Nume: _____ Data: _____ Punctaj: _____

VPN pentru acces la distanță

Securizarea punctelor finale ale personalului la distanță, autentificarea multifactor și configurarea tunelurilor IPsec.

PREZENTARE GENERALĂ DE ÎNVĂȚARE DESPRE VPN-URILE DE ACCES LA DISTANȚĂ

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 VPN cu acces la distanță. Vei explora tunelurile client-la-site, autentificările multifactor, verificările de postură ale punctelor terminale, plafoanele de lățime de bandă și auditul de securitate syslog.

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-business/acces-la-distanta/

Harta ta de învățare despre VPN pentru acces la distanță

- Punctele finale securizate ale personalului la distanță care accesează noduri din rețeaua locală.
- Configurează politicile de autentificare multifactor pentru autentificările la distanță.
- Configurează setări IPsec și OpenVPN de tip client-to-site.
- Auditează jurnalele conexiunilor la distanță pentru încălcări ale controlului accesului.
- Implementează verificări ale stării dispozitivului înainte de a acorda conexiuni la rețea.
- Optimizează debitul serverului pentru a preveni blocajul lățimii de bandă în telemuncă.

INSTRUCȚIUNI PENTRU VPN-URILE DE ACCES LA DISTANȚĂ

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 verificările de postură și autentificările cu mai mulți factori. Încheie cu activitatea bonus Gândește repede.

TUNELURI CLIENT-LA-SITE ȘI CONFORMITATEA PUNCTELOR FINALE (INTRODUCERE)

VPN-urile pentru acces la distanță stabilesc tuneluri securizate client-la-sit pentru angajații aflați în afara biroului. Securizarea acestor conexiuni presupune impunerea autentificării multifactor (MFA), efectuarea verificărilor de conformitate a posturii punctului final și auditarea jurnalelor prin colectoare syslog centrale.

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

Punct de control 1: Provocare cu alegere multiplă

1. Ce standard de autentificare ar trebui să impună portalurile VPN de acces la distanță?

- A) Multi-factor
- B) Un singur factor
- C) Necriptat
- D) Invitat local

2. Ce protocol este standardul pentru securizarea conexiunilor client-to-site pentru munca la distanță?

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3. Ce verificare confirmă dacă un laptop de la distanță este curat înainte de conectare?

- A) Verificare de postură
- B) Test de viteză
- C) Test ping
- D) Numărul de memorii

4. Unde sunt stocate jurnalele de conectare ale lucrătorilor la distanță pentru auditul de securitate?

- A) Server Syslog
- B) Cheie de registru
- C) Memoria clientului
- D) Browser web

5. Ce problemă apare atunci când numărul lucrătorilor la distanță depășește capacitatea de lățime de bandă a gateway-ului?

- A) Strangulare a lățimii de bandă
- B) Scurgere DNS
- C) Trecere prin handshake
- D) Expunerea IP-ului

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Autentificarea multifactor adaugă un token de validare secundar pentru a securiza autentificările la distanță.

- ○ Adevărat
- ○ Fals

7 Întrebare 7

7. Verificările de postură permit dispozitivelor la distanță cu firewall-ul dezactivat să acceseze servere private.

- ○ Adevărat
- ○ Fals

8 Întrebare 8

8. Jurnalele VPN pentru acces la distanță sunt esențiale pentru urmărirea intrărilor neautorizate în rețeaua corporativă.

- ○ Adevărat
- ○ Fals

9 Întrebare 9

9. OpenVPN și IPsec sunt protocoale învechite care nu reușesc să cripteze datele clienților la distanță.

- ○ Adevărat
- ○ Fals

10 Întrebare 10

10. Blocajul lățimii de bandă la gateway apare atunci când traficul de la distanță depășește capacitatea plăcii de conexiune.

- ○ 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 proteja portalurile corporative, autentificările la distanță trebuie să impună autentificare _____ .

