Nume: _____ Data: _____ Punctaj: _____

VPN pentru întreprinderi

Implementarea accesului la rețea Zero Trust, a nodurilor gateway dedicate și a controalelor administrative corporative centralizate.

PREZENTARE GENERALĂ A REȚELELOR VPN DE ÎNTREPRINDERE

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 rețele VPN pentru companii. Vei explora arhitecturile Zero Trust, gateway-urile IP statice dedicate, consolele de administrare, provizionarea și tunelurile IPsec site-la-site.

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/enterprise/

Harta ta de învățare despre rețelele VPN pentru companii

- Implementează cadre Zero Trust Network Access (ZTNA).
- Configurează adrese IP dedicate de gateway ale serverului pentru filtrele de listă albă.
- Gestionează panourile de administrare centralizate ale companiei și listele de licențe ale utilizatorilor.
- Auditează jurnalele de acces la rețea și istoricul conexiunilor utilizatorilor.
- Configurează regulile pentru Single Sign-On (SSO) și autentificarea multifactor.
- Configurează tuneluri IPsec site-to-site între sucursale.

INSTRUCȚIUNI PENTRU REȚELE VPN DE ÎNTREPRINDERE

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 Zero Trust și IPsec de tip site-to-site. Încheie cu activitatea bonus Gândește repede.

ARHITECTURI ZERO TRUST ȘI GATEWAY-URI DEDICATE (INTRODUCERE)

VPN-urile pentru întreprinderi securizează activele corporative prin trecerea la cadre Zero Trust Network Access (ZTNA) și prin includerea pe lista albă a gateway-urilor IP statice dedicate. Managerii IT folosesc console de administrare centralizate pentru a orchestra tuneluri IPsec site-to-site și link-uri single sign-on (SSO).

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

Punct de control 1: Provocare cu alegere multiplă

1. **1. Ce model de securitate înlocuiește VPN-urile corporative vechi?**
   - A) Zero Trust
   - B) Multi-hop
   - C) Peer-to-peer
   - D) Un singur gateway

2. **2. Ce funcție este necesară pentru a restricționa accesul la baza de date doar la serverele companiei?**
   - A) IP dedicat
   - B) Rutare dinamică
   - C) Split tunnel
   - D) Proxy DNS

3. **3. Ce protocol este standardul pentru tunelurile corporative de tip site-to-site?**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **4. Ce instrument central le permite administratorilor să gestioneze licențele angajaților?**
   - A) Consolă de administrare
   - B) Cheie de registru
   - C) Firmware-ul routerului
   - D) Jurnalul de sistem

5. **5. Ce standard de autentificare permite conectarea prin Okta sau Microsoft Entra ID?**
   - A) Single Sign-On
   - B) Secret partajat
   - C) Autentificare EPP
   - D) Cheie WEP

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Zero Trust Network Access acordă accesul la rețea doar după verificarea continuă a încrederii în dispozitiv.

- ○ Adevărat
- ○ Fals

7 Întrebare 7

7. Gateway-urile cu IP dedicat direcționează traficul angajaților laolaltă cu cel al unor utilizatori publici aleatorii.

- ○ Adevărat
- ○ Fals

8 Întrebare 8

8. Consolele administrative centralizate permit managerilor IT să revoce instantaneu locurile individuale ale angajaților.

- ○ Adevărat
- ○ Fals

9 Întrebare 9

9. IPsec este un protocol ușor care nu acceptă tuneluri de rețea site-to-site.

- ○ Adevărat
- ○ Fals

10 Întrebare 10

10. Single Sign-On permite autentificarea sigură a angajaților prin furnizori de identitate corporativi.

- ○ 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. Arhitecturile de securitate moderne înlocuiesc tunelurile vechi cu accesul de tip _____ .

2. Pentru a restricționa accesul la baza de date, companiile configurează o adresă de gateway de tip _____ .

3. Sucursalele sunt conectate securizat prin tuneluri site-to-site _____ .

4. Administratorii IT alocă licențele angajaților din interfața centrală, numită _____ .

5. Integrarea Okta permite angajaților să se autentifice prin sistemul corporativ de tip _____ .

6. Pentru a proteja autentificările, portalurile enterprise impun autentificare _____ .

BANCĂ DE CUVINTE DIN VOCABULAR

CONSOLĂ ADMIN | GATEWAY | IP DEDICAT | IPSEC | MULTIFACTOR | PROVIZIONARE | SINGLE SIGN-ON | ZERO TRUST

Scrie răspunsurile aici:

