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

# Cel mai bun VPN pentru afaceri

Recenzie practică despre securitatea, scalabilitatea și administrarea centralizată a VPN-urilor pentru afaceri.

## PREZENTARE GENERALĂ DE ÎNVĂȚARE: CEL MAI BUN VPN PENTRU AFACERI

**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 rețelele Business VPN și de acces la distanță. Vei explora arhitecturi Zero Trust, tuneluri IPsec site-to-site, cadre SASE, autentificări multifactor și verificări de securitate a punctelor terminale.

### 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-bun-vpn-pentru-afaceri/

# Harta ta de învățare despre VPN pentru companii

- Identifică principalii furnizori VPN pentru afaceri și funcțiile lor specifice echipelor.
- Analizează diferențele dintre confidențialitatea VPN-urilor pentru consumatori și controalele administrative ale VPN-urilor pentru afaceri.
- Diferențiază VPN-urile cu acces la distanță de tunelurile corporative site-to-site.

## INSTRUCȚIUNI PENTRU GHIDUL VPN PENTRU AFACERI

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 configurațiile de acces la distanță pentru întreprinderi. Încheie cu activitatea bonus Gândește repede.

## ACCES LA DISTANȚĂ PENTRU ÎNTREPRINDERI ȘI SECURE EDGE (INTRODUCERE)

Securizarea accesului la distanță în companii presupune trecerea de la modelele VPN tradiționale bazate pe perimetru la arhitecturi Zero Trust. Aplicarea unei autentificări multifactor (MFA) puternice și a cadrelor Secure Access Service Edge (SASE) protejează activele sensibile de punctele finale compromise.

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

## Punct de control 1: Provocare cu alegere multiplă

**1. Ce tip de VPN pentru afaceri conectează între ele rețelele unor birouri întregi?**

- A. VPN site-to-site
- B. VPN de acces la distanță
- C. VPN pentru consumatori
- D. Smart DNS

**2. Care alegere este evidențiată ca cea mai bună în general pentru echipele de afaceri?**

- A. NordLayer
- B. Surfshark
- C. Proton VPN
- D. Private Internet Access

**3. Ce previne o adresă IP statică dedicată pentru echipele de afaceri?**

- A. Includerea adreselor IP pe liste negre
- B. Viteza routerului scade
- C. Comprimarea datelor
- D. Actualizări ale clientului

**4. Ce furnizor este evidențiat ca fiind cel mai bun pentru infrastructură dedicată?**

- A. Proton VPN
- B. NordLayer
- C. Surfshark
- D. Private Internet Access

**5. Ce funcție oferă un panou de administrare centralizat pentru gestionarea utilizatorilor?**

- A. Controale de administrator
- B. Redirecționarea porturilor
- C. Emularea routerului
- D. Tunelare divizată

## Punct de control 2: Provocare Adevărat sau Fals

### 6 Întrebare 6

6. VPN-urile pentru acces la distanță permit angajaților individuali să se conecteze de oriunde.

Adevărat Fals

### 7 Întrebare 7

7. VPN-urile pentru consumatori protejează o întreagă organizație dintr-un singur panou de administrare.

Adevărat Fals

### 8 Întrebare 8

8. Adresele IP dedicate separă traficul companiei de traficul public.

Adevărat Fals

### 9 Întrebare 9

9. Private Internet Access este evidențiat drept cel mai bun pentru marile întreprinderi.

Adevărat Fals

### 10 Întrebare 10

10. SASE integrează rutarea WAN cu cadre de securitate livrate din cloud.

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. Cel mai bine clasat furnizor general pentru echipele de business este _____ .
2. Interconectarea mai multor sucursale corporative se face printr-o conexiune de tip _____ .
3. Pentru a evita includerea adreselor pe liste negre, echipele implementează un _____ .
4. Administratorii gestionează permisiunile dispozitivelor dintr-un _____ central.
5. Adăugarea dinamică de locuri pentru echipele în creștere înseamnă _____ .
6. Respectarea standardelor de reglementare și de audit al datelor necesită _____ .

