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

# Securitatea Surfshark

Examinarea funcțiilor de securitate Surfshark, inclusiv blocarea reclamelor CleanWeb, rutarea dinamică MultiHop, arhitectura SDN Nexus, flota de servere doar cu RAM și modul Camouflage.

## PREZENTARE GENERALĂ DE ÎNVĂȚARE: SECURITATEA SURFSHARK

**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 arhitectura de securitate Surfshark. Vei explora hardware-ul de server exclusiv în RAM, rotirea dinamică a IP-urilor prin Nexus SDN, blocatoarele de reclame CleanWeb și rutarea MultiHop.

### 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/surfshark/securitate/

# Harta ta de învățare despre securitatea Surfshark

- Analizează arhitectura tehnică și regulile de configurare ale Surfshark Security.
- Configurează setările clientului pentru a preveni scurgerile de trafic IP, DNS și WebRTC.
- Compară prețurile personalizate, perioada de încercare și funcțiile de performanță cu modelele standard.

## INSTRUCȚIUNI PENTRU GHIDUL DE SECURITATE SURFSHARK

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 infrastructura doar cu RAM, Nexus SDN și CleanWeb. Încheie cu activitatea bonus Gândește repede.

## FLOTĂ DE SERVERE DOAR RAM, NEXUS SDN ȘI ARHITECTURA CLEANWEB (INTRODUCERE)

Surfshark protejează confidențialitatea utilizatorilor printr-o flotă de servere exclusiv în RAM, rețele definite prin software Nexus cu IP Rotator, blocarea reclamelor CleanWeb și trasee de criptare Dynamic MultiHop.

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

## Punct de control 1: Provocare cu alegere multiplă

1. 1. Cum se numește blocatorul integrat de reclame și malware al Surfshark?
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. 2. Ce arhitectură hardware folosește Surfshark pe toate serverele?
   - A) Hard disk-uri
   - B) 100% doar cu RAM
   - C) Stocare optică
   - D) Bandă magnetică

3. 3. Ce funcție direcționează traficul prin două servere VPN distincte?
   - A) Ocolitor
   - B) MultiHop (VPN dublu)
   - C) Rețeaua Nexus
   - D) IP static

4. 4. Ce funcție de ofuscare deghizează traficul VPN în date web obișnuite?
   - A) Kill Switch
   - B) Modul Camouflage
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. 5. Care este funcția instrumentului Surfshark Bypasser?
   - A) Speed Booster
   - B) Split tunneling
   - C) Manager de parole
   - D) Rezolvator DNS

## Punct de control 2: Provocare Adevărat sau Fals

### 6 Întrebare 6

6. Serverele doar RAM șterg toate datele operaționale imediat la repornirea serverului.

○ Adevărat ○ Fals

### 7 Întrebare 7

7. Modul Camouflage împiedică ISP-urile să detecteze că folosești un VPN.

○ Adevărat ○ Fals

### 8 Întrebare 8

8. CleanWeb 2.0 funcționează în cadrul extensiilor de browser pentru a bloca ferestrele pop-up pentru consimțământul privind cookie-urile.

○ Adevărat ○ Fals

### 9 Întrebare 9

9. Surfshark păstrează marcaje temporale ale conexiunilor și jurnale ale utilizării lățimii de bandă.

○ Adevărat ○ Fals

### 10 Întrebare 10

10. Rețeaua Nexus schimbă periodic adresele IP ale utilizatorilor, fără deconectare.

○ 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. Reclamele web deranjante, scripturile de urmărire și linkurile de phishing sunt blocate de filtrele _____ .

