Emri: _____ Data: _____ Pikët: _____

Siguria e ExpressVPN

Vlerësimi i infrastrukturës së sigurisë së ExpressVPN, protokollit të personalizuar Lightway me burim të hapur, teknologjisë TrustedServer vetëm me RAM, auditimeve të pavarura të sigurisë dhe kill switch-it Network Lock.

PËRMBLEDHJE MËSIMORE PËR SIGURINË E EXPRESSVPN

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 veçorive të sigurisë së ExpressVPN. Do të eksplorosh protokollet me burim të hapur, nyjet e serverëve vetëm me RAM, shifrat dhe kill switch-in Network Lock.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro konfigurimet e VPN-së dhe të sigurisë së rrjetit.**
- [ ] **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-të më të mira

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

Udhërrëfyesi yt mësimor për sigurinë e ExpressVPN

- Analizo arkitekturën teknike dhe rregullat e konfigurimit të sigurisë së ExpressVPN.
- Konfiguro cilësimet e klientit për të parandaluar rrjedhjet e trafikut IP, DNS dhe WebRTC.
- Krahaso çmimet e personalizuara, provën dhe veçoritë e performancës me modelet standarde.

UDHËZIME PËR UDHËZUESIN E SIGURISË SË EXPRESSVPN

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 protokollet me burim të hapur dhe nyjet e serverëve vetëm me RAM. Përfundo me aktivitetin bonus Mendo shpejt.

GRUPE SERVERËSH VETËM ME RAM DHE PROTOKOLLE LIDHJEJE ME BURIM TË HAPUR

ExpressVPN përdor teknologjinë TrustedServer vetëm me RAM për të parandaluar regjistrat lokalë, e kombinuar me protokollin e tij të personalizuar Lightway me burim të hapur dhe një Internet Kill Switch për të ofruar siguri të të dhënave të përdoruesit nga skaji në skaj.

(HYRJE)

ExpressVPN përdor teknologjinë TrustedServer vetëm me RAM për të parandaluar regjistrat lokalë, e kombinuar me protokollin e tij të personalizuar Lightway me burim të hapur dhe një Internet Kill Switch për të ofruar siguri të të dhënave të përdoruesit nga skaji në skaj.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Cili është protokolli i personalizuar me kod të hapur i ExpressVPN-së?**

- A) Lightway
- B) WireGuard
- C) OpenVPN
- D) Chameleon

2 **2. Cila teknologji serveri funksionon ekskluzivisht në RAM të paqëndrueshme?**

- A) TrustedServer
- B) RAM-Core
- C) SecureRAM
- D) Server NoSpy

3 **3. Çfarë ndodh nëse një lidhje VPN ndërpritet papritur?**

- A) Kill switch e bllokon trafikun
- B) Trafiku rrjedh te ofruesi i internetit
- C) Sistemi rinis
- D) Të dhënat bëhen të paenkriptuara

4 **4. Ku është themeluar ExpressVPN për të mbrojtur privatësinë?**

- A) Ishujt e Virgjër Britanikë
- B) Zvicra
- C) Panamaja
- D) Rumania

5 **5. Cila shifër simetrike e enkriptimit përdoret si parazgjedhje?**

- A) AES-256-GCM
- B) Blowfish
- C) DES-64
- D) RC4

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

6 Pyetja 6

6. Teknologjia TrustedServer i ruan regjistrat e serverit në disqet e ngurtë.

E vërtetë E gabuar

7 Pyetja 7

7. ExpressVPN ka kaluar auditime sigurie nga palë të treta.

E vërtetë E gabuar

8 Pyetja 8

8. Protokolli Lightway është ndërtuar mbi bazën e kodit të OpenVPN.

E vërtetë E gabuar

9 Pyetja 9

9. Kill switch është i aktivizuar si parazgjedhje në aplikacionet desktop.

E vërtetë E gabuar

10 Pyetja 10

10. ExpressVPN operon DNS privat në çdo server.

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. Protokolli i brendshëm me shpejtësi të lartë i dizajnuar nga ExpressVPN është _____ .