**BANCĂ DE CUVINTE DIN VOCABULAR**

CONFORMITATE GATEWAY IP STATIC NORDLAYER PANOU DE CONTROL
RUTARE SCALABILITATE SITE-TO-SITE

**Scrie răspunsurile aici:**

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

# Punct de control 4: Asocierea conceptelor-cheie

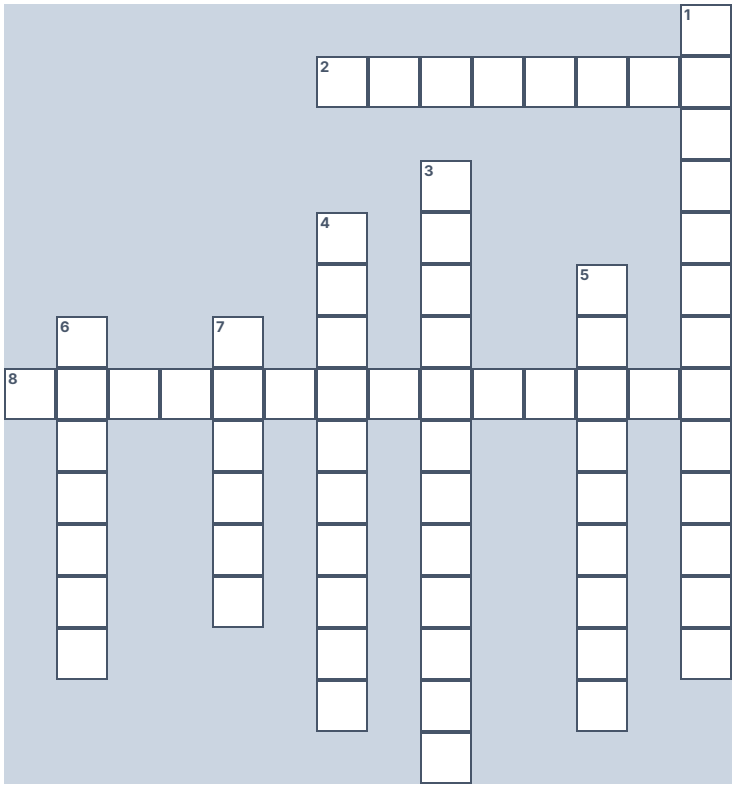
## ASOCIEREA DEFINIȚIILOR

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

| | | | |
|---|---|---|---|
| ☐ | 1. NORDLAYER | A | Creștere dinamică a echipei cu mai multe locuri. |
| ☐ | 2. SITE-LA-SITE | B | Cea mai bună alegere generală pentru afaceri. |
| ☐ | 3. IP STATIC | C | Controlul traficului prin split tunneling. |
| ☐ | 4. PANOU DE CONTROL | D | Audit standard de reglementare. |
| ☐ | 5. SCALABILITATE | E | Nod de intrare pentru autentificare la distanță. |
| ☐ | 6. CONFORMITATE | F | Adresă dedicată care nu se află pe liste negre. |
| ☐ | 7. RUTARE | G | Tunel de interconectare a rețelei de birou. |
| ☐ | 8. GATEWAY | H | Consolă centrală de control administrativ. |

## 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. Adresă dedicată, care nu este pe lista neagră (8)**

**8. Consola centrală de administrare (14)**

### VERTICAL

**1. Creșterea dinamică a echipei, cu mai multe locuri (13)**

**3. Standard de audit și de reglementare (12)**

**4. Tunel de interconectare a rețelelor de birou (10)**

**5. Cea mai bună alegere generală pentru business (9)**

**6. Nod de intrare la distanță pentru autentificare (7)**

**7. Controlul traficului în split tunneling (6)**

# 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: Adresă dedicată, care nu este pe lista neagră (8 litere):**

**8 orizontal: Consola centrală de administrare (14 litere):**

## VERTICAL

**1 vertical: Creșterea dinamică a echipei, cu mai multe locuri (13 litere):**

**3 vertical: Standard de audit și de reglementare (12 litere):**

**4 vertical: Tunel de interconectare a rețelelor de birou (10 litere):**

**5 vertical: Cea mai bună alegere generală pentru business (9 litere):**

**6 vertical: Nod de intrare la distanță pentru autentificare (7 litere):**

**7 vertical: Controlul traficului în split tunneling (6 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.

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

**LISTĂ DE CUVINTE DIN VOCABULAR**

NORDLAYER SITETOSITE IPSTATIC PANOUDECONTROL SCALABILITATE
CONFORMITATE RUTARE GATEWAY

# 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. NORDLAYER |
| B. SITETOSITE |
| C. IPSTATIC |
| D. PANOUDECONTROL |
| E. SCALABILITATE |
| F. CONFORMITATE |
| G. RUTARE |
| H. GATEWAY |

