Emri: _____ Data: _____ Pikët: _____

Si ta zgjedhësh një VPN
Fletë pune

Vlerësimi i ofruesve të VPN-ve, standardeve të sigurisë, auditimeve dhe politikave të regjistrimit

PËRMBLEDHJE E TË MËSUARIT PËR VPN-NË

NXËNËSI

STATUSI I STUDENTIT

Rruga e mbrojtësit të rrjetit

I SIGURT

STATUSI I LIDHJES

Mbrojtja e paketave të të dhënave

AKTIV

MBROJTJE NGA RRJEDHJET

Mbrojtje nga rrjedhjet e DNS dhe IPv6

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes parimeve themelore të Rrjeteve Private Virtuale (VPN). Do të eksplorosh si i sigurojnë të dhënat e tua tunelet e enkriptuara, si funksionojnë protokollet e rrjetit dhe si të identifikosh e të zbutësh rrjedhjet e privatësisë.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro konceptet dhe protokollet e VPN-së.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për VPN-në

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

Udhërrëfyesi yt mësimor për VPN-në

- Vlerëso juridiksionin e ofruesit dhe politikat zero-logs për privatësinë.
- Krahaso protokollet e tunelimit si WireGuard dhe OpenVPN për shpejtësi.
- Analizo veçori sigurie si kill switch-et dhe nyjet e serverëve vetëm me RAM.
- Identifiko auditimet e pavarura të sigurisë dhe planet e çmimeve kur zgjedh.
- Zgjidh vendndodhjet e serverëve sipas shpejtësisë dhe nevojave të tua për heqjen e bllokimeve gjeografike.

UDHËZIMET E FLETËS SË ZGJEDHJES

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për zgjedhjen e infrastrukturës së sigurt VPN. Përfundo me aktivitetin bonus Mendo shpejt.

ZGJEDHJA E NJË VPN (HYRJE)

Zgjedhja e VPN-së së duhur kërkon të shohësh përtej bujës së marketingut. Një ofrues i besueshëm duhet të ketë një politikë të provuar zero-logs, protokolle të sigurta enkriptimi dhe klientë me kod të hapur. Duke vlerësuar veçoritë e sigurisë, jurisdiksionet dhe performancën e shpejtësisë, mund të zgjedhësh një VPN që i përshtatet nevojave të mbrojtjes sate dixhitale.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Cili është faktori kyç kur zgjidhet një ofrues i sigurt VPN-je?

- A. Numri i vendeve me serverë
- B. Një politikë no-logs e audituar në mënyrë të pavarur
- C. Niveli më i ulët i çmimit mujor
- D. Sponsorizime të shkëlqyera reklamuese

2. Cili protokoll VPN ofron ekuilibrin më të mirë mes shpejtësisë dhe aditueshmërisë?

- A. PPTP (i vjetër)
- B. L2TP/IPSec
- C. Vetëm OpenVPN mbi TCP
- D. WireGuard

3. Pse duhet t'i shmangin përdoruesit VPN-të falas për veprimtari të ndjeshme?

- A. Janë të ndaluara në Shtetet e Bashkuara
- B. Shpesh e shesin historikun tënd të shfletimit të uebit
- C. Ata nuk mbështesin shfletimin bazë të uebit
- D. Kërkojnë harduer të veçantë për t'u lidhur

4. Çfarë përcakton jurisdiksioni ligjor i vendit të ofruesit?

- A. Shpejtësia e lidhjes me serverin
- B. Llojet e pajisjeve të mbështetura
- C. Ligjet vendase për ruajtjen e të dhënave dhe urdhrat e kontrollit
- D. Tema vizuale e aplikacionit të klientit

5. Cili është qëllimi kryesor i veçorisë "kill switch" të një klienti VPN?

- A. Për të bllokuar qasjen në internet nëse lidhja VPN bie
- B. Për të fshirë të gjitha aplikacionet e instaluara në pajisje
- C. Për të dyfishuar shpejtësinë e lidhjes me serverin
- D. Për të rindezur sistemin operativ kur është i papunë

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetja 6

6. Një VPN e mbron pajisjen tënde nga shkarkimet e malware-it dhe skedarët me viruse.

E vërtetë E gabuar

7 Pyetja 7

7. Auditimet e pavarura nga firma si Deloitte verifikojnë pretendimet për zero regjistrime.

E vërtetë E gabuar

8 Pyetja 8

8. Ligjet e vendit të origjinës së një ofruesi nuk ndikojnë në privatësinë e të dhënave të përdoruesit.

E vërtetë E gabuar

9 Pyetja 9

9. Baza e kodit kompakte e WireGuard është më e lehtë për t'u audituar se ajo e OpenVPN.

E vërtetë E gabuar

10 Pyetja 10

10. VPN-të falas shpesh shesin reklama ose gjurmojnë përdoruesit për të mbuluar kostot e serverëve.

E vërtetë E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Një politikë _____ e verifikuar në mënyrë të pavarur angazhon ofruesin e VPN-së të mos regjistrojë historikun tënd online.

