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

WireGuard vs OpenVPN Fișă de lucru

Compararea protocoalelor WireGuard și OpenVPN, a dimensiunilor bazelor de cod, a vitezei și a standardelor criptografice

PREZENTARE GENERALĂ DE ÎNVĂȚARE DESPRE VPN

CURSANT
STATUT DE STUDENT
Parcursul apărătorului de rețea

SIGUR
STAREA CONEXIUNII
Protejarea pachetelor de date

ACTIV
PROTECȚIE LA SCURGERI
Protecție împotriva scurgerilor DNS și IPv6

Bun venit! Acest pachet de activități te ghidează prin principiile fundamentale ale rețelelor private virtuale (VPN). Vei explora modul în care tunelurile criptate îți securizează datele, modul în care funcționează protocoalele de rețea și modul în care poți identifica și reduce scurgerile de confidențialitate.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește conceptele și protocoalele VPN.**
- [ ] **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 despre VPN

URL: https://www.vpn.com/ro/vpn/

Harta ta de învățare despre VPN

- Compară complexitatea bazei de cod și viteza de audit a protocoalelor.
- Analizează câștigurile de performanță ale rulării în spațiul nucleului.
- Compară cifrurile OpenSSL cu criptografia modernă WireGuard.
- Configurează perechi de chei publice și private pentru handshake-urile dintre peeri.
- Direcționează traficul VPN prin porturile firewall TCP și UDP.

INSTRUCȚIUNI PENTRU FIȘA DE COMPARARE A PROTOCOALELOR

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 auditarea protocoalelor moderne. Încheie cu activitatea bonus Gândește repede.

WIREGUARD VS OPENVPN (INTRODUCERE)

Alegerea unui protocol VPN presupune echilibrarea vitezei cu opțiunile de configurare. OpenVPN este standardul de zeci de ani și oferă flexibilitate de configurare TCP/UDP. WireGuard este un înlocuitor modern care rulează direct în spațiul kernelului, cu doar 4.000 de linii de cod. Înțelegerea diferențelor dintre protocoale este esențială pentru optimizarea rețelelor tale securizate.

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

Punct de control 1: Provocare cu alegere multiplă

1. Care este dimensiunea aproximativă a bazei de cod a protocolului WireGuard?

- A. Aproximativ 70.000 de linii
- B. Peste 100.000 de linii
- C. Mai puțin de 1.000 de linii
- D. Aproximativ 4.000 de linii

2. În ce spațiu al sistemului de operare rulează WireGuard?

- A. Spațiul utilizatorului
- B. Spațiul kernelului
- C. Spațiul aplicației
- D. Spațiu virtual

3. Pe ce bibliotecă criptografică se bazează în principal OpenVPN?

- A. ChaCha20-Poly1305
- B. Biblioteca criptografică OpenSSL
- C. Cadrul de protocol Noise
- D. Codificare DES în text simplu

4. Care este un avantaj cheie de performanță al WireGuard față de OpenVPN?

- A. Handshake-uri de conectare mai rapide și latență mai mică
- B. Evitarea necesității adreselor IP publice
- C. Suport nativ încorporat pentru dial-up vechi
- D. Consum zero de baterie pe dispozitivele mobile

5. Cum autentifică WireGuard conexiunile peer?

- A. Prin schimbul de parole obișnuite ale utilizatorilor
- B. Prin verificarea certificatelor de înregistrare a domeniului
- C. Prin folosirea unor perechi statice de chei publice și private
- D. Verificând numerele de serie ale hardware-ului

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Baza de cod compactă a WireGuard o face semnificativ mai ușor de auditat.