| DEFINIȚII ȘI CÂMPURI DE ASOCIERE |
| --- |
| 1. Controlul traficului în split tunneling. |
| 2. Consola centrală de administrare. |
| 3. Nod de intrare la distanță pentru autentificare. |
| 4. Adresă dedicată, care nu este pe lista neagră. |
| 5. Standard de audit și de reglementare. |
| 6. Tunel de interconectare a rețelelor de birou. |
| 7. Cea mai bună alegere generală pentru business. |
| 8. Creșterea dinamică a echipei, cu mai multe locuri. |

## Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie ai intermedierii domeniilor. Scrie răspunsurile în casetele de introducere furnizate.

1. ALDONYERR
2. TICPITAS
3. CSLTITEAIABAL
4. EATRRU
5. IOEIESTSTT
6. DETUNRCONPAOLO
7. ITOCOMEATNRF
8. AEYGAWT

# Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

| | | | | |
|---|---|---|---|---|
| 1 | Promisiuni pe care le face un furnizor VPN bun | | | |
| 2 | Lucruri care pot perturba o videoconferință | | | |
| 3 | Reguli pentru munca la distanță în siguranță | | | |
| 4 | Programe de birou pe care le cunoști | | | |
| 5 | Lucruri pe care le poate vedea furnizorul tău de internet | | | |
| 6 | Motive pentru care ai oferi angajaților un VPN | | | |
| 7 | Lucruri de care un VPN nu te poate proteja | | | |
| 8 | Locuri din care lucrează angajații | | | |
| 9 | Instrumente pe care o companie le folosește zilnic | | | |
| 10 | Moduri de a te autentifica în siguranță | | | |
| 11 | Date pe care o companie trebuie să le protejeze | | | |
| 12 | Roluri dintr-un departament IT | | | |
| 13 | Dispozitive pe care le poate avea un angajat | | | |
| 14 | Lucruri de făcut după o breșă de securitate | | | |
| 15 | Cuvinte care descriu Zero Trust | | | |

# 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: ÎNSCRIEREA PE LISTA NEAGRĂ A UNUI IP PUBLIC PARTAJAT



**Scenariu:** O echipă de vânzări accesează bazele de date ale companiei printr-un VPN de consum, dar este blocată pentru că IP-ul de ieșire partajat a fost pus pe lista neagră de sistemele antifraudă.

**Întrebare de discuție:** Propune o configurare a infrastructurii VPN pentru companii care să rezolve această blocare.

## STUDIU DE CAZ 2: INTERCONECTAREA BIROURILOR CORPORATIVE



**Scenariu:** O companie cu birouri la München și Boston trebuie să partajeze în siguranță serverele locale de fișiere, fără a trimite traficul prin spațiile web publice.

**Întrebare de discuție: Alege topologia VPN potrivită pentru afaceri.**

## 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**

| 31 | 7 | 21 | 18 | | 24 | 21 | 26 | 22 | 24 | | 19 | 21 | 18 | 24 | 7 | 13 | 7 | 1 | 31 | 2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | |

| 21 | 7 | 25 | 7 | 15 | 7 | | 16 | 18 | 6 | 7 | 21 | 17 | 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 este un VPN pentru afaceri?

O conexiune de rețea securizată care permite personalului și birourilor aflate la distanță să acceseze în siguranță datele private ale companiei.

### Q2: Prin ce diferă VPN-urile pentru consumatori de cele pentru afaceri?

VPN-urile pentru consumatori ascund navigarea personală; VPN-urile pentru afaceri protejează sistemele corporative cu console administrative centrale.

### Q3: Ce este un VPN site-la-site?

Un tunel care conectează rețelele întregi ale birourilor fizice între ele prin web.