2. Protokolli modern _____ ofron shpejtësi të lartë dhe përdor një bazë kodi shumë të vogël.

3. Një veçori sigurie e quajtur _____ ndalon të gjithë trafikun nëse lidhja VPN dështon papritur.

4. Vendi ligjor i regjistrimit të ofruesit quhet _____ dhe përcakton nëse ai i nënshtrohet traktateve të survejimit.

5. Përdorimi i _____ ndihmon që të dhënat e përdoruesve të mos mbeten pas rindezjes.

6. Verifikimi i një politike pretendimesh zero-knowledge kërkon një _____ sigurie nga palë të treta nga firma me reputacion.

BANKA E FJALËVE TË LEKSIKUT

AUDITIM JURIDIKSION KILL SWITCH OPENVPN PA REGJISTRA SERVERË RAM VPN FALAS WIREGUARD

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të rrjetit

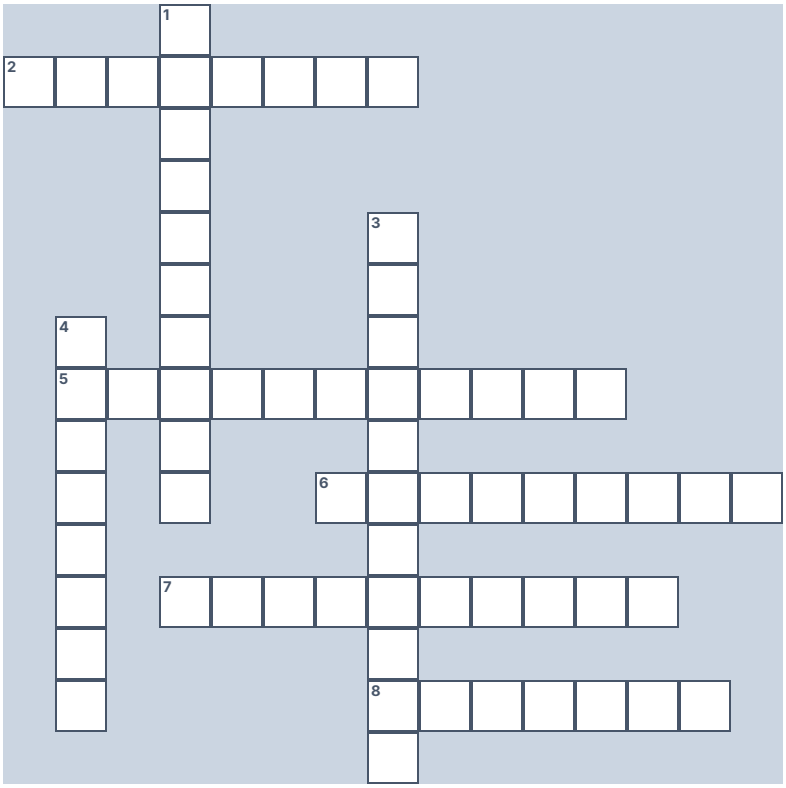
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. WireGuard	A	Shërbim lidhjeje me rrezik të lartë që shpesh monetizohet duke regjistruar dhe shitur të dhënat e shfletimit.
☐	2. Regjistra të audituar	B	Mekanizëm sigurie që bllokon rrugëzimin e internetit nëse tuneli i sigurt shkëputet.
☐	3. Juridiksioni	C	Aleancë ndërkombëtare e ndarjes së inteligjencës midis SHBA-së, MB-së, Kanadasë, Australisë dhe Zelandës së Re.
☐	4. Kill switch	D	Infrastrukturë hardueri që funksionon në memorie të paqëndrueshme, ndaj të dhënat nuk ruhen në disk.
☐	5. Five Eyes	E	Rajoni gjeografik që rregullon detyrimet ligjore të ofruesit të VPN-së.
☐	6. VPN falas	F	Protokoll modern dhe i shpejtë që përdor rreth 4,000 rreshta kodi shumë të audituesshëm.
☐	7. Serverë vetëm me RAM	G	Protokoll me kod të hapur i pjekur dhe i audituar gjerësisht, me bazë kodi shumë më të madhe se WireGuard.
☐	8. OpenVPN	H	Pretendim privatësie i verifikuar nga firma të pavarura të sigurisë kibernetike të palëve të treta.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