2. Për të parandaluar ruajtjen e të dhënave, rrjeti i serverëve mbështetet te nyje vetëm me RAM të quajtura _____ .

3. Kill switch-i i ExpressVPN dikur quhej Network _____ .

4. ExpressVPN është i regjistruar sipas ligjeve të territorit britanik _____ .

5. Ngarkesat e të dhënave sigurohen me shifrën simetrike të fortë _____ .

6. Politika zero-logs është verifikuar dhe _____ në mënyrë të pavarur nga firma kryesore.

BANKA E FJALËVE TË LEKSIKUT

AES-256 AUDITUAR ISHUJT E VIRGJËR LIGHTWAY LOCK RRJEDHJE TRUSTED SERVER ZGJIDHËS DNS

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të VPN-së dhe rrjetit

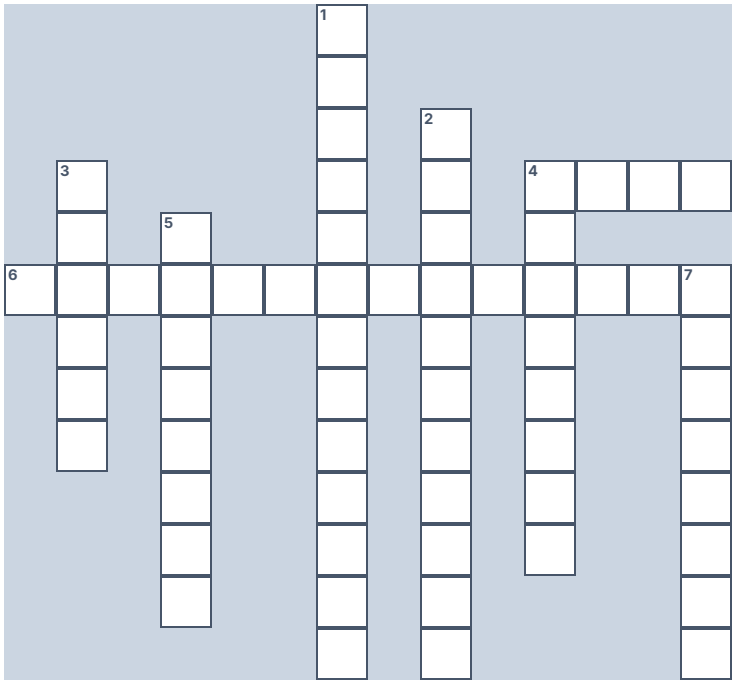
PËRPUTHJA E PËRKUFIZIMEVE

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. LIGHTWAY	A	Juridiksioni i Ishujve të Virgjër Britanikë që ofron privatësi të fortë
☐	2. TRUSTED SERVER	B	Ekspozimi i paqëllimtë i të dhënave private IP, DNS ose WebRTC
☐	3. BRAVË	C	Zgjidhësit e Domain Name System funksionojnë privatisht në çdo nyje serveri
☐	4. ISHUJT	D	Verifikuar në mënyrë të pavarur nga firma sigurie të palëve të treta
☐	5. AES-256	E	Arkitekturë serveri vetëm me RAM që parandalon ruajtjen e të dhënave në disk
☐	6. I AUDITUAR	F	Fjala e fundit e Network Lock, emrit të mëparshëm të kill switch-it
☐	7. RRJEDHJE	G	Protokolli i lehtë i lidhjes me burim të hapur i ExpressVPN
☐	8. DNS	H	Standard enkriptimi simetrik që siguron transmetimin e të dhënave

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

4. Fjala e fundit e Network Lock, emrit të mëparshëm të kill switch-it (4)

6. Juridiksioni i Ishujve të Virgjër Britanikë, që ofron privatësi të fortë (14)

VERTIKALISHT

1. Arkitekturë serverësh vetëm me RAM që parandalon ruajtjen e të dhënave në disk (13)

2. Zgjidhës të Sistemit të Emrave të Domeneve që funksionojnë privatisht në çdo nyje serveri (11)

3. Standard enkriptimi simetrik që siguron transmetimin e të dhënave (6)

4. Protokoll lidhjeje i lehtë dhe me burim të hapur i ExpressVPN (8)

5. Verifikuar në mënyrë të pavarur nga firma sigurie të palëve të treta (8)

7. Ekspozim i paqëllimshëm i të dhënave private IP, DNS ose WebRTC (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

4 horizontalisht: Fjala e fundit e Network Lock, emrit të mëparshëm të kill switch-it (4 shkronja):