### Q4: Ce este un VPN pentru acces la distanță (Remote Access VPN)?

Un tunel care permite angajaților individuali aflați la distanță să se conecteze în siguranță la rețeaua companiei.

### Q5: Care este beneficiul unei adrese IP statice dedicate?

Menține traficul corporativ separat de grupurile publice și evită includerea pe liste negre a IP-urilor partajate.

# 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: Care furnizor este cel mai bun pentru întreprinderile mici?

Private Internet Access (PIA), remarcat pentru prețul accesibil echipelor mici și simplitatea configurării.

### Q7: Care VPN pentru business este clasat pe locul #1 în general?

NordLayer, cu scorul 92/100 acordat de VPN.com pentru funcții și instrumente de administrare.

### Q8: Ce este scalabilitatea echipei în VPN-uri?

Capacitatea de a adăuga dinamic locuri de utilizator, licențe și gateway-uri pe măsură ce o companie crește.

### Q9: De ce este esențială gestionarea centralizată?

Le permite administratorilor să aplice politici de securitate și să revoce accesul angajaților dintr-un singur tablou de bord.

### Q10: Ce este SASE?

Secure Access Service Edge, care combină rutarea WAN cu servicii de securitate furnizate din cloud.

# 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 securizează split tunneling-ul echipele?

Păstrează traficul SaaS privat în interiorul tunelului securizat, în timp ce accesul web public este direcționat local.

### Q2: Ce oferă Proton VPN companiilor?

Infrastructură de servere dedicate, evaluată cu 88/100 de VPN.com (cu sediul în Elveția).

### Q3: Ce standarde de conformitate impun utilizarea VPN-urilor?

PCI DSS impune criptare puternică în rețelele publice; HIPAA și GDPR o așteaptă ca măsură de protecție.

### Q4: Poți rula VPN-uri pentru companii pe routere?

Da, configurarea tunelurilor VPN pe routere protejează automat toate dispozitivele din birou.

### Q5: Ce este autentificarea multifactor?

Solicitarea mai multor credențiale (precum carduri inteligente sau coduri SMS) pentru autentificarea conectărilor.

# 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 ajung adresele IP partajate pe liste negre?

Deoarece sunt folosite în comun de mii de utilizatori, dintre care unii pot desfășura activități rău intenționate.

### Q7: Cum autentifică un gateway utilizatorii?

Prin verificarea certificatelor client, a parolelor și a codurilor multi-factor în directoarele active.

### Q8: Ce oferă Surfshark echipelor?

Alegerea VPN.com pentru pachetele de securitate, cu scorul 84/100, cu servere doar RAM.

### Q9: Cum auditezi conexiunile VPN de business?

Prin inspectarea jurnalelor de conexiune, a metricilor de utilizare a datelor și a istoricului de autentificare în consola de administrare.

### Q10: Ce este controlul accesului Zero Trust?

O paradigmă în care toate dispozitivele sunt considerate neîncrezătoare, iar fiecare sesiune necesită verificare.

# 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**

Un VPN pentru afaceri criptează traficul și protejează sistemele companiei de interceptarea în rețelele publice.

**2. INFORMAȚII DESPRE VPN**

VPN-urile site-to-site conectează în siguranță rețele întregi de sucursale, fără a expune gazdele locale.

**3. INFORMAȚII DESPRE VPN**

VPN-urile pentru consumatori maschează navigarea personală, în timp ce VPN-urile pentru afaceri protejează gateway-urile resurselor enterprise.

**4. INFORMAȚII DESPRE VPN**

VPN.com acordă NordLayer 92/100, cel mai bun VPN de afaceri în ansamblu.

**5. INFORMAȚII DESPRE VPN**

VPN.com acordă Proton VPN 88/100 și îl numește cel mai bun pentru infrastructură dedicată.

**6. INFORMAȚII DESPRE VPN**

VPN.com acordă Private Internet Access 76/100 și îl clasează drept cel mai bun pentru echipele mici de afaceri.

**7. PERSPECTIVĂ ASUPRA VPN-URILOR**

Panourile administrative centrale permit responsabililor de securitate să gestioneze permisiunile utilizatorilor și regulile de acces.