2. Aleancë ndërkombëtare e ndarjes së inteligjencës midis SHBA-së, MB-së, Kanadasë, Australisë dhe Zelandës së Re (8)

5. Pretendim privatësie i verifikuar nga firma të pavarura të sigurisë kibernetike të palëve të treta (11)

6. Protokoll modern dhe i shpejtë që përdor rreth 4,000 rreshta kodi shumë të auditueshëm (9)

7. Mekanizëm sigurie që bllokon rrugëzimin e internetit nëse tuneli i sigurt shkëputet (10)

8. Protokoll i pjekur me burim të hapur, i audituar gjerësisht, me një bazë kodi shumë më të madhe se WireGuard (7)

VERTIKALISHT

1. Infrastrukturë harduerike që funksionon tërësisht në memorie të paqëndrueshme, duke parandaluar ruajtjen e të dhënave (10)

3. Rajoni gjeografik që rregullon detyrimet ligjore të ofruesit të VPN-së (11)

4. Shërbim lidhjeje me rrezik të lartë që shpesh fiton para duke regjistruar dhe shitur të dhënat e shfletimit (8)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

2 horizontalisht: Aleancë ndërkombëtare e ndarjes së inteligjencës midis SHBA-së, MB-së, Kanadasë, Australisë dhe Zelandës së Re (8 shkronja):

5 horizontalisht: Pretendim privatësie i verifikuar nga firma të pavarura të sigurisë kibernetike të palëve të treta (11 shkronja):

6 horizontalisht: Protokoll modern dhe i shpejtë që përdor rreth 4,000 rreshta kodi shumë të auditueshëm (9 shkronja):

7 horizontalisht: Mekanizëm sigurie që bllokon rrugëzimin e internetit nëse tuneli i sigurt shkëputet (10 shkronja):

8 horizontalisht: Protokoll i pjekur me burim të hapur, i audituar gjerësisht, me një bazë kodi shumë më të madhe se WireGuard (7 shkronja):

VERTIKALISHT

1 vertikalisht: Infrastrukturë harduerike që funksionon tërësisht në memorie të paqëndrueshme, duke parandaluar ruajtjen e të dhënave (10 shkronja):

3 vertikalisht: Rajoni gjeografik që rregullon detyrimet ligjore të ofruesit të VPN-së (11 shkronja):

4 vertikalisht: Shërbim lidhjeje me rrezik të lartë që shpesh fiton para duke regjistruar dhe shitur të dhënat e shfletimit (8 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

O P E N V P N S C N X J I Y J
N S X S I D P E L I W Ç G L L
O A J P O F L R L P I Q R S S
I L Ë C R O M V G Q R B U Ç R
S A Z T C P Z E U Ë E I F K Z
K F Ç L D A P R X O G C T I B
I N A Z M R Ç Ë J A U D M L D
D P E F G E Ç R Q P A K D L G
I V Q Z R G E A P U R E A S A
R P N L O J S M X P D I Q W S
U Q Ç L F I V E E Y E S Y I B
J Ë Q X V S H A Q Z Y Y J T Ë
G L P I K T K S N F O P F C Z
A N U Ë T R C Y Q Y B F K H Z
Ë I M O M A V C K Z Y Ë Y N V

LISTA E FJALËVE TË LEKSIKUT

WIREGUARD, PAREGJISTRA, JURIDIKSION, KILLSWITCH, FIVEEYES, VPNFALAS, SERVERËRAM, OPENVPN

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

- **A. WIREGUARD**
- **B. PAREGJISTRA**
- **C. JURIDIKSION**
- **D. KILLSWITCH**
- **E. FIVEEYES**
- **F. VPNFALAS**
- **G. SERVERËRAM**
- **H. OPENVPN**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

_____ 1. Aleancë ndërkombëtare e ndarjes së inteligjencës midis SHBA-së, MB-së, Kanadasë, Australisë dhe Zelandës së Re.

_____ 2. Protokoll modern dhe i shpejtë që përdor rreth 4,000 rreshta kodi shumë të auditueshëm.

_____ 3. Protokoll i pjekur me burim të hapur, i audituar gjerësisht, me një bazë kodi shumë më të madhe se WireGuard.

_____ 4. Shërbim lidhjeje me rrezik të lartë që shpesh fiton para duke regjistruar dhe shitur të dhënat e shfletimit.

_____ 5. Mekanizëm sigurie që bllokon rrugëzimin e internetit nëse tuneli i sigurt shkëputet.

_____ 6. Infrastrukturë harduerike që funksionon tërësisht në memorie të paqëndrueshme, duke parandaluar ruajtjen e të dhënave.

_____ 7. Rajoni gjeografik që rregullon detyrimet ligjore të ofruesit të VPN-së.

_____ 8. Pretendim privatësie i verifikuar nga firma të pavarura të sigurisë kibernetike të palëve të treta.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të VPN-së. Shkruaji përgjigjet në kutitë e plotësueshme.