2. Activitatea utilizatorului nu lasă urme criminalistice deoarece serverele funcționează în regim _____ .

3. Rutarea datelor prin două salturi criptate separate se realizează prin tuneluri _____ .

4. Pentru a ascunde utilizarea VPN de furnizorii de servicii de internet, utilizatorii activează modul _____ .

5. Permiterea aplicațiilor bancare să ocolească tunelul VPN este gestionată prin setările _____ .

6. Arhitectura SDN de nouă generație care conectează flota de servere este sistemul _____ .

**BANCĂ DE CUVINTE DIN VOCABULAR**

BYPASSER | CAMOUFLAGE | CLEANWEB | DOAR RAM | IP ROTATIV | KILL SWITCH | MULTI-HOP | NEXUS

**Scrie răspunsurile aici:**

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

# Punct de control 4: Asocierea conceptelor despre VPN și rețele

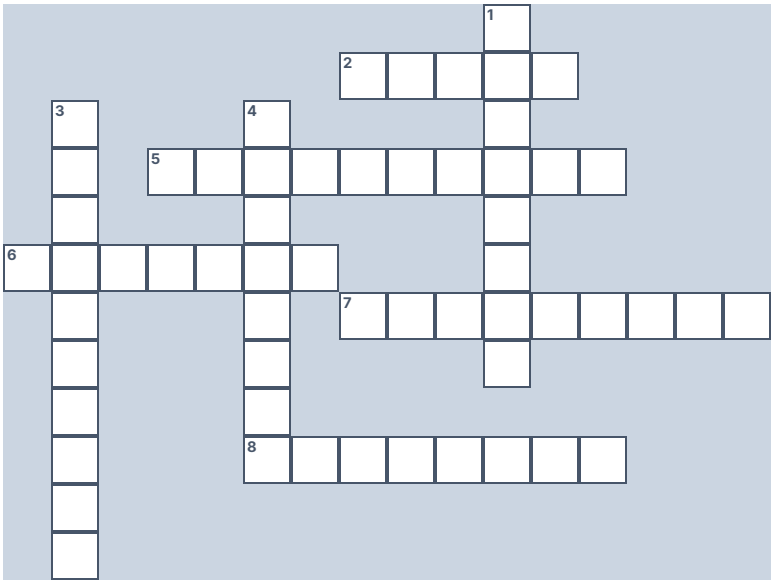
## ASOCIEREA DEFINIȚIILOR

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

| | | | |
|---|---|---|---|
| ☐ | 1. CLEANWEB | A | O funcție automată de siguranță care blochează traficul de rețea atunci când VPN-ul cade. |
| ☐ | 2. DOAR RAM | B | Funcție de split-tunneling care permite anumitor aplicații să ocolească VPN-ul. |
| ☐ | 3. MULTI-HOP | C | Un filtru avansat care blochează reclamele, malware-ul și bannerele de consimțământ pentru cookie-uri. |
| ☐ | 4. CAMOUFLAGE | D | Hardware de server cu memorie volatilă care șterge toate datele la fiecare ciclu de alimentare. |
| ☐ | 5. BYPASSER | E | O funcție care schimbă periodic adresa IP externă fără a întrerupe tunelurile. |
| ☐ | 6. KILL SWITCH | F | Tehnologie de ofuscare care ascunde semnăturile VPN pentru a imita traficul HTTPS obișnuit. |
| ☐ | 7. NEXUS | G | O funcție de rutare double-VPN care criptează traficul prin două noduri de server distincte. |
| ☐ | 8. ROTATIV | H | O rețea proprietară definită prin software, care conectează toate serverele într-o rețea mesh unificată. |

# 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. Rețea proprietară definită prin software, care conectează toate serverele într-o plasă unificată (5)**

**5. Funcție automată de siguranță care blochează traficul de rețea când VPN-ul cade (10)**

**6. Hardware de server cu memorie volatilă, care șterge toate datele la fiecare ciclu de alimentare (7)**

**7. Funcție care schimbă periodic adresa IP externă fără a întrerupe tunelurile (9)**

**8. Funcționalitate de split tunneling care permite anumitor aplicații să ocolească VPN-ul (8)**

## VERTICAL

**1. Funcție de rutare double-VPN care criptează traficul prin două noduri de server distincte (8)**

**3. Tehnologie de ofuscare care ascunde semnăturile VPN pentru a imita traficul HTTPS obișnuit (10)**

**4. Filtru avansat care blochează reclamele, malware-ul și bannerele de consimțământ pentru cookie-uri (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