○ Adevărat ○ Fals

7 Întrebare 7

7. OpenVPN este, în general, mai rapid decât WireGuard deoarece rulează în spațiul nucleului.

○ Adevărat ○ Fals

8 Întrebare 8

8. OpenVPN este foarte configurabil și acceptă atât protocolul UDP, cât și TCP.

○ Adevărat ○ Fals

9 Întrebare 9

9. WireGuard folosește criptografie modernă, precum ChaCha20, pentru criptarea rapidă a pachetelor.

○ Adevărat ○ Fals

10 Întrebare 10

10. WireGuard necesită configurări complexe de autoritate de certificare pentru autentificare.

○ 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. Protocolul modern _____ funcționează direct în nucleul sistemului de operare.
2. Protocolul vechi _____ se bazează pe biblioteca criptografică OpenSSL.
3. Executarea codului în _____ reduce suprasarcina schimbării contextului.
4. OpenVPN rulează în _____ , dirijând pachetele prin interfețe virtuale.
5. WireGuard folosește o _____ (publică și privată) pentru a identifica partenerii de conexiune.
6. Dimensiunea mică a codului sursă sporește gradul de _____ al software-ului.

BANCĂ DE CUVINTE DIN VOCABULAR

AUDITABILITATE | COD COMPACT | OPENSSL | OPENVPN | PERECHE DE CHEI | SPAȚIU KERNEL | SPAȚIU USER | WIREGUARD

Scrie răspunsurile aici:

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

Punct de control 4: Asocierea conceptelor despre rețele

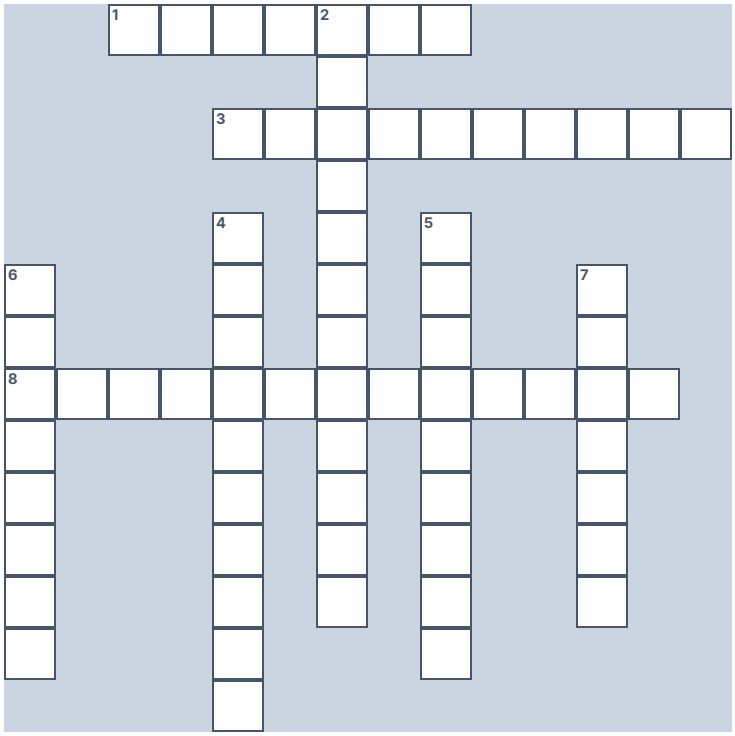
ASOCIEREA DEFINIȚIILOR

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

☐	1. WireGuard	A	Zona de execuție în care rulează OpenVPN, creând o supraîncărcare de comutare a contextului.
☐	2. OpenVPN	B	Dimensiunea compactă a codului sursă WireGuard, care îl face mult mai ușor de auditat.
☐	3. Spațiul kernelului	C	Biblioteca criptografică pe care se bazează OpenVPN pentru algoritmii de cifrare.
☐	4. Spațiul utilizatorului	D	Protocoale de transport pe care le acceptă OpenVPN; WireGuard în sine rulează doar peste UDP.
☐	5. 4.000 DE LINII	E	Zona din sistemul de operare în care rulează WireGuard pentru viteză.
☐	6. OpenSSL	F	Token-uri asimetrice folosite de WireGuard pentru a verifica conexiunile dintre peer-uri.
☐	7. Pereche de chei	G	Protocol VPN modern, conceput pentru viteză mare și auditare simplă a codului.
☐	8. TCP/UDP	H	Protocol robust, mai vechi, care folosește un cod de configurare mare și complex.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

