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

Ghidul celui mai sigur VPN

Analiză tehnică a designului VPN de înaltă securitate, a serverelor cu memorie volatilă doar în RAM, a securității accesului Zero Trust, a apărărilor împotriva scurgerilor DNS prin DNS criptat privat și a configurațiilor WireGuard auditate.

PREZENTARE GENERALĂ A ÎNVĂȚĂRII: GHIDUL CELUI MAI SIGUR 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 standardele tehnice ale VPN-urilor foarte sigure. Vei explora hardware-ul de server doar cu RAM, securitatea accesului Zero Trust, resolverele DNS private criptate și configurațiile WireGuard auditate.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește configurațiile VPN și de securitate a rețelei.**
- [ ] **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 cu cele mai bune VPN-uri

URL: https://www.vpn.com/ro/vpn/cel-mai-sigur-vpn/

Harta ta de învățare despre cel mai sigur VPN

- Analizează arhitectura tehnică și standardele de criptare ale Most Secure VPN Guide.
- Configurează setările clientului pentru a preveni scurgerile de trafic IP, DNS și WebRTC.
- Compară protocoalele proprietare de tunelare cu implementările standard.

INSTRUCȚIUNI PENTRU GHIDUL CELUI MAI SIGUR 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 hardware-ul de servere doar cu RAM și sistemele Zero Trust. Încheie cu activitatea bonus Gândește repede.

INFRASTRUCTURI DOAR RAM ȘI REȚELE ZERO TRUST (INTRODUCERE)

Un VPN cu adevărat securizat se bazează pe un cadru zero trust, pe servere doar cu RAM, pentru a preveni ca confiscarea discurilor să expună jurnalele, pe resolvere DNS criptate private și pe protocoale auditate precum WireGuard. Aceste controale combinate apără activele digitale de mare valoare împotriva amenințărilor de interceptare.

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

Punct de control 1: Provocare cu alegere multiplă

1. Ce arhitectură este fundamentală pentru asigurarea celei mai înalte securități în serverele VPN moderne?

- A) Infrastructură de servere doar cu RAM
- B) Stocare pe disc
- C) Rutare DNS dinamică
- D) Activarea redirecționării porturilor

2. Ce protocol este recomandat pe scară largă pentru cele mai sigure și moderne configurații VPN?

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3. Ce cadru de securitate impune verificarea continuă a fiecărei conexiuni, fără excepție?

- A) Arhitectură Zero Trust
- B) Firewall-uri perimetrale
- C) Rutare dinamică
- D) Chei secrete partajate

4. Care este rolul principal al protecției împotriva scurgerilor DNS a unui client VPN?

- A) Direcționează toate cererile DNS prin resolvere criptate private
- B) Obfuscarea pachetelor IP
- C) Stocarea locală în cache a interogărilor DNS
- D) Dezactivarea serverelor de nume

5. Cum crește rutarea Multi-Hop securitatea generală a unui tunel VPN?

- A) Direcționează datele prin două servere separate, în serie
- B) Crește viteza de compresie
- C) Criptează datele cu cifruri de securitate slabă
- D) Ocolește firewall-urile

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Serverele doar RAM stochează fișierele de jurnal în memorie efemeră, care este ștearsă la repornire.

○ Adevărat ○ Fals

7 Întrebare 7

7. WireGuard folosește algoritmi criptografici moderni, mai puțin vulnerabili la blocajele de viteză.

○ Adevărat ○ Fals

8 Întrebare 8

8. Un kill switch VPN funcționează blocând tot traficul de rețea dacă tunelul cade.

○ Adevărat ○ Fals

9 Întrebare 9

9. Auditurile independente ale unor terți sunt irelevante pentru verificarea angajamentelor de securitate.

○ Adevărat ○ Fals

10 Întrebare 10

10. Modelele Zero Trust presupun că toate conexiunile din rețeaua internă sunt sigure în mod implicit.

○ 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. **Administratorii impun securitatea prin implementarea unui cadru strict** _____ .

2. **Rutarea pachetelor prin mai multe puncte de intrare necesită o configurație sigură** _____ .

3. **Pentru a preveni scurgerile de date de pe unități furate, folosim un design de tip** _____ .

4. **Deturnarea de către furnizorul de internet este atenuată prin configurarea funcțiilor native de** _____ .

5. **Pentru a bloca traficul în timpul întreruperilor conexiunii, activează mecanismul** _____ .