**2 orizontal: Rețea proprietară definită prin software, care conectează toate serverele într-o plasă unificată (5 litere):**

**5 orizontal: Funcție automată de siguranță care blochează traficul de rețea când VPN-ul cade (10 litere):**

**6 orizontal: Hardware de server cu memorie volatilă, care șterge toate datele la fiecare ciclu de alimentare (7 litere):**

**7 orizontal: Funcție care schimbă periodic adresa IP externă fără a întrerupe tunelurile (9 litere):**

**8 orizontal: Funcționalitate de split tunneling care permite anumitor aplicații să ocolească VPN-ul (8 litere):**

## VERTICAL

**1 vertical: Funcție de rutare double-VPN care criptează traficul prin două noduri de server distincte (8 litere):**

**3 vertical: Tehnologie de ofuscare care ascunde semnăturile VPN pentru a imita traficul HTTPS obișnuit (10 litere):**

**4 vertical: Filtru avansat care blochează reclamele, malware-ul și bannerele de consimțământ pentru cookie-uri (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.

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

**LISTĂ DE CUVINTE DIN VOCABULAR**

CLEANWEB DOARRAM MULTIHOP CAMOUFLAGE BYPASSER KILLSWITCH NEXUS IPROTATIV

# 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. CLEANWEB |
| B. DOARRAM |
| C. MULTIHOP |
| D. CAMOUFLAGE |
| E. BYPASSER |
| F. KILLSWITCH |
| G. NEXUS |
| H. IPROTATIV |

**DEFINIȚII ȘI CÂMPURI DE ASOCIERE**

_____ 1. Tehnologie de ofuscare care ascunde semnăturile VPN pentru a imita traficul HTTPS obișnuit.

_____ 2. Funcție automată de siguranță care blochează traficul de rețea când VPN-ul cade.

_____ 3. Filtru avansat care blochează reclamele, malware-ul și bannerele de consimțământ pentru cookie-uri.

_____ 4. Funcționalitate de split tunneling care permite anumitor aplicații să ocolească VPN-ul.

_____ 5. Hardware de server cu memorie volatilă, care șterge toate datele la fiecare ciclu de alimentare.

_____ 6. Funcție care schimbă periodic adresa IP externă fără a întrerupe tunelurile.

_____ 7. Funcție de rutare double-VPN care criptează traficul prin două noduri de server distincte.

_____ 8. Rețea proprietară definită prin software, care conectează toate serverele într-o plasă unificată.

## 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. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. RMRADAO
6. GUOLACAFEM
7. ILKIWTCHSL
8. VTIIOPATR

# Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

| | | | | |
|---|---|---|---|---|
| 1 | Funcții de securitate din Surfshark | | | |
| 2 | Semne că conexiunea ta VPN este lentă | | | |
| 3 | Protocoale VPN pe care le cunoști | | | |
| 4 | Lucruri pe care le protejează criptarea | | | |
| 5 | Amenințări din rețelele Wi-Fi publice | | | |
| 6 | Țări cunoscute pentru legile puternice de protecție a confidențialității | | | |
| 7 | Moduri de a crea o parolă puternică | | | |
| 8 | Dispozitive pe care ai instala Surfshark | | | |
| 9 | Întrebări pentru asistența clienți Surfshark | | | |
| 10 | Setări pe care le activezi pentru mai multă securitate | | | |
| 11 | Lucruri pe care Surfshark le poate ascunde de rețeaua ta | | | |
| 12 | Tipuri de scurgeri VPN | | | |
| 13 | Date pe care un VPN nu ar trebui să le stocheze niciodată | | | |
| 14 | Cuvinte care descriu o aplicație VPN bună | | | |
| 15 | Lucruri pe care le poate verifica un audit | | | |

# 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: OCOLIREA FILTRELOR DIN CAMPUS ȘI DE LA LOCUL DE MUNCĂ



**Scenariu:** Un student descoperă că Wi-Fi-ul campusului universității sale blochează toate porturile standard OpenVPN și WireGuard.