1. UGEIWARDR
2. DNUJOIRISKI
3. EIFEYSEV
4. RAEMVRËSER
5. TASIRAGJPRE
6. CSLITKIWHL
7. VSALAPFN
8. PNNOPVE

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Gjëra që mund t'i fshehë një VPN			
2	Gjëra që kanë më shumë rëndësi se çmimi			
3	Vende ku mund të lexosh vlerësime për VPN-të			
4	Gjëra nga të cilat një VPN nuk mund të të mbrojë			
5	Pyetje për ekipin e shitjeve të një VPN-je			
6	Gjëra që mund të shohë ofruesi yt i internetit			
7	Pika në listën tënde kur zgjedh një VPN			
8	Vende ku do të përdorje një VPN			
9	Shenja paralajmëruese te një ofrues VPN			
10	Fjalë që lidhen me privatësinë			
11	Gjëra që do t'i testoje të parat			
12	Premtime që jep një ofrues i mirë VPN			
13	Arsye për të përdorur një VPN gjatë udhëtimit			
14	Pajisje që mund të përdorin një VPN			
15	Mite për VPN-të			

Pika e kontrollit 8: Studime rasti për VPN-në

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

SARAH (STUDENTJA NË KAFENE)

👩‍💻 "Hej! Jam ulur te Coffee & Bytes. Ka një rrjet publik të pasigurt me emrin 'Free_Wi-Fi_No_Password'. Dua të hyj në emailin e shkollës dhe të ngarkoj detyrën, por kam frikë nga hakerët. Cilat janë rreziqet e përdorimit të këtij rrjeti pa VPN, dhe si i siguron një VPN të dhënat e mia?"

ALEX (STUDENT UDHËTAR)

👩‍💻 "Ç'fatkeqësi! Jam duke udhëtuar jashtë shtetit për një projekt dhe po provoj të shoh një dokumentar biologjie të strehuar në një server në vendin tim. Por faqja thotë 'Ky video nuk është i disponueshëm në vendndodhjen tënde aktuale.' Pse jam i bllokuar, dhe si mund të më ndihmojë një VPN ta shoh?"

Pika e kontrollit 9: Deshifrimi i kodit

Për të përfunduar trajnimin tënd për udhëzuesin e zgjedhjes, deshifro këtë mesazh të fshehur për zgjedhjen e infrastrukturës së sigurt.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

13 20 1 10 1 21 17 20 1 18 17 20 22 6 22 6

22 23 1 15 6 16 12 7 21 11 21 22 6 15 22 7

21 11 9 23 20 22

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për VPN-në (Pjesa A)

Rishiko pyetjet dhe përgjigjet më të zakonshme që kanë klientët e mundshëm për përdorimin e rrjeteve private virtuale.

Q1: Çfarë është një VPN dhe si funksionon?

Një Rrjet Privat Virtual (VPN) enkripton lidhjen tënde të internetit dhe e drejton trafikun tënd përmes një serveri të sigurt të largët. Kjo maskon adresën tënde publike IP dhe kufizon atë që vëzhguesit e rrjetit lokal dhe ISP-ja jote mund të shohin për trafikun e drejtuar përmes tunelit të VPN-së.

Q2: Pse duhet të përdor një VPN?

Një VPN mbron privatësinë tënde dixhitale, siguron lidhjen tënde në rrjete Wi-Fi publike (si kafenetë ose aeroportet), mund të zvogëlojë ngadalësimin e bazuar në aktivitet kur ISP-ja nuk mund ta identifikojë llojin e trafikut të enkriptuar, anashkalon kufizimet gjeografike për të hyrë në përmbajtje globale dhe ndihmon në sigurimin e burimeve të punës në distancë.

Q3: A më bën një VPN plotësisht anonim në internet?

Jo. Ndërsa një VPN e fsheh adresën tënde IP dhe enkripton trafikun, mund të gjurmohesh ende përmes cookie-ve të shfletuesit, llogarive aktive (si Google ose Facebook), fingerprinting-ut të shfletuesit, ose nëse ofruesi yt VPN regjistron të dhënat e tua.

Q4: A do ta ngadalësojë një VPN shpejtësinë e internetit tim?

Po, pak. Procesi i enkriptimit dhe distanca fizike deri te serveri VPN shtojnë vonesë dhe ngarkesë shtesë. Ndikimi ndryshon sipas ofruesit, protokollit, distancës së serverit, pajisjes dhe kushteve të rrjetit.

Q5: Si fiton para?

Kontrollo modelin e biznesit. Abonimet, nivelet freemium dhe shitja e të dhënave ndikojnë të gjitha në sa mund t'i besosh një VPN-je, dhe një shërbim që nuk i mbledh kurrë të dhënat e tua nuk mund t'i shesë. Lexo së pari politikën e privatësisë. [1]

Pika e kontrollit 10: Pyetje të shpeshta bazë për VPN-në (Pjesa B)

Rishiko pyetjet dhe përgjigjet më të zakonshme që kanë klientët e mundshëm për përdorimin e rrjeteve private virtuale.

Q6: A mund të përdor një VPN falas?