6 horizontalisht: Juridiksioni i Ishujve të Virgjër Britanikë, që ofron privatësi të fortë (14 shkronja):

VERTIKALISHT

1 vertikalisht: Arkitekturë serverësh vetëm me RAM që parandalon ruajtjen e të dhënave në disk (13 shkronja):

2 vertikalisht: Zgjidhës të Sistemit të Emrave të Domeneve që funksionojnë privatisht në çdo nyje serveri (11 shkronja):

3 vertikalisht: Standard enkriptimi simetrik që siguron transmetimin e të dhënave (6 shkronja):

4 vertikalisht: Protokoll lidhjeje i lehtë dhe me burim të hapur i ExpressVPN (8 shkronja):

5 vertikalisht: Verifikuar në mënyrë të pavarur nga firma sigurie të palëve të treta (8 shkronja):

7 vertikalisht: Ekspozim i paqëllimshëm i të dhënave private IP, DNS ose WebRTC (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.

A U D I T U A R G Q Z R E P U

E Y A A P N L O S X T P I Q S

S A Q Ç L Y B Ë Q X R V H A Q

N W Z Y A Y J Ë G L U P I K K

D T K S E N F O P F S Z A N U

S H C Ë S T C Y Q Y T B F K Z

Ë G O Ë 2 I M O M V E C K Z Y

H I L Ë 5 Y N V T J D T O B M

D L U S 6 K F T Ç Y S T I Q B

I V Z Y K Q P X G N E Ç A Ç I

J I S H U J T E V I R G J Ë R

G P U V V J H G S G V Ë B E G

Z J R R J E D H J E E S Q U P

Z D G E Q C A J O C R Z K I U

Q T A R V I K K F F L G P Ë J

LISTA E FJALËVE TË LEKSIKUT

LIGHTWAY TRUSTEDSERVER LOCK ISHUJTEVIRGJËR AES256 AUDITUAR RRJEDHJE ZGJIDHËSDNS

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. LIGHTWAY**
- **B. TRUSTEDSERVER**
- **C. LOCK**
- **D. ISHUJTEVIRGJËR**
- **E. AES256**
- **F. AUDITUAR**
- **G. RRJEDHJE**
- **H. ZGJIDHËSDNS**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Ekspozim i paqëllimshëm i të dhënave private IP, DNS ose WebRTC.
2. Juridiksioni i Ishujve të Virgjër Britanikë, që ofron privatësi të fortë.
3. Zgjidhës të Sistemit të Emrave të Domeneve që funksionojnë privatisht në çdo nyje serveri.
4. Protokoll lidhjeje i lehtë dhe me burim të hapur i ExpressVPN.
5. Fjala e fundit e Network Lock, emrit të mëparshëm të kill switch-it.
6. Standard enkriptimi simetrik që siguron transmetimin e të dhënave.
7. Arkitekturë serverësh vetëm me RAM që parandalon ruajtjen e të dhënave në disk.
8. Verifikuar në mënyrë të pavarur nga firma sigurie 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 rrjetit privat virtual (VPN). Shkruaji përgjigjet në kutitë e dhëna.

1. AHTLWIYG
2. LCKO
3. AS265E
4. EJEHDRRJ
5. EVRUSTRERDTES
6. TEGJHJVËRISIRU
7. ARTUAUID
8. DËSHJZDGNSI

Aktivitet bonus: Mendo shpejt

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

1	Veçori që kërkon te ExpressVPN			
2	Kërcënime në Wi-Fi publik			
3	Lloje rrjedhjesh të VPN-së			
4	Mënyra për të krijuar një fjalëkalim të fortë			
5	Butona ose menu në një aplikacion VPN			
6	Gjëra që bën çdo ditë në internet			
7	Njerëz që do t'u rekomandoje ExpressVPN			
8	Vende të njohura për ligje të forta privatësie			
9	Protokolle VPN që njeh			
10	Gjëra që mund të kontrollojë një auditim			
11	Veçori sigurie te ExpressVPN			
12	Gjëra për t'u kontrolluar para blerjes së një VPN-je			
13	Cilësime që i aktivizon për siguri shtesë			
14	Gjëra që mbron enkriptimi			
15	Gjëra që ExpressVPN mund t'i fshehë nga rrjeti yt			

Pika e kontrollit 8: Studime rasti për VPN-në dhe rrjetin

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

STUDIMI I RASTIT 1: ZBATIMI I MBROJTJEVE VETËM ME RAM



Skenari: Një agjenci qeveritare merr me forcë një server ExpressVPN për të nxjerrë regjistrat e përdoruesve dhe historikun e lidhjeve.