**Întrebare de discuție:** Ce funcție Surfshark îi permite studentului să se conecteze fără a fi detectat de administratorii de rețea?

## STUDIU DE CAZ 2: INVESTIGAȚIE JURNALISTICĂ CU RISC RIDICAT



**Scenariu:** Un jurnalist de investigație are nevoie de protecție suplimentară împotriva supravegherii în timp ce cercetează înregistrări corporative sensibile.

**Întrebare de discuție:** Cum oferă Dynamic MultiHop o confidențialitate superioară în comparație cu rutarea printr-un singur server?

## 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

17 7 29 26 22 23 11 11 19 21 18 24 1 24 11 27

19 21 18 24 7 13 7 1 31 2

11 17 24 11 16 11 24 1 24 7 1

**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 este Surfshark CleanWeb?

CleanWeb este o funcție de securitate integrată care blochează reclamele, trackerele, malware-ul și site-urile de phishing.

### Q2: Ce sunt serverele doar în RAM?

Serverele doar RAM rulează pe memorie volatilă, ceea ce înseamnă că datele din memorie sunt șterse ori de câte ori serverele repornesc.

### Q3: Ce este Surfshark MultiHop?

MultiHop (Double VPN) direcționează și criptează conexiunea ta la internet prin două locații de server diferite.

### Q4: Cum funcționează Camouflage Mode?

Modul Camouflage ofuscă traficul VPN, astfel încât ISP-ul tău să nu poată afla că folosești un VPN.

### Q5: Ce este funcția Bypasser?

Bypasser este instrumentul de split tunneling al Surfshark, care permite unor aplicații sau site-uri web specifice să ocolească VPN-ul.

# 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: Are Surfshark un Kill Switch?

Da, Kill Switch te deconectează de la internet dacă VPN-ul se întrerupe neașteptat.

### Q7: Ce standard de criptare folosește Surfshark?

Surfshark folosește AES-256-GCM și ChaCha20, plus AEGIS-256X2 pe noul său protocol Dausos.

### Q8: A fost auditată politica no-logs a Surfshark?

Da, Deloitte a verificat politica no-logs a Surfshark în 2023 și din nou în 2025.

### Q9: Ce este Surfshark Nexus?

Nexus este o arhitectură SDN avansată care conectează toate serverele într-o rețea unificată, pentru o rutare mai fluentă.

### Q10: Ce este funcția IP Rotator?

IP Rotator schimbă automat adresa ta IP la fiecare câteva minute, fără a întrerupe sesiunea ta VPN.

# 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: Prin ce diferă Dynamic MultiHop de Double VPN tradițional?

Dynamic MultiHop îți permite să personalizezi orice combinație de servere de intrare și de ieșire din întreaga lume.

### Q2: Funcționează CleanWeb 2.0 în extensiile de browser?

Da, CleanWeb 2.0 blochează reclamele video, ferestrele de consimțământ pentru cookie-uri și bannerele de alertă în Chrome/Firefox.

### Q3: Ce este Alternative ID în suita de securitate?

Alternative ID generează pseudonime personale unice, adrese de e-mail și măști de telefon.

### Q4: Cum previne Surfshark scurgerile DNS?

Surfshark direcționează toate cererile de domenii prin propriile servere DNS private de pe fiecare nod.

### Q5: Acceptă Surfshark criptarea ChaCha20 pe mobil?

Da, WireGuard pe Android și iOS folosește ChaCha20-Poly1305 pentru o eficiență mobilă superioară.

# 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: Ce este modul NoBorders din Surfshark?

NoBorders detectează automat mediile de rețea restrictive și oferă servere specializate.

### Q7: Cine a efectuat auditurile de securitate ale extensiilor de browser Surfshark?

Firma independentă de securitate cibernetică Cure53 a finalizat audituri ale extensiilor de browser și ale sistemelor de server.