6. **Pentru a reduce la minimum jurnalele stocate în baze de date, alege un furnizor cu un** _____ **complet.**

BANCĂ DE CUVINTE DIN VOCABULAR

CRIPTARE KILL SWITCH MULTI-HOP PROTECȚIE DNS PROTOCOL
SERVER DOAR-RAM SISTEM AUDITAT ZERO TRUST

Scrie răspunsurile aici:

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

Punct de control 4: Asocierea conceptelor despre VPN și rețele

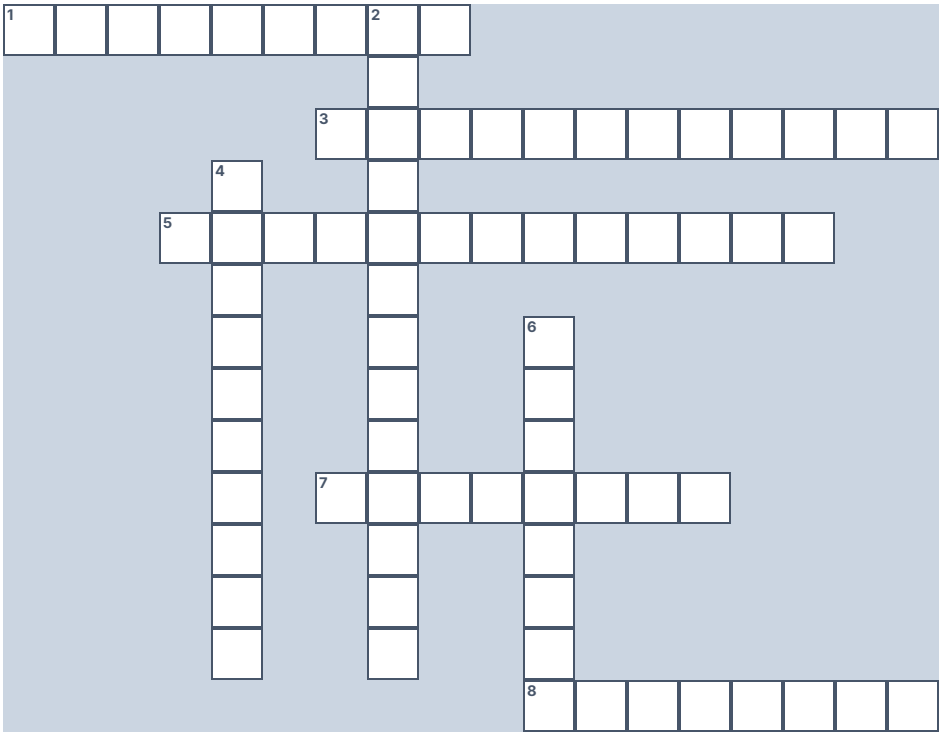
ASOCIEREA DEFINIȚIILOR

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

☐	1. Zero Trust	A	Configurație inspectată independent, care confirmă că nu se stochează niciun jurnal.
☐	2. Multi-Hop	B	Amestecarea criptografică a datelor utile pentru a le securiza în tranzit.
☐	3. Server doar RAM	C	Cadru de securitate care impune autentificarea continuă a tuturor utilizatorilor.
☐	4. Protecție DNS	D	Set de reguli tehnice care determină cum sunt împachetate și trimise datele.
☐	5. Kill Switch	E	Rutare VPN în cascadă care înlănțuie două noduri de server.
☐	6. Sistem auditat	F	Arhitectură de server care folosește memorie volatilă pentru a stoca încărcătura de date.
☐	7. Criptare	G	Impunerea interogărilor DNS private pentru a proteja căutările pe serverele de nume.
☐	8. Protocol	H	Mecanism de siguranță care blochează traficul dacă VPN-ul cedează.