**8. PERSPECTIVĂ ASUPRA VPN-URILOR**

IP-urile statice dedicate împiedică blocarea echipelor de către sistemele antifraudă care partajează IP-uri.

**9. PERSPECTIVĂ ASUPRA VPN-URILOR**

GDPR menționează criptarea ca măsură adecvată pentru protejarea datelor cu caracter personal.

**10. INFORMAȚII DESPRE VPN**

Arhitecturile Zero Trust verifică toate punctele terminale la distanță, indiferent de locație sau de acreditări.

# 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] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

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

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

## Barem: Punct de control 1 – Alegere multiplă

**1** **Topologia tunelului** SITE-LA-SITE — **Răspuns corect: A**

### NOTĂ PENTRU PROFESOR

VPN-urile site-to-site conectează în siguranță între ele sucursale îndepărtate întregi. Citare: NIST Zero Trust.

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

### NOTĂ PENTRU PROFESOR

VPN.com îi acordă NordLayer 92/100 și îl clasează drept cel mai bun în general pentru echipele de afaceri.

**3** **Lista albă de IP-uri** IP DEDICAT — **Răspuns corect: A**

### NOTĂ PENTRU PROFESOR

IP-urile statice dedicate împiedică blocarea accesului echipelor din cauza listelor negre de IP-uri partajate. Citare: NIST Remote Access.

**4** **Întrebarea 4** — **Răspuns corect: A**

### NOTĂ PENTRU PROFESOR

VPN.com îi acordă Proton VPN 88/100 și îl numește cel mai bun pentru infrastructură dedicată.

**5** **Consolă centrală** CONTROALE DE ADMINISTRATOR — **Răspuns corect: A**

### NOTĂ PENTRU PROFESOR

Panourile centralizate permit responsabililor de securitate să gestioneze permisiunile utilizatorilor și locurile. Citare: NIST Remote Access.

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

**6** **Conexiuni la distanță** ACCES LA DISTANȚĂ — **Răspuns corect: Adevărat**

### NOTĂ PENTRU PROFESOR

VPN-urile pentru acces la distanță permit lucrătorilor individuali la distanță să se conecteze la servere private. Citare: NIST Remote Access.

**7** **Tuneluri pentru întreprinderi** LIMITE PENTRU UTILIZATORII INDIVIDUALI — **Răspuns corect: Fals**

### NOTĂ PENTRU PROFESOR

VPN-urile pentru consumatori nu au controale administrative centralizate și nu sunt potrivite pentru auditurile organizațiilor. Citare: CISA Infrastructure.

**8** **Izolarea gateway-ului** TUNEL DEDICAT — **Răspuns corect: Adevărat**

### NOTĂ PENTRU PROFESOR

IP-urile dedicate izolează traficul companiei de zgomotul public pentru a securiza bazele de date. Citare: NIST Zero Trust.

**9** **Întrebarea 9** — **Răspuns corect: Fals**

### NOTĂ PENTRU PROFESOR

VPN.com clasează PIA (76/100) drept cel mai bun pentru întreprinderile mici, nu pentru companiile mari.

**10** **Securitatea fuzionează** STANDARDUL SASE — **Răspuns corect: Adevărat**

### NOTĂ PENTRU PROFESOR

SASE îmbină rutarea WAN enterprise cu securitatea zero-trust livrată din cloud. Citare: Cloudflare Zero Trust.

# 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

| | | | |
|---|---|---|---|
| B 1. NORDLAYER | G 2. SITE-LA-SITE | F 3. IP STATIC | H 4. PANOU DE CONTROL |
| A 5. SCALABILITATE | D 6. CONFORMITATE | C 7. RUTARE | E 8. GATEWAY |

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

| | | | |
|---|---|---|---|
| 1 NORDLAYER | 2 SITE-TO-SITE | 3 IP STATIC | 4 PANOU DE CONTROL |
| 5 SCALABILITATE | 6 CONFORMITATE | | |

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

| | | | |
|---|---|---|---|
| 1 G – RUTARE | 2 D – PANOUDECONTROL | 3 H – GATEWAY | 4 C – IPSTATIC |
| 5 F – CONFORMITATE | 6 B – SITETOSITE | 7 A – NORDLAYER | 8 E – SCALABILITATE |

### NOTE DE DISCUȚIE PENTRU PROFESORI

**Termeni-cheie:**
Verifică dacă elevii pot explica NORDLAYER, SITE-LA-SITE și IP STATIC 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.