VPN-të falas mund të mbështeten te reklamat, veçoritë e kufizuara, analitika e përdorimit, kufijtë e të dhënave ose modele të tjera monetizimi. Përdoruesit duhet të shqyrtojnë politikën e privatësisë, pronësinë, auditimet dhe modelin e biznesit të ofruesit përpara përdorimit.

Q7: Çfarë është një politikë "no-logs"?

Një politikë no-logs përshkruan cilat të dhëna aktiviteti dhe lidhjeje thotë një ofrues se nuk i ruan. Shtrirja e saktë ndryshon, ndaj lexuesit duhet të shqyrtojnë politikën dhe gjetjet e auditimeve të pavarura.

Q8: Si ta zgjedh VPN-në më të mirë?

Kërko politika no-logs të audituara, protokolle të forta (WireGuard, OpenVPN), vendndodhje të sigurta serverësh, shpejtësi të larta, serverë vetëm me RAM, funksion kill switch dhe juridiksion jashtë aleancave të ndarjes së inteligjencës (si 5/9/14 Eyes).

Q9: A mund ta përdor një VPN në telefonin dhe televizorin tim smart?

Po. Ofruesit modernë të VPN-ve ofrojnë aplikacione të dedikuara për iOS, Android, macOS, Windows, Linux dhe televizorë inteligjentë, si dhe konfigurime në ruter për të mbrojtur të gjitha pajisjet në rrjetin e shtëpisë sate.

Q10: Çfarë është një Kill Switch?

Kill Switch është një veçori sigurie që e shkëput automatikisht pajisjen tënde nga interneti nëse lidhja VPN bie. Kjo parandalon rrjedhjen e të dhënave të tua të pa enkriptuara ose të adresës reale IP.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për VPN-në (Pjesa C)

Eksploro aspektet teknike dhe strukturore të rrjeteve private virtuale dhe të protokolleve të sigurta të tunelimit.

Q1: Cili është ndryshimi midis WireGuard, OpenVPN dhe IKEv2?

WireGuard është një protokoll modern dhe i lehtë (vetëm ~4,000 rreshta kodi) që ofron shpejtësi të larta dhe kohë të shpejta lidhjeje. OpenVPN është një protokoll me kod të hapur shumë i sigurt dhe i provuar. IKEv2 është i shkëlqyer për pajisjet celulare falë aftësisë për t'u rilidhur shpejt kur ndërrohen rrjetet.

Q2: Çfarë është rrugëzimi double VPN ose Multi-Hop?

Multi-Hop e rutuon trafikun tënd nëpër dy ose më shumë serverë VPN në sekuencë. Kjo shton një shtresë të dytë enkriptimi dhe ndihmon ta mbajë të fshehur adresën tënde të vërtetë IP nga hop-i i dytë nëse një server kompromentohet.

Q3: Çfarë është rrjedhja e WebRTC dhe si e parandalon një VPN?

WebRTC është një protokoll i shfletuesit që mund të zbulojë adresat e tua reale IP lokale dhe publike edhe kur një VPN është aktive. VPN-të premium bllokojnë ose falsifikojnë kërkesat WebRTC në aplikacionet e tyre për desktop/celular dhe në shtesat e shfletuesit.

Q4: Çfarë janë serverët vetëm me RAM dhe pse kanë rëndësi?

Serverët tradicionalë i shkruajnë të dhënat në disqet e ngurtë, të cilët mund të konfiskohen ose kompromentohen. Serverët vetëm me RAM (pa disk) funksionojnë tërësisht në memorie të paqëndrueshme (RAM). Kur serveri riniset ose fiket, të dhënat e mbajtura në memorie fshihen.

Q5: Si i anashkalon Obfuscation bllokimet e VPN-ve?

Maskimi (obfuscation, ose "Stealth VPN") i shndërron paketat e trafikut VPN që të duken si trafik i zakonshëm uebi HTTPS (porti 443). Kjo ndihmon të kalohet Inspektimi i Thellë i Paketave (DPI) që përdorin qeveritë ose rrjetet e shkollave/zyrave për të bllokuar VPN-të.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për VPN-në (Pjesa D)

Eksploro aspektet teknike dhe strukturore të rrjeteve private virtuale dhe të protokolleve të sigurta të tunelimit.

Q6: Çfarë është Split Tunneling dhe kur duhet ta përdor?

Split Tunneling të lejon të zgjedhësh cilat aplikacione rrugëzohen përmes tunelit të enkriptuar VPN dhe cilat lidhen drejtpërdrejt me internetin. Përdore për të drejtuar aplikacionet e ndjeshme bankare përmes VPN-së, ndërsa lojërat lokale lidhen drejtpërdrejt, duke shmangur vonesën e shtuar nga VPN-ja.

Q7: Si funksionon Forward Secrecy (Perfect Forward Secrecy)?

PFS siguron që për çdo seancë të krijohet një çelës enkriptimi unik e i përkohshëm. Edhe nëse një çelës privat kompromentohet në të ardhmen, ai nuk mund të përdoret për të deshifruar seancat e kaluara ose të ardhshme, sepse ato përdorën çelësa të pavarur.