2. Clienții la distanță criptează datele din tunel folosind protocolul standard _____ .

3. Dispozitivele trebuie să treacă o verificare de _____ **securitate înainte de a primi conexiuni la rețea.**

4. Jurnalele auditabile de intrare sunt transmise continuu către un server central _____ .

5. Traficul intens din timpul programului de lucru poate duce la congestia gateway-ului din cauza lipsei de _____ .

6. Driverele adaptorului virtual gestionează procesul de _____ **tip client-la-site în Windows și macOS.**

BANCĂ DE CUVINTE DIN VOCABULAR

CRIPTARE FIREWALL LĂȚIME DE BANDĂ MULTIFACTOR OPENVPN POSTURĂ SYSLOG TUNELARE

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor-cheie

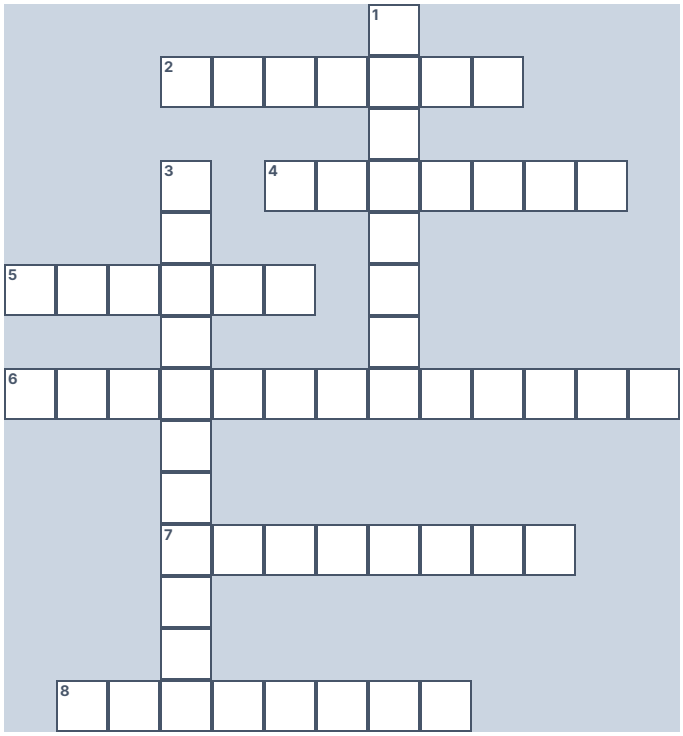
ASOCIEREA DEFINIȚIILOR

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

☐	1. MULTIFACTOR	A	Încapsularea datelor într-o cale securizată.
☐	2. OPENVPN	B	Colector central de jurnale de securitate.
☐	3. POSTURĂ	C	Limită a capacității de date a rețelei.
☐	4. SYSLOG	D	Protocol standard client-to-site.
☐	5. LĂȚIME DE BANDĂ	E	Validarea la distanță a stării dispozitivului.
☐	6. CRIPTARE	F	Reguli ale sistemului de filtrare a traficului.
☐	7. TUNELARE	G	Amestecarea criptografică a pachetelor.
☐	8. FIREWALL	H	Securitate la autentificare care necesită token-uri suplimentare.

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. Validarea stării de sănătate a dispozitivului de la distanță (7)

4. Protocol standard client-la-site (7)

5. Colector central al jurnalelor de securitate (6)

6. Limita capacității de date a rețelei (13)

7. Codificarea criptografică a pachetelor (8)

8. Reguli ale sistemului de filtrare a traficului (8)

VERTICAL

1. Încapsularea datelor într-o cale securizată (8)

3. Securitate la autentificare care cere token-uri suplimentare (11)

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: Validarea stării de sănătate a dispozitivului de la distanță (7 litere):

4 orizontal: Protocol standard client-la-site (7 litere):

5 orizontal: Colector central al jurnalelor de securitate (6 litere):

6 orizontal: Limita capacității de date a rețelei (13 litere):

7 orizontal: Codificarea criptografică a pachetelor (8 litere):

8 orizontal: Reguli ale sistemului de filtrare a traficului (8 litere):

VERTICAL

1 vertical: Încapsularea datelor într-o cale securizată (8 litere):

3 vertical: Securitate la autentificare care cere token-uri suplimentare (11 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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

MULTIFACTOR OPENVPN POSTURĂ SYSLOG LĂȚIMEDEBANDĂ CRIPTARE TUNELARE FIREWALL

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. MULTIFACTOR
B. OPENVPN
C. POSTURĂ
D. SYSLOG
E. LĂȚIMEDEBANDĂ
F. CRIPTARE
G. TUNELARE
H. FIREWALL

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Colector central al jurnalelor de securitate.
2. Reguli ale sistemului de filtrare a traficului.
3. Încapsularea datelor într-o cale securizată.
4. Codificarea criptografică a pachetelor.
5. Protocol standard client-la-site.
6. Limita capacității de date a rețelei.
7. Validarea stării de sănătate a dispozitivului de la distanță.
8. Securitate la autentificare care cere token-uri suplimentare.