### Q8: Cum protejează Surfshark împotriva scurgerilor IPv6?

Surfshark direcționează traficul IPv6 în siguranță sau îl restricționează în mod sigur pentru a preveni orice scurgere necriptată.

### Q9: Unde se află jurisdicția legală a Surfshark?

Surfshark funcționează conform legislației din Țările de Jos, respectând standardele europene stricte de confidențialitate GDPR.

### Q10: Acceptă Surfshark autentificarea în doi factori (2FA)?

Da, iar Surfshark One adaugă o blocare 2FA, astfel încât doar tu poți modifica setările funcțiilor.

# 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**

1. Surfshark afirmă că întreaga sa rețea de peste 4.500 de servere rulează pe hardware volatil, fără discuri, doar cu RAM.

**2. INFORMAȚII DESPRE VPN**

2. Firma din Big Four, Deloitte, a verificat politica Surfshark de a nu păstra jurnale în 2023 și din nou în noiembrie 2025.

**3. INFORMAȚII DESPRE VPN**

3. Arhitectura proprietară Nexus conectează toate serverele globale într-o rețea dinamică definită prin software.

**4. INFORMAȚII DESPRE VPN**

4. Rotating IP îți schimbă adresa IP aproximativ la fiecare cinci minute, fără a întrerupe conexiunea VPN.

**5. INFORMAȚII DESPRE VPN**

5. CleanWeb 2.0 blochează direct în browsere ferestrele pop-up intruzive de consimțământ pentru cookie-uri și reclamele video.

**6. INFORMAȚII DESPRE VPN**

6. Dynamic MultiHop permite utilizatorilor să creeze trasee de criptare personalizate prin două servere, în 100 de țări.

**7. PERSPECTIVĂ ASUPRA VPN-URILOR**

7. Modul Camuflaj elimină semnăturile antetelor VPN, astfel încât traficul nu se mai deosebește de HTTPS obișnuit.

**8. PERSPECTIVĂ ASUPRA VPN-URILOR**

8. Alternative ID generează pseudonime de unică folosință și măști de e-mail pentru a proteja utilizatorii de scurgerile din bazele de date.

**9. PERSPECTIVĂ ASUPRA VPN-URILOR**

9. Surfshark aplică criptarea simetrică AES-256-GCM alături de ChaCha20 pe protocoalele WireGuard.

**10. INFORMAȚII DESPRE VPN**

10. Modul NoBorders se activează automat în rețelele restricționate pentru a oferi acces rezilient prin tunel.

# 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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

## Barem: Punct de control 1 – Alegere multiplă

**1** **Blocator de conținut integrat** APĂRARE ÎMPOTRIVA RECLAMELOR ȘI A MALWARE-ULUI **Răspuns corect: B**

### NOTĂ PENTRU PROFESOR

CleanWeb este filtrul de securitate integrat al Surfshark, care blochează reclamele, domeniile de tracking, site-urile de phishing și scripturile URL rău intenționate la nivelul rețelei. Citare: CleanWeb Security Specs.

**2** **Infrastructură 100% doar cu RAM** ARHITECTURA RAM **Răspuns corect: B**

### NOTĂ PENTRU PROFESOR

Surfshark rulează servere exclusiv în RAM, așa că datele din memoria serverului sunt șterse când serverul este oprit sau repornit. Citare: Cure53 Infrastructure Audit.

**3** **Dublă tunelare MultiHop** VPN MULTI-HOP **Răspuns corect: B**

### NOTĂ PENTRU PROFESOR

MultiHop (Double VPN) criptează traficul prin două noduri de server distincte, în țări diferite, pentru a preveni atacurile de corelare a traficului. Citare: Surfshark MultiHop Guide.

**4** **Ofuscarea prin modul Camouflage** OFUSCARE **Răspuns corect: B**

### NOTĂ PENTRU PROFESOR

Modul Camouflage modifică antetele pachetelor OpenVPN pentru a deghiza traficul VPN în trafic HTTPS obișnuit, ocolind blocările restrictive ale firewall-urilor. Citare: Surfshark Stealth Whitepaper.