Q8: Çfarë janë aleancat 5/9/14 Eyes dhe pse duhet të më interesojnë?

Juridiksioni mund të ndikojë në procesin ligjor me të cilin përballet një ofrues, por rreziku praktik i privatësisë varet edhe nga të dhënat që ruan ofruesi, arkitektura e tij teknike, pronësia, raportimi i transparencës dhe historiku i auditimeve.

Q9: Çfarë është mbrojtja nga rrjedhjet e DNS-së?

Mbrojtja nga rrjedhjet e DNS e detyron pajisjen tënde t'i dërgojë kërkesat e kërkimit të faqeve të internetit (kërkesat DNS) nëpërmjet serverëve DNS privatë dhe të enkriptuar të VPN-së, në vend të serverëve të ISP-së sate. Kjo e pengon ISP-në tënde të gjurmojë se cilat faqe vizitoni.

Q10: Pse të kontrollosh kush e drejton dhe e mbështet një VPN?

Reputacioni ka rëndësi. Hulumto pronarët dhe drejtuesit e kompanisë, kërko auditime publike nga palë të treta dhe shiko çfarë thonë ekspertët e pavarur të sigurisë dhe shtypi përpara se t'i besosh. [1]

Pjesa 11: 10 fakte interesante për VPN-të dhe njohuri nga bota reale

Rishiko këto fakte dhe njohuri reale shumë të vlefshme për historinë, tregun dhe teknologjinë e VPN-ve.

1. PROTOKOLLI I PARË VPN

PPTP (Point-to-Point Tunneling Protocol), një protokoll i hershëm VPN nga një grup i udhëhequr nga Microsoft në vitet 1990, tani konsiderohet i pasigurt, prandaj VPN-të moderne përdorin WireGuard ose OpenVPN. [1]

2. VLERËSIMI I TREGUT

Tregu global i VPN-ve ka përjetuar rritje të shpejtë, të nxitur nga kërkesat në rritje për punë në distancë dhe nevojat e sigurisë së ndërmarrjeve.

3. REVOLUCIONI WIREGUARD

WireGuard ka një bazë kodi shumë të thjeshtuar, të projektuar për efikasitet, që e bën më të lehtë për t'u audituar për cenueshmëri sigurie se protokollet tradicionale. [3]

4. STANDARDE TË RREPTA AUDITIMI

Ofruesit kryesorë të VPN-ve angazhojnë firma si Deloitte, KPMG ose PwC për të kontrolluar pretendimet pa regjistrim (no-logs), dhe firma sigurie si Cure53 për të testuar aplikacionet dhe serverët e tyre. [4]

5. ORIGJINA E ALEANCËS 5-EYES

Partneriteti i inteligjencës Five Eyes mes SHBA-së, Mbretërisë së Bashkuar, Kanadasë, Australisë dhe Zelandës së Re u zhvillua nga bashkëpunimi i Aleatëve në inteligjencën e sinjaleve në kohën e Luftës së Dytë Botërore.

6. INSPEKTIMI I THELLË I PAKETAVE

Firewall-et e avancuar përdorin Deep Packet Inspection (DPI) për të analizuar metadatat e paketave të rrjetit dhe për të bllokuar karakteristikat standarde të lidhjes VPN.

7. PËRDORIMI KORPORATIV

Shumë organizata u japin punonjësve në distancë një VPN për të hyrë në sisteme të brendshme si bazat e të dhënave, gjë që i bën VPN-të një mjet të zakonshëm sigurie në vendin e punës.

8. VPN-TË TË DECENTRALIZUARA

VPN-të e decentralizuara (dVPN) e shpërndajnë trafikun nëpër një rrjet nyjesh të drejtuara nga bashkëveta (peer), duke zvogëluar varësinë nga një ofrues i vetëm i centralizuar.

9. ANONIMITETI I TOR KUNDRAS VPN-SË

Një VPN e tunelon trafikun përmes një ofruesi të vetëm, ndërsa Tor (The Onion Router) e dërgon trafikun përmes tre releve vullnetare (guard, middle, exit) për të maksimizuar privatësinë. [5]

10. KOSTOJA E SHKELJEVE TË TË DHËNAVE

Kombinimi i një VPN-je me një model qasjeje zero-trust, që kontrollon çdo përdorues dhe pajisje, i ndihmon organizatat të mbrojnë të dhënat dhe të kufizojnë dëmin e shkeljeve të të dhënave.