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. IAOUFCMTLRT
2. PSĂRUTO
3. ĂLEABDĂȚDMENI
4. EREALTUN
5. VNNEOPP
6. OLSSGY
7. CETARRPI
8. EIWLFLAR

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

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

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: IMPUNEREA MFA



Scenariu: Un analist de afaceri încearcă să se autentifice în baza de date a companiei în timp ce lucrează de la distanță. Introduce corect numele de utilizator și parola, dar portalul VPN blochează accesul și cere un cod de pe un token fizic.

Întrebare de discuție: Ce politică de securitate impune acest pas de dublă verificare?

STUDIU DE CAZ 2: CONFORMITATEA POSTURII DISPOZITIVULUI



Scenariu: Un colaborator extern își conectează laptopul personal la rețeaua corporativă la distanță. Clientul VPN întrerupe imediat conexiunea și notifică utilizatorul că definițiile antivirusului sunt depășite.

Întrebare de discuție: Ce verificare specializată a gateway-ului VPN a blocat această încercare de conectare?

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 6 7 1 5 5 7 22 15 1

6 11 22 24 1 17 25 2 19 21 18 24 7 13 7 1 31 2

21 7 25 7 1 26 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 un VPN de acces la distanță?

O metodă de conectare securizată care le permite angajaților care lucrează în afara biroului să se conecteze direct la serverele private ale companiei.

Q2: De ce este diferit client-la-site de site-la-site?

Modelul client-la-site conectează dispozitivele individuale ale utilizatorilor, în timp ce site-la-site leagă locații fizice întregi de birouri.

Q3: Ce este o verificare a posturii dispozitivului?

O scanare care verifică starea de securitate a unui dispozitiv la distanță (antivirus, nivelul de actualizare a sistemului de operare) înainte de a acorda accesul.

Q4: De ce este folosit OpenVPN pentru accesul la distanță?

Datorită protocolului său de securitate puternic, compatibilității între platforme și capacității de a gestiona conexiuni individuale.

Q5: Cum protejează MFA accesul la distanță?

Adaugă un token secundar de verificare, împiedicând accesul chiar dacă parolele angajaților sunt scurse sau furate.

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: Ce este un server syslog?

Un depozit centralizat de jurnale care stochează evenimentele de conectare, autentificările și alertele de sistem pentru auditurile de conformitate.

Q7: Ce cauzează blocajul lățimii de bandă?

Când cerințele agregate de lățime de bandă ale angajaților la distanță depășesc limita de viteză a internetului gateway-ului corporativ.

Q8: Pot conecta computerul de acasă la un VPN de serviciu?

Doar dacă dispozitivul trece auditurile corporative de verificare a posturii de securitate și este autorizat de administratorii IT.

Q9: Ce este încapsularea în rețea?

Încapsularea pachetelor de date în tranzit în antete de protocol criptate pentru a securiza transmisia.

Q10: Cum optimizează split tunneling-ul accesul la distanță?

Le permite angajaților să folosească ISP-ul local pentru navigarea obișnuită, în timp ce fișierele legate de muncă sunt direcționate prin 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: Cum îmbunătățește autentificarea bazată pe certificate accesul la distanță?

Leagă permisiunile de conectare de certificate digitale locale preinstalate, blocând dispozitivele negestionate sau neautorizate.

Q2: Care este riscul de securitate al split tunneling-ului pentru munca la distanță?

Creează o punte potențială prin care un dispozitiv local compromis poate direcționa amenințări externe în rețeaua privată.

Q3: Cum inspectează verificările de postură setările din registry?

Clientul VPN rulează scripturi locale care interoghează căile din registry pentru a verifica dacă software-ul de securitate corporativ rulează activ.

Q4: De ce folosesc syslog-urile implicit portul UDP 514?

Pentru a transmite jurnalele rapid, cu un overhead minim, deși configurările securizate impun acum încapsularea TLS peste TCP.

Q5: Cum rezolvă companiile blocajele de lățime de bandă ale gateway-ului?

Prin implementarea load balancerelor și distribuirea traficului de la distanță între nodurile de server regionale.

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: Care este funcția adaptoarelor virtuale TAP/TUN pe clienții la distanță?

Acționează ca plăci de rețea virtuale, direcționând traficul TCP/IP la nivel de dispozitiv direct în tunelul VPN criptat.