Pyetje për diskutim: Çfarë informacioni do të gjejnë në server dhe pse?

STUDIMI I RASTIT 2: TUNELET E PAQËNDRUESHME TË LIDHJES WI-FI



Skenari: Një punonjës në distancë përdor Wi-Fi-n publik të një hoteli, i cili ndërpritet çdo disa minuta ndërsa ai redakton dokumente.

Pyetje për diskutim: Si i mbron ExpressVPN të dhënat e tij nga rrjedhja gjatë ndërprerjeve?

Pika e kontrollit 9: Deshifrimi i kodit

Një inxhinier rrjeti siguron kanalet e drejtimit dhe tunelet e klientëve. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

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

22	20	23	21	22	6	5	21	6	20	24	6	20		8	21	10	11	16

14	17	9	6	22		6		18	7	20	5	17	20	23	6	21	24	6

4	5	17		5	11	22	7

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 për Rrjetet Private Virtuale (VPN) dhe tunelimin.

Q1: Çfarë enkriptimi përdor ExpressVPN?

ExpressVPN përdor si parazgjedhje enkriptimin simetrik AES-256-GCM.

Q2: Çfarë është protokolli Lightway?

Lightway është protokolli i personalizuar i ExpressVPN-it, i ndërtuar për shpejtësi, siguri dhe qëndrueshmëri.

Q3: A e regjistron ExpressVPN historikun tim të kërkimeve?

Jo, ExpressVPN zbaton një politikë të rreptë zero regjistrash, të audituar në mënyrë të pavarur.

Q4: Çfarë është Internet Kill Switch?

Është kill switch-i natyral i ExpressVPN që bllokon trafikun e internetit nëse lidhja ndërpritet.

Q5: A është protokolli Lightway me burim të hapur?

Po, kodi bazë i protokollit Lightway është me burim të hapur dhe gjendet në GitHub. [9]

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

Rishiko pyetjet dhe përgjigjet më të zakonshme për Rrjetet Private Virtuale (VPN) dhe tunelimin.

Q6: A ekzekuton ExpressVPN DNS privat?

Po, ExpressVPN operon DNS-in e vet privat dhe të enkriptuar në çdo server. [7]

Q7: Çfarë është teknologjia TrustedServer?

Është një konfigurim serveri ku OS-i dhe aplikacionet funksionojnë tërësisht në memorie RAM të paqëndrueshme.

Q8: A është audituar ExpressVPN?

Po, ExpressVPN është audituar nga firma si PwC, Cure53 dhe F-Secure. [1]

Q9: A mbron ExpressVPN nga rrjedhjet e DNS-së dhe IPv6?

Po, Internet Kill Switch bllokon trafikun IPv4, IPv6 dhe DNS jashtë tunelit.

Q10: Ku ndodhet ExpressVPN?

ExpressVPN është i regjistruar në Ishujt e Virgjër Britanikë (BVI).

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

Eksploro aspektet e avancuara teknike të protokolleve të tunelimit të VPN-ve, integrimeve të klientëve mobil dhe zbatimit në ndërmarrje.

Q1: Si e përmirëson sigurinë arkitektura vetëm me RAM?

Të dhënat nuk shkruhen në hard disqe, dhe të dhënat e mbajtura në memorie fshihen sa herë që serveri fiket.

Q2: Pse ka rëndësi juridiksioni i BVI për privatësinë?

ExpressVPN ka bazë në BVI, prandaj kërkesat ligjore për të dhëna i nënshtrohen ligjeve të BVI.

Q3: A e mbështet ExpressVPN fshehtësinë e përsosur të përcjelljes (perfect forward secrecy)?

Po, Lightway përdor çelësa dinamikë që pastrohen dhe rigjenerohen rregullisht.

Q4: Si i parandalon Network Lock rrjedhjet e IP-së?

Bllokon të gjithë trafikun në nivel sistemi sa herë që lidhja VPN ndërpritet.

Q5: A mbron Lightway nga sulmet kuantike?