1. Bibliotecă criptografică pe care OpenVPN se bazează pentru algoritmii de cifrare (7)

3. Zona de execuție în care rulează OpenVPN, ceea ce creează suprasarcină de schimbare a contextului (10)

8. Token-uri asimetrice folosite de WireGuard pentru a verifica partenerii de conexiune (13)

VERTICAL

2. Zona de execuție a sistemului de operare în care rulează WireGuard pentru viteză (12)

4. Dimensiunea redusă a bazei de cod WireGuard, care o face mult mai ușor de auditat (10)

5. Protocol VPN modern, conceput pentru viteză mare și auditarea simplă a codului (9)

6. Protocoale de transport acceptate de OpenVPN; WireGuard însuși rulează doar peste UDP (8)

7. Protocol robust, mai vechi, cu o bază de cod mare și o configurare complexă (7)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

1 orizontal: Bibliotecă criptografică pe care OpenVPN se bazează pentru algoritmii de cifrare (7 litere):

3 orizontal: Zona de execuție în care rulează OpenVPN, ceea ce creează suprasarcină de schimbare a contextului (10 litere):

8 orizontal: Token-uri asimetrice folosite de WireGuard pentru a verifica partenerii de conexiune (13 litere):

VERTICAL

2 vertical: Zona de execuție a sistemului de operare în care rulează WireGuard pentru viteză (12 litere):

4 vertical: Dimensiunea redusă a bazei de cod WireGuard, care o face mult mai ușor de auditat (10 litere):

5 vertical: Protocol VPN modern, conceput pentru viteză mare și auditarea simplă a codului (9 litere):

6 vertical: Protocoale de transport acceptate de OpenVPN; WireGuard însuși rulează doar peste UDP (8 litere):

7 vertical: Protocol robust, mai vechi, cu o bază de cod mare și o configurare complexă (7 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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

WIREGUARD OPENVPN SPAȚIUKERNEL SPAȚIUUSER CODCOMPACT OPENSSL PERECHEDECHEI TCPȘIUDP

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. WIREGUARD**
- **B. OPENVPN**
- **C. SPAȚIUKERNEL**
- **D. SPAȚIUUSER**
- **E. CODCOMPACT**
- **F. OPENSSL**
- **G. PERECHEDECHEI**
- **H. TCPȘIUDP**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Bibliotecă criptografică pe care OpenVPN se bazează pentru algoritmii de cifrare.
2. Zona de execuție a sistemului de operare în care rulează WireGuard pentru viteză.
3. Protocol robust, mai vechi, cu o bază de cod mare și o configurare complexă.
4. Token-uri asimetrice folosite de WireGuard pentru a verifica partenerii de conexiune.
5. Protocoale de transport acceptate de OpenVPN; WireGuard însuși rulează doar peste UDP.
6. Dimensiunea redusă a bazei de cod WireGuard, care o face mult mai ușor de auditat.
7. Protocol VPN modern, conceput pentru viteză mare și auditarea simplă a codului.
8. Zona de execuție în care rulează OpenVPN, ceea ce creează suprasarcină de schimbare a contextului.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie despre VPN. Scrie răspunsurile în casetele completabile.