Q7: Cum susține IKEv2 MOBIKE mobilitatea angajaților la distanță?

Actualizează dinamic asocierile adreselor IP, menținând VPN-ul activ pe măsură ce utilizatorul trece între Wi-Fi și datele celulare.

Q8: Care este diferența dintre rutarea split și cea cu tunel complet?

Rutarea completă forțează tot traficul de internet al dispozitivului prin VPN, în timp ce rutarea divizată trimite doar adresele IP de destinație ale companiei.

Q9: Cum gestionează dispozitivele NAT conexiunile VPN la distanță?

Prin maparea intervalelor de porturi locale la adrese IP publice de gateway pentru a direcționa pachetele de date criptate care se întorc.

Q10: Ce standarde de conformitate impun auditarea accesului la distanță?

Standarde precum HIPAA, SOC 2 și PCI DSS cer înregistrarea și monitorizarea tuturor sesiunilor de conectare la distanță.

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

VPN-urile pentru acces la distanță stabilesc tuneluri securizate client-la-sit pentru lucrătorii aflați în afara biroului.

2. INFORMAȚII DESPRE VPN

Autentificarea multifactor este cerută de reglementările de conformitate pentru a proteja portalurile de afaceri la distanță.

3. INFORMAȚII DESPRE VPN

Verificările de postură confirmă setările de securitate ale clientului local înainte de a acorda acces la rețeaua privată.

4. INFORMAȚII DESPRE VPN

Serverele Syslog agregă jurnalele conexiunilor pentru a audita și a detecta încercările de acces neautorizat.

5. INFORMAȚII DESPRE VPN

Blocajele lățimii de bandă la gateway apar atunci când cerințele agregate de trafic de la distanță depășesc limitele de internet ale serverului.

6. INFORMAȚII DESPRE VPN

Adaptoarele de rețea virtuale încapsulează interogările de rețea ale sistemului de operare în protocoale securizate.

7. PERSPECTIVĂ ASUPRA VPN-URILOR

Suportul MOBIKE permite clienților la distanță să schimbe rețeaua fără a întrerupe tunelul VPN.

8. PERSPECTIVĂ ASUPRA VPN-URILOR

Rutarea prin tunel complet securizează tot traficul de internet al angajaților, dar crește sarcina pe gateway-ul corporativ.

9. PERSPECTIVĂ ASUPRA VPN-URILOR

Autentificarea prin certificate leagă autorizarea conexiunii VPN direct de hardware-ul gestionat de companie.

10. INFORMAȚII DESPRE VPN

Cadre precum SOC 2 și PCI DSS se așteaptă la înregistrarea și monitorizarea sesiunilor de acces la distanță.

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/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

Barem: Punct de control 1 – Alegere multiplă

1 **Token-uri de autentificare** SECURITATE MFA — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Autentificarea multifactor impune o verificare secundară pentru autentificări. Citare: MFA Implementation.

2 **Tunel OpenVPN** CLIENT-LA-SITE — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

OpenVPN este un protocol standard pentru securizarea tunelurilor client-site. Citație: OpenVPN Client.

3 **Audituri de postură** VERIFICAREA DISPOZITIVULUI — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Verificările de postură scanează dispozitivele finale pentru a identifica firewall-urile și instrumentele antivirus active. Citație: Posture Compliance.

4 **Agregator de jurnale** SERVER SYSLOG — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Serverele Syslog colectează jurnalele evenimentelor de securitate pentru a monitoriza încălcările de acces. Citare: Syslog Standard.

5 **Depășirea limitei cardului** BLOCAJ LA GATEWAY — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Blocajul lățimii de bandă la gateway apare atunci când traficul utilizatorilor depășește limitele serverului. Citare: Capacity Planning.

Barem: Punct de control 2 – Adevărat sau fals

6 **Token-uri de autentificare** VERIFICĂRI MFA

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Autentificarea multifactor impune o verificare secundară pentru autentificări. Citare: MFA Implementation.

7 **Întrebarea 7**

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Verificările de postură blochează dispozitivele cu firewall-ul sau antivirusul oprit, deci astfel de dispozitive sunt respinse.

8 **Agregator de jurnale** SERVER SYSLOG

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Serverele Syslog colectează jurnalele evenimentelor de securitate pentru a monitoriza încălcările de acces. Citare: Syslog Standard.

9 **Întrebarea 9**

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

OpenVPN și IPsec sunt protocoale actuale care criptează traficul clienților la distanță.