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

Punct de control 4: Asocierea conceptelor-cheie

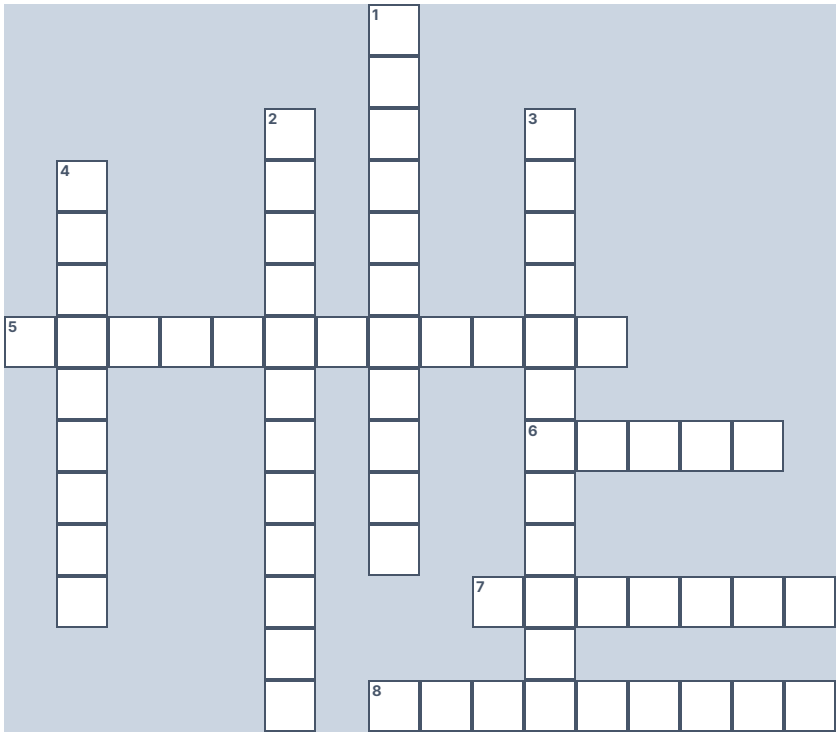
ASOCIEREA DEFINIȚIILOR

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

☐	1. ZERO TRUST	A	Alocarea licențelor de acces VPN pentru angajați.
☐	2. IP DEDICAT	B	Legătura de identitate cu Okta și Entra ID.
☐	3. IPSEC	C	Securitate la autentificare care necesită token-uri suplimentare.
☐	4. CONSOLĂ DE ADMINISTRARE	D	Adresa gateway-ului din lista albă statică.
☐	5. AUTENTIFICARE UNICĂ	E	Standard pentru tuneluri site-to-site.
☐	6. MULTIFACTOR	F	Nod de rutare pentru intrarea în rețea.
☐	7. GATEWAY	G	Portal central pentru locurile gestionate de managerul IT.
☐	8. PROVIZIONARE	H	Cadru de verificare continuă a încrederii.

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

5. Portal central pentru managerii IT, de unde se administrează locurile (12)

6. Standard pentru tuneluri site-to-site (5)

7. Nod de rutare care servește drept intrare în rețea (7)

8. Adresă statică de gateway pentru lista albă (9)

VERTICAL

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

2. Legătură de identitate cu Okta și Entra ID (12)

3. Alocarea licențelor de acces VPN pentru angajați (12)

4. Cadru de verificare continuă a încrederii (9)

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

5 orizontal: Portal central pentru managerii IT, de unde se administrează locurile (12 litere):

6 orizontal: Standard pentru tuneluri site-to-site (5 litere):

7 orizontal: Nod de rutare care servește drept intrare în rețea (7 litere):

8 orizontal: Adresă statică de gateway pentru lista albă (9 litere):

VERTICAL

1 vertical: Securitate la autentificare care cere token-uri suplimentare (11 litere):

2 vertical: Legătură de identitate cu Okta și Entra ID (12 litere):

3 vertical: Alocarea licențelor de acces VPN pentru angajați (12 litere):

4 vertical: Cadru de verificare continuă a încrederii (9 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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

ZEROTRUST IPDEDICAT IPSEC CONSOLĂADMIN SINGLESIGNON
MULTIFACTOR GATEWAY PROVIZIONARE

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. IPDEDICAT
C. IPSEC
D. CONSOLĂADMIN
E. SINGLESIGNON
F. MULTIFACTOR
G. GATEWAY
H. PROVIZIONARE

DEFINIȚII ȘI CÂMPURI DE ASOCIERE
1. Adresă statică de gateway pentru lista albă.
2. Nod de rutare care servește drept intrare în rețea.
3. Alocarea licențelor de acces VPN pentru angajați.
4. Securitate la autentificare care cere token-uri suplimentare.
5. Standard pentru tuneluri site-to-site.
6. Cadru de verificare continuă a încrederii.
7. Legătură de identitate cu Okta și Entra ID.
8. Portal central pentru managerii IT, de unde se administrează locurile.