1. UGEIWARDR
2. LPIUSNEAERKȚ
3. CMCPOOTCAD
4. HEERDCIEHCPEE
5. VNNEOPP
6. EIȚUSSPURA
7. OSSLPNE
8. ȘCIPTDUP

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Motive pentru care ai alege WireGuard			
2	Promisiuni pe care le face un furnizor VPN bun			
3	Motive pentru care ai alege OpenVPN			
4	Motive pentru care ai folosi un VPN în călătorii			
5	Lucruri pe care le poate vedea furnizorul tău de internet			
6	Moduri de a recunoaște o rețea Wi-Fi falsă			
7	Mituri despre VPN-uri			
8	Locuri în care ai folosi un VPN			
9	Lucruri rapide din viața de zi cu zi			
10	Lucruri de care un VPN nu te poate proteja			
11	Lucruri care fac un cod mai ușor de verificat			
12	Lucruri pe care le poate ascunde un VPN			
13	Deosebiri dintre WireGuard și OpenVPN			
14	Cuvinte legate de confidențialitate			
15	Nume de criptări pe care le cunoști			

Punct de control 8: Studii de caz despre VPN

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

SARAH (STUDENTA DIN CAFENEA)

👩‍💻 „Salut! Sunt în Wi-Fi-ul cafenelei, iar aplicația mea VPN îmi permite să aleg între WireGuard și OpenVPN. Apelurile mele video se întrerup mereu când trec între rețeaua cafenelei și hotspot-ul telefonului. Ce protocol ar trebui să aleg și de ce ar gestiona mai bine această trecere?”

ALEX (STUDENT CĂLĂTOR)

👩‍💻 „Sunt în străinătate, într-o rețea de hotel care pare să blocheze cea mai mare parte a traficului VPN. WireGuard nu se conectează deloc, dar trebuie să accesez resursele școlii mele de acasă. Ce este probabil blocat și cum m-ar putea ajuta OpenVPN să trec de blocaj?”

Punct de control 9: Descifrează codul

Pentru a-ți finaliza instruirea privind auditarea protocoalelor, descifrează acest mesaj ascuns despre execuția în spațiul nucleului.

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

24	21	7	5	11		6	7		15	1		18	19	7	17	27	19	17		15	1

26	17		24	26	17	7	15		16	1	11		21	1	19	11	6

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 pe care le au potențialii clienți despre utilizarea rețelelor private virtuale.

Q1: Ce este un VPN și cum funcționează?

O rețea privată virtuală (VPN) îți criptează conexiunea la internet și îți direcționează traficul printr-un server securizat la distanță. Aceasta maschează adresa ta IP publică și limitează ce pot vedea observatorii din rețeaua locală și ISP-ul tău despre traficul direcționat prin tunelul VPN.

Q2: De ce contează protocoalele?

Protocolul stabilește cum își construiește VPN-ul tunelul, ce criptografie îți protejează datele și cât de repede se conectează și se reconectează. WireGuard și OpenVPN sunt cele două protocoale open-source oferite de majoritatea aplicațiilor VPN și fac compromisuri diferite între simplitate, viteză și configurabilitate.

Q3: Este unul dintre ele mai privat decât celălalt?

Niciun protocol nu te face anonim. Ambele criptează traficul din tunel cu cifruri puternice; confidențialitatea ta depinde în mare parte de ce înregistrează furnizorul VPN și de modul în care gestionează cheile, conturile și serverele.

Q4: Îmi va încetini un VPN viteza internetului?

Da, ușor. Procesul de criptare și distanța fizică față de serverul VPN adaugă latență și suprasarcină. Impactul variază în funcție de furnizor, protocol, distanța până la server, dispozitiv și condițiile de rețea.

Q5: Sunt ambele open source?

Da. Atât WireGuard, cât și ediția comunitară OpenVPN își publică codul sursă, astfel că cercetătorii independenți le pot analiza. Baza de cod redusă a WireGuard face o analiză completă mult mai rapidă.

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

Parcurge cele mai frecvente întrebări și răspunsuri pe care le au potențialii clienți despre utilizarea rețelelor private virtuale.

Q6: Care dintre ele este mai rapid?

WireGuard este de obicei mai rapid: rulează în nucleu, folosește criptarea suplă ChaCha20-Poly1305 și finalizează rapid handshake-urile. OpenVPN are mai multă suprasarcină, dar vitezele reale depind și de încărcarea serverului și de distanță.

Q7: Pot ambele să ruleze peste TCP și UDP?