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. Cadru de securitate care cere autentificarea continuă a tuturor utilizatorilor (9)

3. Impunerea interogărilor DNS private pentru a proteja căutările la serverele de nume (12)

5. Configurație inspectată independent, care confirmă că nu se stochează loguri (13)

7. Amestecarea criptografică a datelor pentru a securiza tranzitul (8)

8. Set de reguli tehnice care stabilesc cum sunt împachetate și trimise datele (8)

VERTICAL

2. Arhitectură de server care folosește memorie volatilă pentru a stoca datele (13)

4. Mecanism de siguranță care blochează traficul dacă VPN-ul cade (10)

6. Rutare VPN în cascadă care înlănțuie două noduri de server (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

1 orizontal: Cadru de securitate care cere autentificarea continuă a tuturor utilizatorilor (9 litere):

3 orizontal: Impunerea interogărilor DNS private pentru a proteja căutările la serverele de nume (12 litere):

5 orizontal: Configurație inspectată independent, care confirmă că nu se stochează loguri (13 litere):

7 orizontal: Amestecarea criptografică a datelor pentru a securiza tranzitul (8 litere):

8 orizontal: Set de reguli tehnice care stabilesc cum sunt împachetate și trimise datele (8 litere):

VERTICAL

2 vertical: Arhitectură de server care folosește memorie volatilă pentru a stoca datele (13 litere):

4 vertical: Mecanism de siguranță care blochează traficul dacă VPN-ul cade (10 litere):

6 vertical: Rutare VPN în cascadă care înlănțuie două noduri de server (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.

T J Ș S V R Z D H D S Â A K Q

A Â H C T I W S L L I K Z C M

T L J U P R O T O C O L R U S

I Ț A S W Î L L G H M I L H R

D F K T K S W H Ă Ț P T E Y O

U Y W S G T X A P T I Ț N N Z

A O H Q T H P U A H Ț O Ț T J

M A D P M K Ă R O N U F F P R

E W Y Î J U E P Î Y V X P Î I

T Z I T S U R T O R E Z Î M A

S S E R V E R D O A R R A M D

I H Ă Ș A Î E V D J Z J D J Q

S M P R O T E C Ț I E D N S Î

A E O J N B M Â C G I Ă Ă O R

L P V T H Y E Y S G X W H E R

LISTĂ DE CUVINTE DIN VOCABULAR

ZEROTRUST MULTIHOP SERVERDOARRAM PROTECȚIEDNS KILLSWITCH

SISTEMAUDITAT CRIPTARE PROTOCOL

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. ZEROTRUST**
- **B. MULTIHOP**
- **C. SERVERDOARRAM**
- **D. PROTECȚIEDNS**
- **E. KILLSWITCH**
- **F. SISTEMAUDITAT**
- **G. CRIPTARE**
- **H. PROTOCOL**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Mecanism de siguranță care blochează traficul dacă VPN-ul cade.
2. Impunerea interogărilor DNS private pentru a proteja căutările la serverele de nume.
3. Rutare VPN în cascadă care înlănțuie două noduri de server.
4. Set de reguli tehnice care stabilesc cum sunt împachetate și trimise datele.
5. Amestecarea criptografică a datelor pentru a securiza tranzitul.
6. Arhitectură de server care folosește memorie volatilă pentru a stoca datele.
7. Configurație inspectată independent, care confirmă că nu se stochează loguri.
8. Cadru de securitate care cere autentificarea continuă a tuturor utilizatorilor.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie despre rețelele private virtuale (VPN). Scrie răspunsurile în casetele de introducere furnizate.

1. RTOEZUSTR
2. AEERRSRDMAROV
3. KWCIISHLTL
4. PREATCRI
5. IHUPTMOL
6. SEEDCNIPRȚOT
7. ITUMSIDETASAT
8. TROLPOCO

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Lacăte sau chei pe care le folosești în fiecare zi			
2	Lucruri pe care le poate ascunde un VPN			
3	Lucruri care fac un VPN sigur			
4	Mituri despre VPN-uri			
5	Motive pentru care ai folosi un VPN în călătorii			
6	Locuri sigure din lumea reală			
7	Cuvinte care înseamnă „protejat”			
8	Promisiuni pe care le face un furnizor VPN bun			
9	Cuvinte legate de confidențialitate			
10	Tipuri de audit sau inspecție			
11	Cuvinte din această fișă de lucru pe care vrei să le ții minte			
12	Lucruri pe care un hacker vrea să le fure			
13	Moduri de a recunoaște o rețea Wi-Fi falsă			
14	Locuri în care ai folosi un VPN			
15	Lucruri pe care le poate vedea furnizorul tău de internet			

Punct de control 8: Studii de caz despre VPN și rețele

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

STUDIU DE CAZ 1: ÎNTĂRIREA INFRASTRUCTURII ENTERPRISE



Scenariu: O bancă comercială își reproiectează topologia de acces la distanță. Are nevoie de o arhitectură zero trust care să lege toate dispozitivele client de serverele securizate.