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. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. YAWEAGT
5. CDPTIEIAD
6. NODMLIACOĂNS
7. CIMUARTOLFT
8. OOIAIEPZRRNV

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

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

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: MIGRAREA LA ZERO TRUST



Scenariu: O companie vrea să-și securizeze serverele locale verificând continuu certificatele de conformitate ale dispozitivelor, starea firewall-ului și locația utilizatorului, în loc să aibă încredere în oricine se află în interiorul rețelei.

Întrebare de discuție: Ce cadru ar trebui să implementeze directorul de securitate IT pentru a realiza acest lucru?

STUDIU DE CAZ 2: RESTRICȚIA GATEWAY



Scenariu: O companie găzduiește baze de date financiare private în cloud. Vrea să blocheze orice acces public din internet la panourile de administrare, permițând autentificarea numai de pe punctele terminale verificate ale companiei.

Întrebare de discuție: Ce configurare de rețea ar trebui să stabilească administratorul bazei de date pe firewall-ul din cloud?

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		27	7	21	11	8	11	5	2
8	11	7	5	1	21	7		6	11	22	19	18	31	11	24	11	27	
				6	11	17		21	7	25	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 un VPN pentru întreprinderi?

Un tunel de rețea securizat conceput pentru companii, care permite lucrătorilor la distanță să acceseze rețelele companiei cu administrare centralizată.

Q2: Prin ce diferă Zero Trust de VPN-urile tradiționale?

VPN-urile tradiționale au încredere în oricine se află în tunel, în timp ce Zero Trust verifică continuu fiecare dispozitiv și fiecare conexiune de utilizator.

Q3: Ce este o adresă IP dedicată în VPN-urile pentru companii?

O adresă IP statică rezervată exclusiv afacerii tale, care îți permite să o pui pe lista albă pentru accesul securizat la bazele de date din cloud.

Q4: De ce este important SSO pentru VPN-urile de business?

Single Sign-On permite angajaților să folosească datele de autentificare corporative (precum Okta sau Microsoft Entra ID) pentru a se conecta în siguranță.

Q5: Ce este un VPN site-la-site?

Un tunel care conectează două birouri fizice (precum o sucursală și sediul central) prin internetul public folosind IPsec.

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 este funcția unei console de administrare?

Un panou de control pentru administratorii IT, pentru a adăuga sau elimina locurile angajaților, a atribui gateway-uri și a monitoriza conexiunile active.

Q7: Cum securizează MFA VPN-urile de business?

Prin solicitarea unui cod secundar (precum un token dintr-o aplicație de autentificare) pentru a preveni accesul neautorizat cu parole compromise.

Q8: Pot audita istoricul conexiunilor angajaților?

Da, VPN-urile pentru companii înregistrează marcajele de timp ale conexiunii, durata și adresele IP atribuite, pentru auditul de conformitate.

Q9: Ce este ZTNA?

Zero Trust Network Access, un model de securitate care acordă acces doar la anumite aplicații, nu la întreaga rețea.

Q10: Care este rolul nodurilor gateway?

Servesc drept puncte sigure de intrare pentru traficul de la distanță, direcționând datele direct către serverele corporative private.

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 protejează IPsec comunicațiile corporative de tip site-to-site?

IPsec criptează traficul la nivelul rețelei, folosind Encapsulating Security Payload (ESP), pentru a asigura confidențialitatea și integritatea datelor.

Q2: De ce eșuează securitatea clasică bazată pe perimetru în cazul angajaților la distanță?

Deoarece angajații accesează datele din mai multe locații și de pe mai multe dispozitive, perimetrul unui singur firewall de rețea devine depășit.

Q3: Cum implementează managerii IT aprovizionarea automată?

Prin maparea protocoalelor SCIM între furnizorii de identitate (Okta) și consola de administrare VPN pentru a sincroniza directoarele de utilizatori.

Q4: Care este beneficiul split tunneling în mediile corporative?

Direcționează traficul SaaS local (precum Microsoft 365) în afara tunelului VPN, păstrând lățimea de bandă a gateway-ului corporativ pentru bazele de date private.

Q5: Cum validează verificările de postură a dispozitivului securitatea endpoint-urilor?

Clientul VPN scanează dispozitivul înainte de conectare pentru a verifica dacă firewall-ul este activ, antivirusul rulează, iar patch-urile sistemului de operare sunt la zi.