Nu. OpenVPN poate rula peste UDP sau TCP, iar modul TCP ajută în rețelele care blochează UDP. WireGuard își trimite pachetele doar prin UDP, deci poate eșua în rețelele care permit doar TCP. [4]

Q8: Cum aleg cel mai bun VPN?

Caută politici no-logs auditate, protocoale puternice (WireGuard, OpenVPN), locații de server sigure, viteze mari, servere doar în RAM, o funcție kill switch și o jurisdicție din afara alianțelor de partajare a informațiilor (precum 5/9/14 Eyes).

Q9: Pot folosi WireGuard și OpenVPN pe telefon?

Da. WireGuard este multiplatformă, cu aplicații pentru Windows, macOS, Linux, iOS și Android, iar clienții OpenVPN există pentru aceleași sisteme. Majoritatea aplicațiilor VPN te lasă să alegi oricare dintre ele. [1]

Q10: De ce este WireGuard atât de mic?

WireGuard acceptă un singur set fix de cifruri moderne, în loc de multe opțiuni. Implementarea sa pentru Linux necesită sub 4.000 de linii de cod, ceea ce o face mai ușor de auditat decât bazele de cod VPN mai mari. [3]

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

Explorează aspecte tehnice și structurale ale rețelelor private virtuale și ale protocoalelor de tunelare securizată.

Q1: Care este diferența dintre WireGuard, OpenVPN și IKEv2?

WireGuard este un protocol modern și ușor (doar aproximativ 4.000 de linii de cod), care oferă viteze mari și timpi de conectare rapizi. OpenVPN este un protocol open-source foarte sigur și verificat în practică. IKEv2 este excelent pentru dispozitivele mobile datorită capacității sale de a se reconecta rapid la schimbarea rețelei.

Q2: Ce cifruri folosește WireGuard?

WireGuard folosește ChaCha20 cu Poly1305 pentru criptare, Curve25519 pentru schimbul de chei, BLAKE2s pentru hashing și framework-ul Noise pentru handshake. Nu există negociere de cifruri, astfel că utilizatorii nu pot alege o opțiune slabă. [2]

Q3: Ce cifruri și biblioteci poate folosi OpenVPN?

OpenVPN este strâns integrat cu biblioteca OpenSSL și folosește TLS pentru schimbul de chei. Administratorii pot alege cifruri pentru canalul de date, precum AES-256-GCM, ceea ce adaugă flexibilitate, dar și loc pentru setări slabe. [4]

Q4: Cum autentifică fiecare protocol partenerii de comunicare?

Partenerii WireGuard se identifică reciproc prin chei publice statice, la fel ca la schimbul de chei SSH, iar fiecare cheie corespunde unor IP-uri de tunel permise. OpenVPN se bazează de obicei pe o autoritate de certificare cu certificate X.509, adesea combinate cu un nume de utilizator și o parolă.

Q5: Cum ocolește ofuscarea blocările VPN?

Ofuscarea (sau „Stealth VPN") deghizează traficul VPN astfel încât să arate ca trafic HTTPS obișnuit (portul 443). Aceasta poate ajuta la ocolirea inspecției profunde a pachetelor (DPI) folosite de guverne sau de rețelele școlare/de birou pentru a bloca VPN-urile.

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

Explorează aspecte tehnice și structurale ale rețelelor private virtuale și ale protocoalelor de tunelare securizată.

Q6: Ce se întâmplă când trec de la Wi-Fi la rețeaua mobilă?

WireGuard este fără conexiune (connectionless): trimite pachete de la noua adresă, iar tunelul continuă după un handshake rapid. OpenVPN păstrează starea sesiunii, așa că o schimbare de rețea poate necesita o reconectare care durează puțin mai mult.

Q7: Cum funcționează confidențialitatea directă (Forward Secrecy / Perfect Forward Secrecy)?

PFS asigură generarea unei chei de criptare unice și temporare pentru fiecare sesiune în parte. Chiar dacă o cheie privată este compromisă în viitor, ea nu poate fi folosită pentru a decripta sesiunile trecute sau viitoare, deoarece acestea au folosit chei independente.