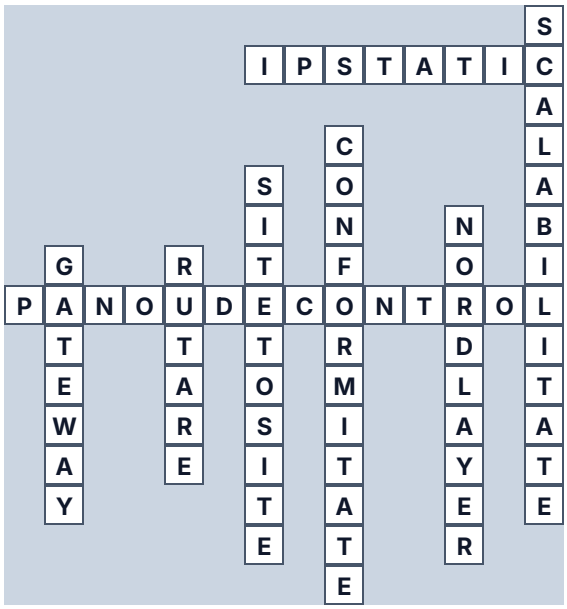
**Evaluarea surselor:**
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

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

## SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

## SOLUȚIA CUVINTELOR ÎNCRUCIȘATE




## GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

### ORIZONTAL

**2 orizontal: IPSTATIC** Adresă dedicată, care nu este pe lista neagră (8 litere)

**8 orizontal: PANOUDECONTROL** Consola centrală de administrare (14 litere)

### VERTICAL

**1 vertical: SCALABILITATE** Creșterea dinamică a echipei, cu mai multe locuri (13 litere)

**3 vertical: CONFORMITATE** Standard de audit și de reglementare (12 litere)

**4 vertical: SITETOSITE** Tunel de interconectare a rețelelor de birou (10 litere)

**5 vertical: NORDLAYER** Cea mai bună alegere generală pentru business (9 litere)

**6 vertical: GATEWAY** Nod de intrare la distanță pentru autentificare (7 litere)

**7 vertical: RUTARE** Controlul traficului în split tunneling (6 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. ALDONYERR — NORDLAYER
2. TICPITAS — IPSTATIC
3. CSLTITEAIABAL — SCALABILITATE
4. EATRRU — RUTARE
5. IOEIESTSTT — SITETOSITE
6. DETUNRCONPAOLO — PANOUDECONTROL
7. ITOCOMEATNRF — CONFORMITATE
8. AEYGAWT — GATEWAY

## BAREMUL PROVOCĂRII CU CODUL SECRET

**"ZERO TRUST PROTEJEAZĂ REȚELE MODERNE"**

# Barem pentru studiile de caz

## A Studiu de caz 1: Înscrierea pe lista neagră a unui IP public partajat

Soluția profesorului

### GHID DE NOTARE

**Răspunsurile elevilor ar trebui să acopere următoarele puncte:**

- Analiza scenariului: O echipă de vânzări accesează bazele de date corporative folosind un VPN de consum, dar este blocată deoarece IP-ul de ieșire partajat a fost inclus pe lista neagră de sistemele antifraudă.
- Strategie și soluție recomandate: Implementează servere dedicate pentru business, împreună cu o adresă IP statică, pentru a separa traficul corporativ de grupurile publice.

## B Studiu de caz 2: Interconectarea birourilor corporative

Soluția profesorului

### GHID DE NOTARE

**Răspunsurile elevilor ar trebui să acopere următoarele puncte:**

- Analiza scenariului: O companie cu birouri la München și Boston trebuie să partajeze în siguranță serverele locale de fișiere, fără a trimite traficul prin spații web publice.
- Strategie și soluție recomandate: Configurează un tunel VPN site-la-site pentru a interconecta în siguranță, prin internet, cele două rețele locale ale birourilor.