Întrebare de discuție: Care este principalul beneficiu al micro-segmentării rețelei într-un model VPN Zero Trust?

STUDIU DE CAZ 2: PROTECȚIILE SERVERELOR DOAR RAM



Scenariu: Un furnizor de VPN axat pe securitate își modernizează serverele pentru a preveni ca confiscarea fizică a unui server să expună istoricul jurnalelor utilizatorilor.

Întrebare de discuție: Explică modul în care configurațiile hardware exclusiv RAM (RAM-Only) previn extragerea criminalistică a datelor în cazul confiscării fizice a serverelor.

Punct de control 9: Descifrează codul

Un inginer de rețea securizează canalele de rutare și tunelurile clientului. Folosește cheia literă–număr de mai jos pentru a descifra mesajul, 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

27 19 17 26 21 11 15 7 22 11 9 26 21 7

19 21 18 24 7 13 7 1 31 2 1 5 24 11 27 7

27 1 15 18 21 18 1 22 7

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 despre rețelele private virtuale (VPN) și tunelare.

Q1: Ce face un VPN „cel mai sigur"?

O combinație de Zero Trust, servere doar cu RAM și protocoale auditate.

Q2: Ce sunt serverele doar în RAM?

Servere care rulează în memorie volatilă, concepute să nu stocheze jurnale pe disc.

Q3: Ce este un VPN Zero Trust?

Un cadru care verifică continuu fiecare cerere de acces și fiecare conexiune.

Q4: De ce este considerat WireGuard sigur?

Are un cod sursă mic, ușor de auditat, și folosește algoritmi de criptare moderni.

Q5: Cum previn VPN-urile sigure scurgerile DNS?

Prin direcționarea tuturor interogărilor prin resolvere DNS private și criptate.

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

Parcurge cele mai frecvente întrebări și răspunsuri despre rețelele private virtuale (VPN) și tunelare.

Q6: Necesită un VPN sigur audituri?

Da, auditurile independente verifică afirmațiile privind lipsa jurnalelor și securitatea codului.

Q7: Care este rolul unui kill switch?

Oprește imediat traficul de rețea dacă conexiunea VPN se întrerupe.

Q8: Ce criptare este folosită în VPN-urile sigure?

AES-256 și ChaCha20 sunt standardele industriei pentru criptare.

Q9: Este sigură rutarea Multi-Hop?

Da, înlănțuie două sau mai multe servere pentru a preveni analiza traficului.

Q10: Cum ajută jurisdicția offshore?

Poate limita legile aplicabile, dar nu oferă imunitate absolută.

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

Explorează aspecte tehnice avansate ale protocoalelor de tunelare VPN, ale integrărilor clienților mobili și ale implementării în întreprinderi.

Q1: Cum previn serverele doar în RAM riscurile de confiscare a datelor?

Deoarece rulează în RAM, scoaterea din priză șterge datele păstrate în memorie.

Q2: Cum înlocuiește Zero Trust securitatea perimetrală standard?

Tratează fiecare client ca ostil, necesitând autentificare continuă.

Q3: Ce face codul WireGuard mai ușor de auditat?

Codul său pentru Linux are sub 4.000 de linii, mult mai puțin decât stivele VPN obișnuite. [4]

Q4: Cum protejează DNSSEC interogările DNS?

Semnează înregistrările DNS astfel încât resolverele să poată detecta răspunsurile falsificate sau modificate.

Q5: Cum îngreunează Multi-Hop corelarea traficului?

Prin separarea IP-urilor de intrare și de ieșire între diferiți furnizori de găzduire.

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

Explorează aspecte tehnice avansate ale protocoalelor de tunelare VPN, ale integrărilor clienților mobili și ale implementării în întreprinderi.

Q6: De ce sunt riscante jurisdicțiile Five Eyes pentru VPN-uri?

Statele membre partajează informații și pot folosi ordine legale pentru a solicita date ale utilizatorilor.

Q7: Cum este implementat un kill switch la nivelul nucleului?

Folosește reguli de firewall ale sistemului (precum iptables sau WFP) pentru a bloca traficul de ieșire.

Q8: Ce este confidențialitatea directă în handshake-urile VPN?

Generează chei de sesiune unice, astfel încât sesiunile anterioare să nu poată fi decriptate.

Q9: Cum atenuează VPN-urile sigure scurgerile WebRTC?

Prin blocarea cererilor WebRTC sau prin direcționarea lor prin tunel.