**5** **Split tunneling Bypasser** SPLIT TUNNELING **Răspuns corect: B**

### NOTĂ PENTRU PROFESOR

Bypasser este instrumentul de split tunneling al Surfshark, care le permite utilizatorilor să selecteze aplicații sau site-uri web specifice care să fie direcționate direct prin conexiunea lor obișnuită la ISP. Citare: Surfshark Client Features.

## Barem: Punct de control 2 – Adevărat sau fals

**6** **Ștergerea datelor din memoria volatilă** — SECURITATEA SERVERELOR — **Răspuns corect: Adevărat**

### NOTĂ PENTRU PROFESOR

Serverele doar RAM nu stochează date pe hard disk-uri permanente; repornirea hardware-ului șterge imediat toată memoria operațională. Citare: RAM Server Architecture.

**7** **Ascunderea față de ISP prin modul Camouflage** — ASCUNDEREA TRAFICULUI — **Răspuns corect: Adevărat**

### NOTĂ PENTRU PROFESOR

Modul Camouflage elimină semnăturile protocolului OpenVPN, împiedicând ISP-urile să detecteze că utilizatorul este conectat la un tunel VPN. Citare: Deep Packet Inspection Guide.

**8** **Extensii de browser CleanWeb 2.0** — EXTENSIE DE BROWSER — **Răspuns corect: Adevărat**

### NOTĂ PENTRU PROFESOR

CleanWeb 2.0 funcționează în cadrul extensiilor de browser pentru a bloca în timp real ferestrele pop-up pentru consimțământul privind cookie-urile, reclamele video și scripturile de redirecționare rău intenționate. Citare: CleanWeb 2.0 Release Notes.

**9** **Zero păstrare a jurnalelor de conexiune** — POLITICĂ NO-LOGS — **Răspuns corect: Fals**

### NOTĂ PENTRU PROFESOR

Surfshark menține o politică strictă zero-logs, auditată independent, fără a înregistra adrese IP, marcaje temporale ale conexiunilor sau jurnale ale lățimii de bandă. Citare: Deloitte No-Logs Audit.

**10** **Rotația dinamică a IP-urilor Nexus** — REȚEAUA NEXUS — **Răspuns corect: Adevărat**

### NOTĂ PENTRU PROFESOR

Rețeaua definită prin software Surfshark Nexus schimbă dinamic adresele IP ale utilizatorilor la fiecare câteva minute, fără a întrerupe conexiunea VPN activă. Citare: Surfshark Nexus Architecture.

# 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. CLEANWEB | D 2. DOAR RAM | G 3. MULTI-HOP | F 4. CAMOUFLAGE |
| B 5. BYPASSER | A 6. KILL SWITCH | H 7. NEXUS | E 8. ROTATIV |

## PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

| | | | |
|---|---|---|---|
| 1 CLEANWEB | 2 DOAR RAM | 3 MULTI-HOP | 4 CAMOUFLAGE |
| 5 BYPASSER | 6 NEXUS | | |

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

| | | | |
|---|---|---|---|
| 1 D – CAMOUFLAGE | 2 F – KILLSWITCH | 3 A – CLEANWEB | 4 E – BYPASSER |
| 5 B – DOARRAM | 6 H – IPROTATIV | 7 C – MULTIHOP | 8 G – NEXUS |

### NOTE DE DISCUȚIE PENTRU PROFESORI

**Termeni-cheie:**
Verifică dacă elevii pot explica CLEANWEB, DOAR RAM și MULTI-HOP 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.

