FIREWALL FURNIZOR ISP GEOBLOCARE INTIMITATE LĂȚIME DE BANDĂ PROTOCOL SERVER TUNELARE

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre rețele

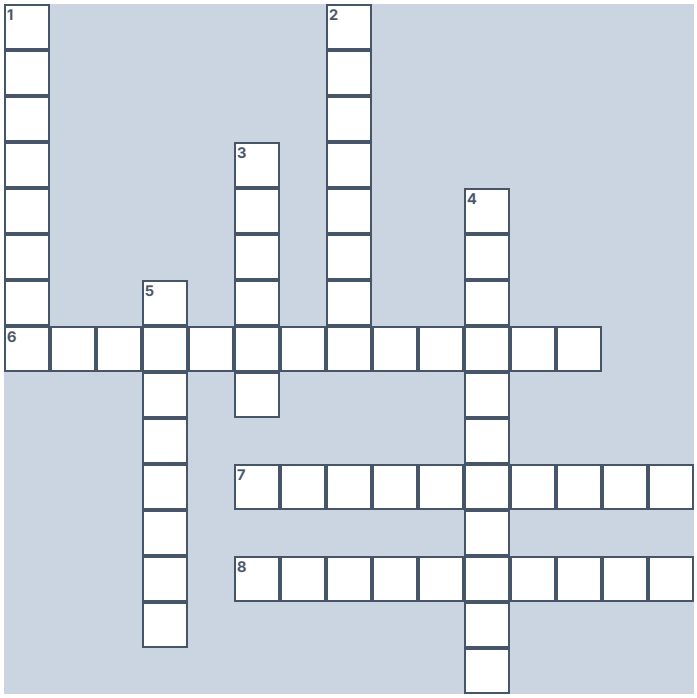
ASOCIEREA DEFINIȚIILOR

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

☐	1. Tunelare	A	Un set de reguli care determină modul în care datele sunt transmise prin rețea.
☐	2. Protocol	B	Rata maximă de transfer al datelor printr-o conexiune.
☐	3. Lățime de bandă	C	O restricție care împiedică accesul pe web în funcție de locația fizică.
☐	4. Server	D	Un sistem de securitate care monitorizează și blochează traficul neautorizat.
☐	5. Geoblocare	E	Un computer la distanță care îți direcționează traficul și îți maschează IP-ul.
☐	6. Firewall	F	Starea de a fi liber de urmărire sau de supraveghere publică.
☐	7. Confidențialitate	G	Furnizorul de servicii de internet care transportă traficul tău și poate vedea activitatea necriptată.
☐	8. ISP	H	Încapsularea pachetelor de date în alt pachet pentru un tranzit securizat.

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

6. Rata maximă de transfer de date printr-o conexiune (13)

7. Restricție care împiedică accesul la web în funcție de locația fizică (10)

8. Starea de a fi ferit de urmărire sau de supraveghere publică (10)

VERTICAL

1. Set de reguli care determină modul în care datele sunt transmise prin rețea (8)

2. Împachetarea pachetelor de date în interiorul altui pachet pentru un tranzit securizat (8)

3. Un computer aflat la distanță, care îți rutează traficul și îți maschează IP-ul (6)

4. Furnizorul de servicii de internet, care îți înregistrează traficul dacă nu este criptat (11)

5. Sistem de securitate care monitorizează și blochează traficul neautorizat (8)

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

6 orizontal: Rata maximă de transfer de date printr-o conexiune (13 litere):

7 orizontal: Restricție care împiedică accesul la web în funcție de locația fizică (10 litere):

8 orizontal: Starea de a fi ferit de urmărire sau de supraveghere publică (10 litere):

VERTICAL

1 vertical: Set de reguli care determină modul în care datele sunt transmise prin rețea (8 litere):

2 vertical: Împachetarea pachetelor de date în interiorul altui pachet pentru un tranzit securizat (8 litere):

3 vertical: Un computer aflat la distanță, care îți rutează traficul și îți maschează IP-ul (6 litere):

4 vertical: Furnizorul de servicii de internet, care îți înregistrează traficul dacă nu este criptat (11 litere):

5 vertical: Sistem de securitate care monitorizează și blochează traficul neautorizat (8 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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

TUNELARE PROTOCOL LĂȚIMEDEBANDĂ SERVER GEOBLOCARE FIREWALL
INTIMITATE FURNIZORISP

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. TUNELARE

B. PROTOCOL

C. LĂȚIMEDEBANDĂ

D. SERVER

E. GEOBLOCARE

F. FIREWALL

G. INTIMITATE

H. FURNIZORISP

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Starea de a fi ferit de urmărire sau de supraveghere publică.

2. Restricție care împiedică accesul la web în funcție de locația fizică.

3. Set de reguli care determină modul în care datele sunt transmise prin rețea.

4. Sistem de securitate care monitorizează și blochează traficul neautorizat.

5. Rata maximă de transfer de date printr-o conexiune.

6. Un computer aflat la distanță, care îți rutează traficul și îți maschează IP-ul.

7. Furnizorul de servicii de internet, care îți înregistrează traficul dacă nu este criptat.

8. Împachetarea pachetelor de date în interiorul altui pachet pentru un tranzit securizat.