Q10: Cum asigură auditurile independente conformitatea cu cerințele de confidențialitate?

Auditorii efectuează teste de penetrare și inspectează configurațiile serverelor.

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

Parcurge fapte din lumea reală despre vitezele de criptare VPN, auditurile protocoalelor, conectivitatea mobilă și munca la distanță în întreprinderi.

1. INFORMAȚII DESPRE VPN

Serverele doar RAM își încarcă sistemul de operare în memorie la pornire, astfel încât nimic nu rămâne pe disc după o repornire.

2. INFORMAȚII DESPRE VPN

WireGuard folosește framework-ul Noise cu Curve25519, ChaCha20, Poly1305, BLAKE2s și HKDF. [3]

3. INFORMAȚII DESPRE VPN

Zero Trust acordă accesul pe resursă și nu oferă nicio încredere implicită bazată pe locația în rețea (NIST SP 800-207). [1]

4. INFORMAȚII DESPRE VPN

Alianța de informații Five Eyes include SUA, Regatul Unit, Canada, Australia și Noua Zeelandă.

5. INFORMAȚII DESPRE VPN

Scurgerile WebRTC apar atunci când browserele dezvăluie adresa IP publică reală a clientului prin interogări STUN.

6. INFORMAȚII DESPRE VPN

Perfect forward secrecy (PFS) asigură că: compromiterea unei chei pe termen lung nu expune cheile sesiunilor anterioare. [3]

7. PERSPECTIVĂ ASUPRA VPN-URILOR

Cure53, o firmă de securitate din Berlin, a publicat audituri ale mai multor furnizori de VPN.

8. PERSPECTIVĂ ASUPRA VPN-URILOR

Scurgerile DNS apar atunci când interogările DNS ocolesc tunelul VPN și ajung la serverele de nume ale furnizorului local de internet.

9. PERSPECTIVĂ ASUPRA VPN-URILOR

Cipurile RAM volatile necesită alimentare electrică constantă pentru a păstra datele și își pierd conținutul la oprire.

10. INFORMAȚII DESPRE VPN

Sistemele Zero Trust pentru întreprinderi impun verificări ale posturii dispozitivului înainte de a permite conectarea la resurse securizate. [1]

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile interactive sunt alcătuite pe baza standardelor tehnice, a specificațiilor și a cadrelor de reglementare globale.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

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

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

[4] 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/

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

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

Barem: Punct de control 1 – Alegere multiplă

1 **Server doar RAM** DOAR RAM — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Serverele doar RAM nu stochează jurnale pe disc și șterg datele la repornire. Citare: Most Secure VPN.

2 **Întrebarea 2** — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

WireGuard combină un cod sursă mic și auditabil cu cifruri moderne.

3 **Modelul Zero Trust** ZERO TRUST — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Modelele Zero Trust verifică în mod continuu conformitatea dispozitivului înainte de acordarea accesului. Citare: Most Secure VPN.

4 **Protecție DNS** PROTECȚIE DNS — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Protecția împotriva scurgerilor DNS direcționează interogările de căutare prin resolvere private. Citare: Most Secure VPN.

5 **Tuneluri Multi-Hop** MULTI-HOP — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Rutarea Multi-Hop înlănțuie două noduri de server separate, în serie. Citare: Most Secure VPN.

Barem: Punct de control 2 – Adevărat sau fals

6 **Server doar RAM** DOAR RAM — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Hardware-ul serverelor doar RAM nu scrie date pe disc și se șterge la repornire. Citare: Most Secure VPN.

7 **Viteza WireGuard** WIREGUARD — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

WireGuard folosește criptografie modernă care evită blocajele de procesare. Citat: Most Secure VPN.

8 **Kill Switch** COMUTATOR DE SIGURANȚĂ (FAILSAFE) — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Un kill switch blochează tot traficul dacă conexiunea VPN cade. Citare: Most Secure VPN.

9 **Audituri ale unor terți** AUDITURILE SUNT ESENȚIALE — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Auditurile unor terți sunt esențiale pentru a verifica afirmațiile despre confidențialitate ale companiilor. Citare: Most Secure VPN.