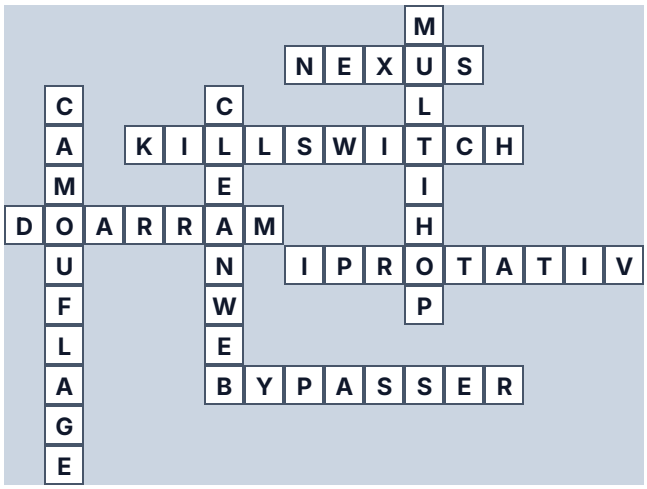
**Evaluarea surselor:**
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

# Chei de rezolvare ale puzzle-urilor și note pentru profesor

## SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

## SOLUȚIA CUVINTELOR ÎNCRUCIȘATE




## GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

### ORIZONTAL

**2 orizontal: NEXUS** Rețea proprietară definită prin software, care conectează toate serverele într-o plasă unificată (5 litere)

**5 orizontal: KILLSWITCH** Funcție automată de siguranță care blochează traficul de rețea când VPN-ul cade (10 litere)

**6 orizontal: DOARRAM** Hardware de server cu memorie volatilă, care șterge toate datele la fiecare ciclu de alimentare (7 litere)

**7 orizontal: IPROTATIV** Funcție care schimbă periodic adresa IP externă fără a întrerupe tunelurile (9 litere)

**8 orizontal: BYPASSER** Funcționalitate de split tunneling care permite anumitor aplicații să ocolească VPN-ul (8 litere)

### VERTICAL

**1 vertical: MULTIHOP** Funcție de rutare double-VPN care criptează traficul prin două noduri de server distincte (8 litere)

**3 vertical: CAMOUFLAGE** Tehnologie de ofuscare care ascunde semnăturile VPN pentru a imita traficul HTTPS obișnuit (10 litere)

**4 vertical: CLEANWEB** Filtru avansat care blochează reclamele, malware-ul și bannerele de consimțământ pentru cookie-uri (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. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. R M R A D A O — **DOARRAM**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. V T I I O P A T R — **IPROTATIV**

## BAREMUL PROVOCĂRII CU CODUL SECRET

**"NEXUS ȘI IP ROTATIV PROTEJEAZĂ INTIMITATEA"**

# Barem pentru studiile de caz

## A STUDIU DE CAZ 1: OCOLIREA FILTRELOR DIN CAMPUS ȘI DE LA LOCUL DE MUNCĂ

Soluția profesorului

### BAREM DE NOTARE ȘI GHID DE SOLUȚII

- Analiza scenariului: Un student constată că Wi-Fi-ul campusului universității sale blochează toate porturile standard OpenVPN și WireGuard.
- Întrebare de focalizare: Care funcție Surfshark îi permite studentului să se conecteze fără a fi detectat de administratorii de rețea?
- Strategie și soluție recomandate: Activează Camouflage Mode (OpenVPN), care ascunde metadatele VPN, astfel încât firewall-urile văd navigare HTTPS obișnuită.

## B STUDIU DE CAZ 2: INVESTIGAȚIE JURNALISTICĂ CU RISC RIDICAT

Soluția profesorului

### BAREM DE NOTARE ȘI GHID DE SOLUȚII

- Analiza scenariului: Un jurnalist de investigație are nevoie de protecție suplimentară împotriva supravegherii în timp ce cercetează documente corporative sensibile.
- Întrebare de focalizare: Cum oferă Dynamic MultiHop o confidențialitate superioară în comparație cu rutarea printr-un singur server?
- Strategie și soluție recomandate: Dynamic MultiHop direcționează traficul prin servere de intrare și de ieșire din două țări, astfel încât niciun server singur să nu poată expune utilizatorul.