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. RELTAUEN
2. DMĂEȚLNDĂBAEI
3. GORCELEBAO
4. ITMEIATINT
5. OCRLTPOO
6. EVSRRE
7. FLWALIER
8. IOPZRFIUSRN

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Lucruri pe care le asociezi cu cuvântul „tunel”			
2	Lucruri pe care le-ai învăța familia despre VPN-uri			
3	Lucruri de pe un site web care te pot urmări			
4	Mituri despre VPN-uri			
5	Cuvinte din această fișă de lucru pe care vrei să le ții minte			
6	Dispozitive care pot folosi un VPN			
7	Lucruri de care un VPN nu te poate proteja			
8	Țări pe care ai vrea să le „vizitezi” online			
9	Promisiuni pe care le face un furnizor VPN bun			
10	Moduri de a recunoaște o rețea Wi-Fi falsă			
11	Întrebări pe care le ai despre VPN-uri			
12	Servicii VPN pe care le cunoști			
13	Cuvinte legate de confidențialitate			
14	Lucruri pe care le poate ascunde un VPN			
15	Motive pentru care ai folosi un VPN într-o cafenea			

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

Un VPN îți criptează traficul pentru a-l securiza. Folosește cheia literă–număr de mai jos pentru a descifra mesajul de securitate cibernetică, scriind literele corespunzătoare în spațiile libere.

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

19 21 18 24 7 13 7 1 31 2

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

24 26 17 7 15 22 7 5 26 21 11 31 1 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: 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 legală folosirea unui VPN?

Folosirea VPN-urilor este legală în multe țări, dar unele jurisdicții restricționează, reglementează sau blochează serviciile VPN. Utilizatorii ar trebui să verifice legile locale în vigoare înainte de utilizare. Pentru mai multe detalii, consultă ghidurile despre legalitate de pe VPN.com.

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. [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: 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 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: 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: Poate un VPN ocoli limitarea vitezei internetului de către furnizor (ISP)?

Uneori. Un VPN poate ajuta atunci când un ISP încetinește selectiv anumite activități identificabile, dar nu va depăși congestia, plafoanele de date, limitele de viteză la nivel de cont sau calitatea slabă a rețelei.

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) a fost dezvoltat de un grup de furnizori care includea Microsoft și a fost publicat ca RFC 2637 în iulie 1999 pentru a susține VPN-urile de acces la distanță. [6]

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 auditori externi (precum Cure53 sau PwC) pentru a efectua revizuiri independente ale codului și a verifica faptul că nu înregistrează activitatea utilizatorilor.

5. ORIGINILE ALIANȚEI 5-EYES

Alianța Five Eyes a apărut din acordul de informații de semnale UKUSA din 1946 dintre SUA și Regatul Unit, la care s-au alăturat ulterior Canada, Australia și Noua Zeelandă.

6. INSPECȚIA PROFUNDĂ A PACHETELOR

Inspecția aprofundată a pachetelor (DPI) examinează conținutul pachetelor și tiparele de trafic, nu doar antetele, iar unele firewall-uri o folosesc pentru a detecta și a bloca protocoalele VPN obișnuite.

7. UTILIZARE CORPORATIVĂ

Un procent mare dintre angajații companiilor din lume folosesc VPN-uri securizate pentru a se autentifica în bazele de date interne, ceea ce îl face un standard de securitate important.

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 și exit), astfel încât niciun releu să nu cunoască ambele capete.

10. COSTUL ÎNCĂLCĂRILOR DE DATE

Adoptarea unui model de acces securizat zero-trust împreună cu un VPN îi ajută pe cei din organizații să protejeze proprietatea intelectuală și să reducă impactul financiar al încălcărilor de securitate a datelor.

Referințe tehnice și surse

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

LITERATURĂ ACADEMICĂ ȘI STANDARDE DE SECURITATE

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.

https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.

https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

REZUMATUL STANDARDELOR TEHNICE

- Standarde de încapsulare: RFC 4301 definește rutarea securizată a pachetelor de internet IPsec/L2TP.
- Urmărirea de către ISP: Direcționarea interogărilor DNS prin tunelul VPN criptat poate reduce vizibilitatea DNS pentru ISP-ul local.
- Protocoale de control al firewall-ului: pachetele stealth ofuscate ocolesc filtrele de pachete aprofundate.

Barem: Punct de control 1 – Alegere multiplă

1 Întrebarea 1

Răspuns corect: B

NOTĂ PENTRU PROFESOR

Un protocol VPN definește regulile pentru construirea tunelului și criptarea datelor; celelalte opțiuni descriu cabluri, blocante de reclame și furnizori de internet.

2 Întrebarea 2

Răspuns corect: A

NOTĂ PENTRU PROFESOR

Distanța adaugă latență, iar un server supraîncărcat are mai puțină capacitate de împărțit; rezoluția ecranului, cookie-urile și aranjarea tastaturii nu afectează viteza conexiunii.