Q8: Este OpenVPN încă o alegere bună dacă WireGuard este mai rapid?

Da. OpenVPN este matur și larg utilizat, rulează prin TCP când UDP este blocat și acceptă configurări de întreprindere bazate pe certificate. Mulți furnizori oferă ambele protocoale, astfel încât utilizatorii pot comuta dacă unul este blocat sau lent.

Q9: Ce porturi folosesc?

Portul standard al OpenVPN este 1194, dar poate fi mutat pe orice port UDP sau TCP, inclusiv 443. WireGuard ascultă pe un port UDP stabilit în configurația sa; 51820 este portul folosit în exemplele sale oficiale.

Q10: Ce protocol este mai ușor de configurat manual?

WireGuard este de obicei mai simplu: generezi o pereche de chei, schimbi cheile publice și listezi IP-urile permise. OpenVPN necesită certificate, o CA și mai multe opțiuni, deși profilurile .ovpn le grupează într-un singur fișier.

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

Parcurge aceste fapte și informații valoroase din lumea reală despre istoria, piața și tehnologia VPN-urilor.

1. PRIMUL PROTOCOL VPN

PPTP (Point-to-Point Tunneling Protocol) a fost dezvoltat de un grup de furnizori care includea Microsoft și a fost publicat ca RFC 2637 în iulie 1999 pentru a susține VPN-urile de acces la distanță. [6]

2. DOUĂ TRANSPORTURI

OpenVPN își poate transporta tunelul prin UDP sau TCP, iar în modul TLS canalele sale de control și de date folosesc un singur port. [4]

3. REVOLUȚIA WIREGUARD

WireGuard are o bază de cod foarte simplificată, concepută pentru eficiență, ceea ce o face mai ușor de auditat pentru vulnerabilități de securitate decât protocoalele tradiționale. [3]

4. CRIPTOGRAFIA MODERNĂ

WireGuard combină ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 și HKDF în cadrul framework-ului de protocol Noise, fără opțiuni de cifru pe care utilizatorii să le poată alege greșit. [2]

5. OPENSSL ÎN OPENVPN

OpenVPN este strâns integrat cu biblioteca OpenSSL și își derivă din aceasta multe dintre capabilitățile criptografice, inclusiv TLS-ul folosit pentru schimbul de chei. [4]

6. INSPECȚIA PROFUNDĂ A PACHETELOR

Inspecția aprofundată a pachetelor (DPI) examinează conținutul pachetelor și tiparele de trafic, nu doar antetele, iar unele firewall-uri o folosesc pentru a detecta și a bloca protocoalele VPN obișnuite.

7. CHEI DE TIP SSH

Conexiunile WireGuard se stabilesc prin schimbul unor chei publice simple, la fel ca la schimbul de chei SSH, fără a fi nevoie de o autoritate de certificare. [1]

8. MULTIPLATFORMĂ

WireGuard a fost lansat mai întâi pentru nucleul Linux și este acum disponibil pentru Windows, macOS, BSD, iOS și Android, astfel că același protocol funcționează pe majoritatea dispozitivelor. [1]

9. FORWARD SECRECY

WireGuard repetă handshake-ul Noise_IK la fiecare câteva minute pentru a roti cheile simetrice de sesiune, oferind secretizare directă perfectă (perfect forward secrecy) chiar dacă o cheie pe termen lung se scurge ulterior. [2]

10. INTERFEȚE TUN/TAP

OpenVPN este conceput să funcționeze cu interfața de rețea virtuală TUN/TAP, disponibilă pe majoritatea platformelor, care transportă pachetele tunelului. [4]

Referințe tehnice și surse

Publicațiile citate, specificațiile criptografice și standardele oficiale ale documentelor utilizate în această fișă de lucru.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.

https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Barem: Compararea protocoalelor WireGuard și OpenVPN, a dimensiunilor codului sursă, a vitezei și a standardelor criptografice

1 **Dimensiunea codului WireGuard** PROTOCOALE — **Răspuns corect: D**

NOTĂ PENTRU PROFESOR

WireGuard este extrem de compact, rulând pe aproximativ 4.000 de linii de cod. Acest lucru menține suprafața de atac mică și face auditarea mai ușoară. Citat: WireGuard Project.