10 **Întrebarea 10** — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Zero Trust nu acordă nicio încredere implicită pe baza locației din rețea. [1]

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

C 1. Zero Trust	E 2. Multi-Hop	F 3. Server doar RAM	G 4. Protecție DNS
H 5. Kill Switch	A 6. Sistem auditat	B 7. Criptare	D 8. Protocol

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 ZERO TRUST	2 MULTI-HOP	3 SERVER DOAR-RAM	4 PROTECȚIE DNS
5 KILL SWITCH	6 SISTEM AUDITAT		

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

1 E – KILLSWITCH	2 D – PROTECȚIEDNS	3 B – MULTIHOP	4 H – PROTOCOL
5 G – CRIPTARE	6 C – SERVERDOARRAM	7 F – SISTEMAUDITAT	8 A – ZEROTRUST

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica Zero Trust, Multi-Hop și Server doar RAM 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.

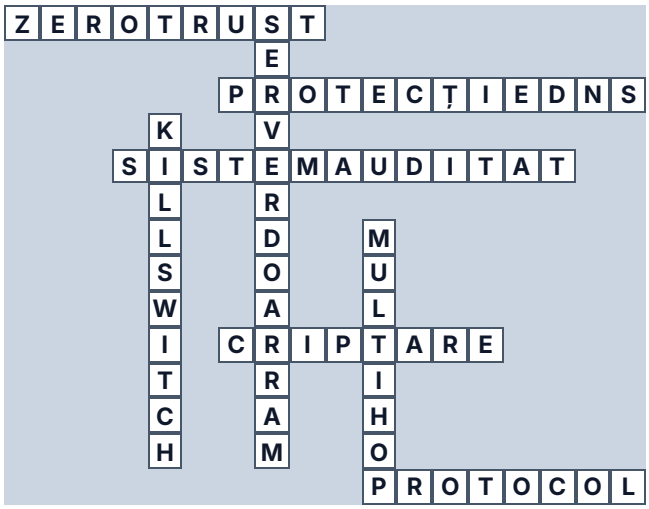
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

1 orizontal: ZEROTRUST Cadru de securitate care cere autentificarea continuă a tuturor utilizatorilor (9 litere)

3 orizontal: PROTECȚIEDNS Impunerea interogărilor DNS private pentru a proteja căutările la serverele de nume (12 litere)

5 orizontal: SISTEMAUDITAT Configurație inspectată independent, care confirmă că nu se stochează loguri (13 litere)

7 orizontal: CRIPTARE Amestecarea criptografică a datelor pentru a securiza tranzitul (8 litere)

8 orizontal: PROTOCOL Set de reguli tehnice care stabilesc cum sunt împachetate și trimise datele (8 litere)

VERTICAL

2 vertical: SERVERDOARRAM Arhitectură de server care folosește memorie volatilă pentru a stoca datele (13 litere)

4 vertical: KILLSWITCH Mecanism de siguranță care blochează traficul dacă VPN-ul cade (10 litere)

6 vertical: MULTIHOP Rutare VPN în cascadă care înlănțuie două noduri de server (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. RTOEZUSTR — ZEROTRUST
2. AEERRSRDMAROV — SERVERDOARRAM
3. KWCIISHLTL — KILLSWITCH
4. PREATCRI — CRIPTARE
5. IHUPTMOL — MULTIHOP
6. SEEDCNIPRȚOT — PROTECȚIEDNS
7. ITUMSIDETASAT — SISTEMAUDITAT
8. TROLPOCO — PROTOCOL

BAREMUL PROVOCĂRII CU CODUL SECRET

"VPN URILE SIGURE PROTEJEAZĂ ACTIVE VALOROASE"

Barem pentru studiile de caz

A STUDIU DE CAZ 1: ÎNTĂRIREA INFRASTRUCTURII ENTERPRISE

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O bancă corporativă își reproiectează topologia de acces la distanță. Cere o arhitectură zero trust care să lege toate dispozitivele client de servere securizate.
- Strategie și soluție recomandată: Indicații de notare: Explică faptul că micro-segmentarea limitează accesul la resurse specifice, împiedicând mișcarea laterală a amenințărilor dacă un dispozitiv este compromis.

B STUDIU DE CAZ 2: PROTECȚIILE SERVERELOR DOAR RAM

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un furnizor de VPN axat pe securitate își modernizează serverele pentru a preveni ca o confiscare fizică a serverelor să expună istoricul jurnalelor utilizatorilor.
- Strategie și soluție recomandată: Indicații de notare: Explică faptul că serverele RAM-Only nu au stocare pe disc fizic. Pierderea alimentării șterge automat toate datele efemere din memoria volatilă.