Referenca teknike dhe burime

Botime të cituara, specifikime kriptografike dhe standarde zyrtare dokumentesh të përdorura në këtë fletë pune.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

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

https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

Çelësi i përgjigjeve: Vlerësimi i ofruesve të VPN-së, standardet e sigurisë, auditimet dhe politikat e regjistrimit

1 **Politika e logjeve të audituara** PROTOKOLLE — **Përgjigjja e saktë: B**

SHËNIM PËR MËSUESIN

Një politikë no-logs e audituar në mënyrë të pavarur është mënyra më praktike për të kontrolluar pretendimet e një ofruesi për privatësi zero-knowledge. Marketingu tërheqës ose pretendimet e vetë ofruesit nuk mjaftojnë. Citim: Deloitte Advisory, Cure53 Audit.

2 **Epërsia e WireGuard** VONESA — **Përgjigjja e saktë: D**

SHËNIM PËR MËSUESIN

WireGuard ofron rutim modern dhe të shpejtë të lidhjeve në hapësirën e kernelit me një bazë kodi kompakte (~4,000 rreshta), që i bën auditimet shumë efikase. Citim: IETF Protocol RFC, WireGuard Project.

3 **Pyetja 3** — **Përgjigjja e saktë: B**

SHËNIM PËR MËSUESIN

VPN-të falas prapë paguajnë për serverët, dhe FTC paralajmëron se disa aplikacione VPN ndajnë të dhëna të përdoruesve me palë të treta, për shembull për të shfaqur reklama.

4 **Juridiksionet ligjore** KONTROLLET E RUTERIMIT — **Përgjigjja e saktë: C**

SHËNIM PËR MËSUESIN

Juridiksioni përcakton nëse VPN-ja i nënshtrohet ligjeve të survejimit, detyrimeve vendase të ruajtjes së të dhënave dhe urdhrave të fshehtë qeveritarë të thirrjes. Citim: Privacy Rights Clearinghouse.

5 **Mbrojtja Kill Switch** PRIVATËSI — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Kill switch-i e ndërpret menjëherë rrugëzimin e përshtatësit të rrjetit të sistemit nëse tuneli bie, duke parandaluar rrjedhjet e ekspozimit të IP-së së vërtetë dhe DNS-së. Citim: IETF Tunnel RFC.

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Kufizimet e malware-it** MASKIMI I IP-SË — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Një VPN ofron një kanal të sigurt të enkriptuar, por nuk skanon ngarkesat ose skedarët. Nevojitet softuer antivirus për të bllokuar malware-in. Citim: Deloitte Advisory.

7 **Auditim i pavarur** SHPEJTËSITË — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Raportet e auditimit verifikojnë konfigurimet e softuerit të serverit, përputhshmërinë me konfigurimin vetëm me RAM dhe mungesën e bazave të të dhënave të regjistrimit. Citim: Deloitte Advisory, Cure53 Audit.

8 **Pyetja 8** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Ofruesit duhet të ndjekin ligjet e vendit të tyre, të cilat mund të përfshijnë rregulla për ruajtjen e të dhënave dhe urdhra për dorëzimin e të dhënave që mbajnë.

9 **Madhësia e bazës së kodit të protokollit** FIREWALL-E — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Një bazë kodi më e vogël zvogëlon sipërfaqen e mundshme të sulmit dhe e bën më të lehtë për ekipet e sigurisë të verifikojnë integritetin e protokollit. Citim: WireGuard Project.

10 **Monetizimi me reklama** PA REGJISTRA — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Pa tarifa abonimi, VPN-të falas mbështeten te nxjerrja e të dhënave, profilizimi i trafikut dhe injektimi i reklamave në shfletues për të gjeneruar të ardhura. Citim: EDRi Retention Guidelines.

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

F 1. WireGuard	H 2. Regjistra të audituar	E 3. Juridiksioni	B 4. Kill switch
C 5. Five Eyes	A 6. VPN falas	D 7. Serverë vetëm me RAM	G 8. OpenVPN

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 PA REGJISTRA	2 WIREGUARD	3 KILL SWITCH	4 JURIDIKSION
5 SERVERË RAM	6 AUDITIM		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – VPNFALAS
5 D – KILLSWITCH	6 G – SERVERËRAM	7 C – JURIDIKSION	8 B – PAREGJISTRA

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë WireGuard, Regjistra të audituar dhe Juridiksioni me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

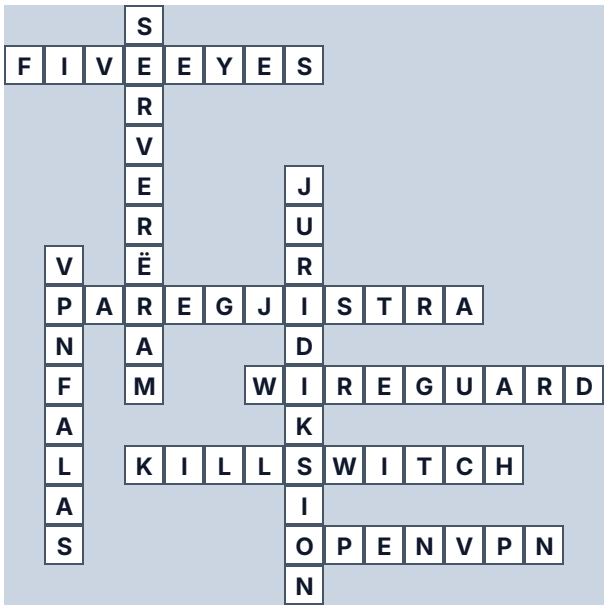
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