2 **Viteza din spațiul nucleului** LATENȚĂ — **Răspuns corect: B**

NOTĂ PENTRU PROFESOR

Prin execuția directă în spațiul kernelului, WireGuard evită suprasolicitarea cauzată de comutarea contextului, ceea ce permite un debit ridicat. Citare: WireGuard Project.

3 **Întrebarea 3** — **Răspuns corect: B**

NOTĂ PENTRU PROFESOR

OpenVPN este strâns integrat cu OpenSSL, care furnizează cifruri precum AES-GCM și îl face foarte configurabil, dar mai complex.

4 **Performanța protocolului** CONTROALELE RUTĂRII — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

WireGuard stabilește handshake-uri în milisecunde și răspunde instantaneu la roaming-ul de rețea (de exemplu, trecerea de la Wi-Fi la rețeaua celulară). Citat: Microsoft Native Gateway, Apple Support.

5 **Criptografie asimetrică** CONFIDENȚIALITATE — **Răspuns corect: C**

NOTĂ PENTRU PROFESOR

WireGuard folosește Cryptokey Routing, asociind cheile publice cu adresele IP de tunel permise, similar configurărilor SSH. Citat: WireGuard Project.

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Implementarea WireGuard pentru Linux are sub 4.000 de linii, așa că echipele de securitate o pot revizui mult mai rapid decât baze de cod VPN mult mai mari, precum OpenVPN.

7 Latența spațiului utilizatorului VITEZE

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

OpenVPN rulează în spațiul utilizatorului, trecând pachetele încoace și încolo prin interfața virtuală a nucleului, ceea ce adaugă o suprasarcină de comutare de context (cu excepția cazului în care se folosește descărcarea în nucleu, precum OpenVPN DCO). Citație: DD-WRT custom firmware.

8 Configurare OpenVPN RISCUL DE SNIFFING

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

OpenVPN poate rula peste TCP (pentru fiabilitate/ocolirea firewall-urilor) sau UDP (pentru viteză), fiind compatibil cu firewall-urile complexe de întreprindere. Citație: IETF Cryptographic Protocols.

9 Criptografie modernă FIREWALLURI

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

WireGuard renunță la cifrurile vechi în favoarea unor primitive moderne și sigure, precum ChaCha20 și Poly1305, care rulează rapid pe procesoarele mobile. Citat: WireGuard Project.

10 Simplificarea perechii de chei NO-LOGS

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

WireGuard nu folosește certificate sau ierarhii CA complexe; se bazează pe perechi simple de chei publice/private schimbate între parteneri (peers). Citat: WireGuard Project.

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

G 1. WireGuard	H 2. OpenVPN	E 3. Spațiul kernelului	A 4. Spațiul utilizatorului
B 5. 4.000 DE LINII	C 6. OpenSSL	F 7. Pereche de chei	D 8. TCP/UDP

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 WIREGUARD	2 OPENVPN	3 SPAȚIU KERNEL	4 SPAȚIU USER
5 PERECHE DE CHEI	6 AUDITABILITATE		

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

1 F – OPENSSL	2 C – SPAȚIUKERNEL	3 B – OPENVPN	4 G – PERECHEDECHEI
5 H – TCPȘIUDP	6 E – CODCOMPACT	7 A – WIREGUARD	8 D – SPAȚIUUSER

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica WireGuard, OpenVPN și Spațiul kernelului 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.