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 rolul traversării NAT în configurațiile VPN pentru business?

NAT-T încapsulează pachetele IPsec în UDP pentru a le permite să treacă prin routerele și firewall-urile de acasă fără întreruperi ale conexiunii.

Q7: Cum previn companiile blocajele de lățime de bandă ale gateway-ului?

Prin implementarea mai multor noduri gateway regionale și echilibrarea traficului utilizatorilor de intrare între ele cu ajutorul load balancerelor.

Q8: De ce sunt preferate listele albe de IP-uri statice în locul celor dinamice?

Listele albe statice împiedică IP-urile externe neautorizate să încerce handshake-uri de conectare, reducând dramatic suprafața de atac.

Q9: Care este rolul autentificării pe bază de certificate în VPN-urile enterprise?

Validează certificate digitale unice instalate pe dispozitivele gestionate de companie, blocând computerele personale negestionate.

Q10: Cum reduce ZTNA riscul mișcării laterale?

Prin izolarea sesiunilor utilizatorilor la resurse autorizate specifice, împiedicând hackerii să se deplaseze prin rețea dacă un nod este compromis.

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

Arhitecturile Zero Trust verifică în mod continuu starea de securitate a fiecărui dispozitiv care încearcă o conexiune la rețea.

2. INFORMAȚII DESPRE VPN

Gateway-urile cu IP dedicat le permit companiilor să blocheze accesul la bazele de date din cloud prin includerea pe lista albă a adreselor statice.

3. INFORMAȚII DESPRE VPN

IPsec este protocolul standard din industrie pentru configurarea tunelurilor securizate de rețea site-to-site între birouri.

4. INFORMAȚII DESPRE VPN

Consolele de administrare permit departamentelor IT să aloce, să gestioneze și să audite locurile de acces VPN ale angajaților.

5. INFORMAȚII DESPRE VPN

Single Sign-On integrează accesul VPN cu furnizori de identitate corporativi precum Okta și Entra ID.

6. INFORMAȚII DESPRE VPN

Autentificarea multifactor blochează încercările de conectare neautorizate care provin din chei de parolă furate.

7. PERSPECTIVĂ ASUPRA VPN-URILOR

Split tunneling optimizează lățimea de bandă corporativă excluzând traficul SaaS public din tunelul criptat.

8. PERSPECTIVĂ ASUPRA VPN-URILOR

Verificările posturii dispozitivului confirmă setările locale de securitate înainte de acordarea accesului la serverele corporative.

9. PERSPECTIVĂ ASUPRA VPN-URILOR

Sincronizarea directoarelor SCIM automatizează controalele de acces la integrarea și plecarea angajaților.

10. INFORMAȚII DESPRE VPN

Zero Trust Network Access limitează accesul utilizatorilor la anumite aplicații autorizate, împiedicând mișcarea laterală în rețea.

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 **Zero Trust** MODEL ZTNA **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Modelele Zero Trust verifică în mod continuu conformitatea dispozitivului înainte de intrarea în rețea. Citare: NIST Zero Trust.

2 **IP dedicat** IP STATIC **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Adresele IP dedicate permit includerea gateway-urilor pe lista albă pentru a bloca traficul public. Citare: Dedicated IP Guide.

3 **Standardul IPsec** TUNEL IPSEC **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

IPsec este protocolul standard folosit pentru tunelurile site-to-site între sucursale. Citare: IPsec Tunneling.

4 **Alocare IT** CONSOLĂ DE ADMINISTRARE **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Panourile administrative centralizate permit managerilor IT să aloce licențe pe locuri. Citare: CISA Guidelines.

5 **Întrebarea 5** **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce standard de autentificare permite conectarea prin Okta sau Microsoft Entra ID? → Single Sign-On

Barem: Punct de control 2 – Adevărat sau fals

6 **Zero Trust** VERIFICĂRI ZTNA Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Modelele Zero Trust verifică în mod continuu conformitatea dispozitivului înainte de intrarea în rețea. Citare: NIST Zero Trust.

7 **Întrebarea 7** Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

IP-urile dedicate sunt rezervate unei singure companii, astfel încât traficul ei nu este amestecat cu al altor utilizatori.

8 **Alocare IT** LOC DE ADMINISTRATOR IT Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Panourile administrative centralizate permit managerilor IT să aloce licențe pe locuri. Citare: CISA Guidelines.

9 **Standardul IPsec** SITE-LA-SITE Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

IPsec este protocolul standard folosit pentru tunelurile site-to-site între sucursale. Citare: IPsec Tunneling.