O	P	E	N	V	P	N	S	C	N	X	J	I	Y	J
N	S	X	S	I	D	P	E	L	I	W	Ç	G	L	L
O	A	J	P	O	F	L	R	L	P	I	Q	R	S	S
I	L	Ë	C	R	O	M	V	G	Q	R	B	U	Ç	R
S	A	Z	T	C	P	Z	E	U	Ë	E	I	F	K	Z
K	F	Ç	L	D	A	P	R	X	O	G	C	T	I	B
I	N	A	Z	M	R	Ç	Ë	J	A	U	D	M	L	D
D	P	E	F	G	E	Ç	R	Q	P	A	K	D	L	G
I	V	Q	Z	R	G	E	A	P	U	R	E	A	S	A
R	P	N	L	O	J	S	M	X	P	D	I	Q	W	S
U	Q	Ç	L	F	I	V	E	E	Y	E	S	Y	I	B
J	Ë	Q	X	V	S	H	A	Q	Z	Y	Y	J	T	Ë
G	L	P	I	K	T	K	S	N	F	O	P	F	C	Z
A	N	U	Ë	T	R	C	Y	Q	Y	B	F	K	H	Z
Ë	I	M	O	M	A	V	C	K	Z	Y	Ë	Y	N	V

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

2 horizontalisht: FIVEEYES Aleancë ndërkombëtare e ndarjes së inteligjencës midis SHBA-së, MB-së, Kanadasë, Australisë dhe Zelandës së Re (8 shkronja)

5 horizontalisht: PAREGJISTRA Pretendim privatësie i verifikuar nga firma të pavarura të sigurisë kibernetike të palëve të treta (11 shkronja)

6 horizontalisht: WIREGUARD Protokoll modern dhe i shpejtë që përdor rreth 4,000 rreshta kodi shumë të auditueshëm (9 shkronja)

7 horizontalisht: KILLSWITCH Mekanizëm sigurie që bllokon rrugëzimin e internetit nëse tuneli i sigurt shkëputet (10 shkronja)

8 horizontalisht: OPENVPN Protokoll i pjekur me burim të hapur, i audituar gjerësisht, me një bazë kodi shumë më të madhe se WireGuard (7 shkronja)

VERTIKALISHT

1 vertikalisht: SERVERËRAM Infrastrukturë harduerike që funksionon tërësisht në memorie të paqëndrueshme, duke parandaluar ruajtjen e të dhënave (10 shkronja)

3 vertikalisht: JURIDIKSION Rajoni gjeografik që rregullon detyrimet ligjore të ofruesit të VPN-së (11 shkronja)

4 vertikalisht: VPNFALAS Shërbim lidhjeje me rrezik të lartë që shpesh fiton para duke regjistruar dhe shitur të dhënat e shfletimit (8 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1. UGEIWARDR	WIREGUARD	5. TASIRAGJPRE	PAREGJISTRA
2. DNUJOIRISKI	JURIDIKSION	6. CSLITKIWHL	KILLSWITCH
3. EIFEYSEV	FIVEEYES	7. VSALAPFN	VPNFALAS
4. RAEMVRËSER	SERVERËRAM	8. PNNOPVE	OPENVPN

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"KRAHASO RAPORTET E TUA ME NJË SISTEM TË SIGURT"

Çelësi i studimeve të rastit

A Skenari A: Siguria në rrjete publike

PËRGJIMI DHE ENKRIPTIMI | Dilema e Sarës

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Rreziqet: Përgjimi i paketave, përgjimi i të dhënave dhe sulmet man-in-the-middle. Dikush në të njëjtin rrjet të kafenesë mund të kapte detajet e hyrjes ose skedarin e detyrave të saj.
- Mbrojtja e VPN-së: Enkripton ngarkesat e paketave të rrjetit, duke e bërë trafikun e përgjuar të tunelit të palexueshëm për përgjuesit pasivë të rrjetit lokal kur VPN-ja është konfiguruar saktë.

B Skenari B: Qasja te burimet e bllokuara

BLLOKIMI GJEOGRAFIK DHE IP-TË | Dilema e Alexit

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Pse u bllokua: Hosti i transmetimit përdor gjeobllokimin, që e lidh adresën lokale IP të udhëtarit me shtetin e tij fizik dhe e bllokon sipas licencimit territorial.
- Si ndihmon VPN-ja: Maskon vendndodhjen e tij reale duke rrugëzuar trafikun përmes një serveri në vendin e tij. Faqja shikon IP-në e vendit të tij dhe lejon qasjen.