3 Întrebarea 3

Răspuns corect: C

NOTĂ PENTRU PROFESOR

În rețelele deschise, alții pot intercepta pachetele necriptate; un VPN criptează traficul, astfel încât datele interceptate să nu poată fi citite.

4 Întrebarea 4

Răspuns corect: B

NOTĂ PENTRU PROFESOR

Blocarea geografică potrivește adresa IP publică a unui vizitator cu o bază de date de locații și refuză accesul în afara teritoriilor permise.

5 Întrebarea 5

Răspuns corect: B

NOTĂ PENTRU PROFESOR

Furnizorul de internet poate vedea că trimiți date criptate către un server VPN, dar nu ce site-uri vizitezi și nici ce cauți.

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Site-urile văd adresa IP a serverului VPN în loc de a ta, ceea ce le ascunde locația ta aproximativă.

7 Întrebarea 7

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Criptarea și hop-ul suplimentar către serverul VPN reduc de obicei ușor viteza; un VPN nu poate dubla viteza de bază a conexiunii tale.

8 Întrebarea 8

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Pe un Wi-Fi nesecurizat, instrumentele de packet sniffing pot captura trafic necriptat, precum datele de autentificare trimise fără HTTPS.

9 Întrebarea 9

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Administratorii pot bloca porturile VPN cunoscute, precum 1194 al OpenVPN, sau pot folosi inspecția profundă a pachetelor (DPI) pentru a detecta traficul VPN.

10 Întrebarea 10

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

O politică fără jurnale (no-logs) este promisiunea unui furnizor de a nu păstra înregistrări ale activității tale; nicio lege nu cere VPN-urilor să stocheze căutările timp de 30 de zile.

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

H 1. Tunelare	A 2. Protocol	B 3. Lățime de bandă	E 4. Server
C 5. Geoblocare	D 6. Firewall	F 7. Confidențialitate	G 8. ISP

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 TUNELARE	2 LĂȚIME DE BANDĂ	3 GEOBLOCARE	4 PROTOCOL
5 FIREWALL	6 SERVER		

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

1 G – INTIMITATE	2 E – GEOBLOCARE	3 B – PROTOCOL	4 F – FIREWALL
5 C – LĂȚIMEDEBANDĂ	6 D – SERVER	7 H – FURNIZORISP	8 A – TUNELARE

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica Tunelare, Protocol și Lățime de bandă 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.

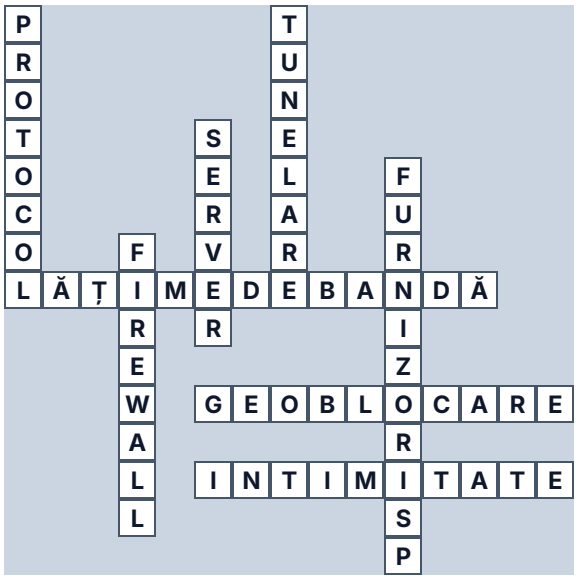
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



ORIZONTAL

6 orizontal: LĂȚIMEDEBANDĂ Rata maximă de transfer de date printr-o conexiune (13 litere)

7 orizontal: GEOBLOCARE Restricție care împiedică accesul la web în funcție de locația fizică (10 litere)

8 orizontal: INTIMITATE Starea de a fi ferit de urmărire sau de supraveghere publică (10 litere)

VERTICAL

1 vertical: PROTOCOL Set de reguli care determină modul în care datele sunt transmise prin rețea (8 litere)

2 vertical: TUNELARE Împachetarea pachetelor de date în interiorul altui pachet pentru un tranzit securizat (8 litere)

3 vertical: SERVER Un computer aflat la distanță, care îți rutează traficul și îți maschează IP-ul (6 litere)

4 vertical: FURNIZORISP Furnizorul de servicii de internet, care îți înregistrează traficul dacă nu este criptat (11 litere)

5 vertical: FIREWALL Sistem de securitate care monitorizează și blochează traficul neautorizat (8 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. RELTAUEN — **TUNELARE**
2. DMĂEȚLNDĂBAEI — **LĂȚIMEDEBANDĂ**
3. GORCELEBAO — **GEOBLOCARE**
4. ITMEIATINT — **INTIMITATE**
5. OCRLTPOO — **PROTOCOL**
6. EVSRRE — **SERVER**
7. FLWALIER — **FIREWALL**
8. IOPZRFIUSRN — **FURNIZORISP**

BAREMUL PROVOCĂRII CU CODUL SECRET

"PROTEJEAZĂ INTIMITATEA CU UN TUNEL SECURIZAT"

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.