10 **Link Okta SSO** AUTENTIFICARE SSO Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Single Sign-On integrează autentificările VPN cu directoare corporative precum Okta. Citare: Okta SSO.

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. ZERO TRUST	D 2. IP DEDICAT	E 3. IPSEC	G 4. CONSOLĂ DE ADMINISTRARE
B 5. AUTENTIFICARE UNICĂ	C 6. MULTIFACTOR	F 7. GATEWAY	A 8. PROVIZIONARE

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 ZERO TRUST	2 IP DEDICAT	3 IPSEC	4 CONSOLĂ ADMIN
5 SINGLE SIGN-ON	6 MULTIFACTOR		

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

1 B – IPDEDICAT	2 G – GATEWAY	3 H – PROVIZIONARE	4 F – MULTIFACTOR
5 C – IPSEC	6 A – ZEROTRUST	7 E – SINGLESIGNON	8 D – CONSOLĂADMIN

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica ZERO TRUST, IP DEDICAT și IPSEC 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.

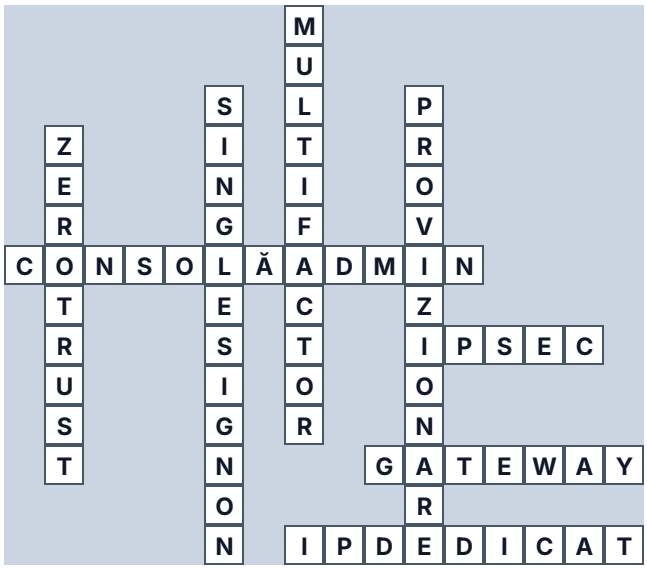
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

5 orizontal: CONSOLĂADMIN Portal central pentru managerii IT, de unde se administrează locurile (12 litere)

6 orizontal: IPSEC Standard pentru tuneluri site-to-site (5 litere)

7 orizontal: GATEWAY Nod de rutare care servește drept intrare în rețea (7 litere)

8 orizontal: IPDEDICAT Adresă statică de gateway pentru lista albă (9 litere)

VERTICAL

1 vertical: MULTIFACTOR Securitate la autentificare care cere token-uri suplimentare (11 litere)

2 vertical: SINGLESIGNON Legătură de identitate cu Okta și Entra ID (12 litere)

3 vertical: PROVIZIONARE Alocarea licențelor de acces VPN pentru angajați (12 litere)

4 vertical: ZEROTRUST Cadru de verificare continuă a încrederii (9 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. ICESP — **IPSEC**
3. SIISOGNENLNG — **SINGLESIGNON**
4. YAWEAGT — **GATEWAY**
5. CDPTIEIAD — **IPDEDICAT**
6. NODMLIACOĂNS — **CONSOLĂADMIN**
7. CIMUARTOLFT — **MULTIFACTOR**
8. OOIAIEPZRRNV — **PROVIZIONARE**

BAREMUL PROVOCĂRII CU CODUL SECRET

"ZERO TRUST VERIFICĂ FIECARE DISPOZITIV DIN REȚEA"

Barem pentru studiile de caz

A Studiu de caz 1: Migrarea la Zero Trust

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O companie dorește să-și securizeze serverele locale verificând continuu certificatele de conformitate ale dispozitivelor, starea firewall-ului și locația utilizatorului, în loc să aibă încredere în oricine se află în interiorul rețelei.
- Strategie și soluție recomandată: Directorul ar trebui să migreze la un model Zero Trust Network Access (ZTNA), care impune verificări de securitate continue, bazate pe context.

B Studiu de caz 2: Restricția gateway

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O companie găzduiește în cloud baze de date financiare private. Vrea să blocheze tot accesul public de pe internet la panourile de administrare, permițând autentificarea doar de pe punctele finale verificate ale companiei.
- Strategie și soluție recomandată: Administratorul ar trebui să configureze un gateway cu IP dedicat pe VPN-ul enterprise și să adauge această adresă statică pe lista albă a firewall-ului bazei de date din cloud.