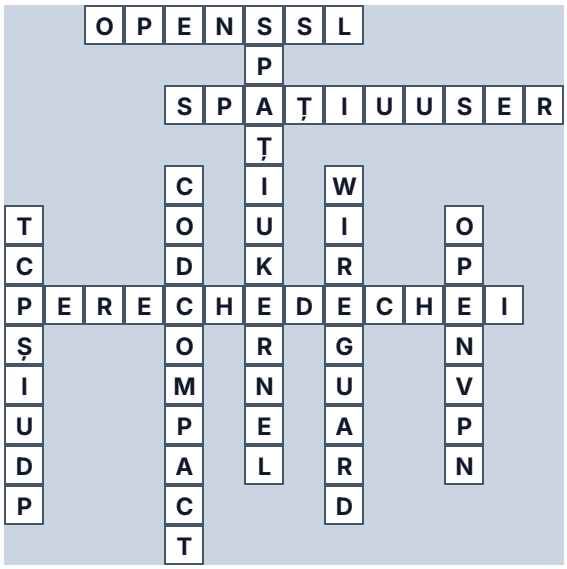
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

1 orizontal: OPENSSL Bibliotecă criptografică pe care OpenVPN se bazează pentru algoritmii de cifrare (7 litere)

3 orizontal: SPAȚIUUSER Zona de execuție în care rulează OpenVPN, ceea ce creează suprasarcină de schimbare a contextului (10 litere)

8 orizontal: PERECHEDECHEI Token-uri asimetrice folosite de WireGuard pentru a verifica partenerii de conexiune (13 litere)

VERTICAL

2 vertical: SPAȚIUKERNEL Zona de execuție a sistemului de operare în care rulează WireGuard pentru viteză (12 litere)

4 vertical: CODCOMPACT Dimensiunea redusă a bazei de cod WireGuard, care o face mult mai ușor de auditat (10 litere)

5 vertical: WIREGUARD Protocol VPN modern, conceput pentru viteză mare și auditarea simplă a codului (9 litere)

6 vertical: TCPȘIUDP Protocoale de transport acceptate de OpenVPN; WireGuard însuși rulează doar peste UDP (8 litere)

7 vertical: OPENVPN Protocol robust, mai vechi, cu o bază de cod mare și o configurare complexă (7 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. UGEIWARDR — **WIREGUARD**
2. LPIUSNEAERKȚ — **SPAȚIUKERNEL**
3. CMCPOOTCAD — **CODCOMPACT**
4. HEERDCIEHCPEE — **PERECHEDECHEI**
5. VNNEOPP — **OPENVPN**
6. EIȚUSSPURA — **SPAȚIUUSER**
7. OSSLPNE — **OPENSSL**
8. ȘCIPTDUP — **TCPȘIUDP**

BAREMUL PROVOCĂRII CU CODUL SECRET

"TRECI DE LA OPENVPN LA UN TUNEL MAI RAPID"

Barem pentru studiile de caz

A Scenariul A: alegerea unui protocol

SNIFFING ȘI CRIPTARE | Dilema Sarei

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Recomandare: WireGuard. Designul său ușor și fără conexiune permanentă permite tunelului să își revină rapid când se schimbă rețeaua ei, iar ChaCha20-Poly1305 menține criptarea rapidă.
- Securitate: Ambele protocoale îi criptează traficul pe Wi-Fi-ul din cafenea, deci oricare dintre ele îi protejează autentificările atunci când este configurat corect; alegerea influențează în principal viteza și stabilitatea.

B Scenariul B: Ocolirea blocărilor VPN

GEO-BLOCARE ȘI ADRESE IP | Dilema lui Alex

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- De ce este blocat: WireGuard folosește doar UDP, iar firewall-ul hotelului blochează probabil UDP sau recunoaște pachetele WireGuard prin filtrare sau inspecție profundă a pachetelor (DPI).
- Cum ajută OpenVPN: poate rula prin TCP, inclusiv pe portul 443 folosit de HTTPS, pe care firewall-urile din hoteluri îl blochează rar complet, deoarece navigarea web depinde de el.