10 **Depășirea limitei cardului** BLOCAJ LA GATEWAY

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Blocajul lățimii de bandă la gateway apare atunci când traficul utilizatorilor depășește limitele serverului. Citare: Capacity Planning.

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. MULTIFACTOR	D 2. OPENVPN	E 3. POSTURĂ	B 4. SYSLOG
C 5. LĂȚIME DE BANDĂ	G 6. CRIPTARE	A 7. TUNELARE	F 8. FIREWALL

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 MULTIFACTOR	2 OPENVPN	3 POSTURĂ	4 SYSLOG
5 LĂȚIME DE BANDĂ	6 TUNELARE		

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

1 D – SYSLOG	2 H – FIREWALL	3 G – TUNELARE	4 F – CRIPTARE
5 B – OPENVPN	6 E – LĂȚIMEDEBANDĂ	7 C – POSTURĂ	8 A – MULTIFACTOR

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica MULTIFACTOR, OPENVPN și POSTURĂ 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.

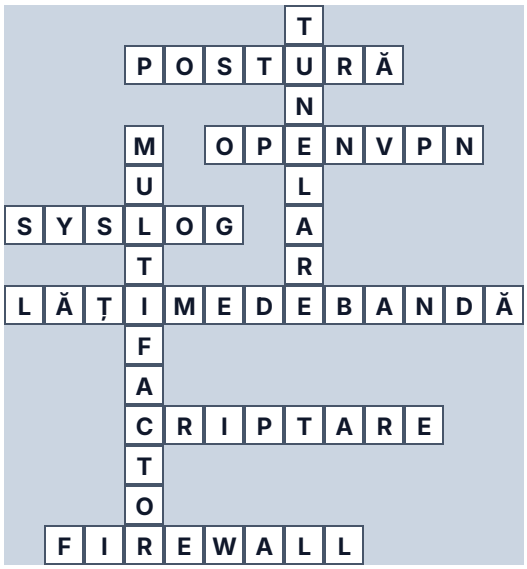
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

2 orizontal: POSTURĂ Validarea stării de sănătate a dispozitivului de la distanță (7 litere)

4 orizontal: OPENVPN Protocol standard client-la-site (7 litere)

5 orizontal: SYSLOG Colector central al jurnalelor de securitate (6 litere)

6 orizontal: LĂȚIMEDEBANDĂ Limita capacității de date a rețelei (13 litere)

7 orizontal: CRIPTARE Codificarea criptografică a pachetelor (8 litere)

8 orizontal: FIREWALL Reguli ale sistemului de filtrare a traficului (8 litere)

VERTICAL

1 vertical: TUNELARE Încapsularea datelor într-o cale securizată (8 litere)

3 vertical: MULTIFACTOR Securitate la autentificare care cere token-uri suplimentare (11 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. I A O U F C M T L R T — **MULTIFACTOR**
2. P S Ă R U T O — **POSTURĂ**
3. Ă L E A B D Ă Ț D M E N I — **LĂȚIMEDEBANDĂ**
4. E R E A L T U N — **TUNELARE**
5. V N N E O P P — **OPENVPN**
6. O L S S G Y — **SYSLOG**
7. C E T A R R P I — **CRIPTARE**
8. E I W L F L A R — **FIREWALL**

BAREMUL PROVOCĂRII CU CODUL SECRET

"VPN DE ACCES LA DISTANȚĂ PROTEJEAZĂ REȚEAUA"

Barem pentru studiile de caz

A Studiu de caz 1: Impunerea MFA

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un analist de afaceri încearcă să se autentifice în baza de date corporativă în timp ce lucrează de la distanță. Introduce corect numele de utilizator și parola, dar portalul VPN blochează accesul și cere un cod de la un token fizic.
- Strategie și soluție recomandată: Portalul VPN corporativ impune o politică strictă de autentificare multifactor (MFA) pentru a securiza conectările la distanță.

B Studiu de caz 2: Conformitatea posturii dispozitivului

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un colaborator extern își conectează laptopul personal la rețeaua corporativă de la distanță. Clientul VPN întrerupe imediat conexiunea, anunțând utilizatorul că definițiile sale antivirus sunt învechite.
- Strategie și soluție recomandată: Gateway-ul de acces la distanță a efectuat o verificare a posturii de securitate a punctului final și a blocat dispozitivul din cauza configurațiilor de securitate învechite.