Po, Lightway ka mbrojtje post-kuantike duke përdorur standardin NIST ML-KEM.

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

Eksploro aspektet e avancuara teknike të protokolleve të tunelimit të VPN-ve, integrimeve të klientëve mobil dhe zbatimit në ndërmarrje.

Q6: A mund ta përgjojnë agjencitë qeveritare trafikun e Lightway?

Mund ta përgjojnë, por nuk mund ta deshifrojnë për shkak të enkriptimit AES-256/ChaCha20.

Q7: Si i mbron DNS-ja private regjistrat e kërkimeve të përdoruesit?

Përpunon të gjitha kërkesat DNS brenda tunelit të enkriptuar, duke parandaluar monitorimin nga ISP-ja.

Q8: Për çfarë përdoret Lightway Turbo?

Përdor tunelim me shumë korsi për të dërguar më shumë të dhëna njëherësh për shpejtësi më të larta.

Q9: Cili është avantazhi i Lightway ndaj WireGuard?

Lightway është ndërtuar posaçërisht për t'i përballuar shpejt kalimet mes rrjeteve (si nga Wi-Fi në celular) pa u ndërprerë.

Q10: Sa shpesh riinstalohet softueri i serverit?

Me TrustedServer, i gjithë stoku i softuerit ringarkohet nga një imazh i sigurt vetëm për lexim në çdo rindezje.

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

Rishiko fakte reale për shpejtësitë e enkriptimit të VPN-së, auditimet e protokolleve, lidhjen mobile dhe punën në distancë të ndërmarrjeve.

1. PERSPEKTIVË PËR VPN-NË

Lightway përdor AES-256-GCM, ose ChaCha20/Poly1305 në pajisje me energji të ulët. [6]

2. PERSPEKTIVË PËR VPN-NË

Teknologjia TrustedServer është projektuar që t'i ekzekutojë të gjitha operacionet e serverit në RAM. [4]

3. PERSPEKTIVË PËR VPN-NË

Ishujt e Virgjër Britanikë (BVI) shërbejnë si juridiksion korporativ. [8]

4. PERSPEKTIVË PËR VPN-NË

Lightway u rishkrua nga C në Rust dhe u auditua nga Cure53 dhe Praetorian. [3]

5. PERSPEKTIVË PËR VPN-NË

Internet Kill Switch bllokon trafikun në nivel sistemi nëse VPN-ja ndërpritet. [5]

6. PERSPEKTIVË PËR VPN-NË

Të gjitha kërkesat DNS zgjidhen përmes serverëve privatë të enkriptuar DNS. [7]

7. NJOHURI PËR VPN-NË

ExpressVPN ka publikuar më shumë se 20 auditime të pavarura nga palë të treta. [1]

8. NJOHURI PËR VPN-NË

Shërbimi nuk regjistron adresa IP, historik shfletimi ose metadata të trafikut.

9. NJOHURI PËR VPN-NË

Perfect Forward Secrecy ruhet duke përdorur rotacion dinamik të çelësave të seancës. [1]

10. PERSPEKTIVË PËR VPN-NË

Protokolli Lightway mbështet si shtresat e transportit UDP, ashtu edhe TCP.

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet teknike globale, specifikimet dhe kuadrot rregullatore.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[1] ExpressVPN. (n.d.). ExpressVPN Trust Center.
https://www.expressvpn.com/trust

[2] ExpressVPN. (n.d.). Lightway: A VPN Protocol by ExpressVPN.
https://www.expressvpn.com/lightway

[3] ExpressVPN. (2025). Lightway's Rust rewrite undergoes two security audits, by Cure53 and Praetorian.
https://www.expressvpn.com/blog/lightway-audits-cure53-praetorian/

[4] ExpressVPN. (n.d.). ExpressVPN TrustedServer Technology.
https://www.expressvpn.com/features/trustedserver

[5] ExpressVPN. (n.d.). VPN Kill Switch: What It Is & How ExpressVPN Keeps You Safe.
https://www.expressvpn.com/features/network-lock

[6] ExpressVPN. (n.d.). How Secure Is VPN Encryption?
https://www.expressvpn.com/what-is-vpn/vpn-encryption

[7] ExpressVPN. (n.d.). Get a VPN With Private DNS.
https://www.expressvpn.com/features/dns

[8] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[9] ExpressVPN. (n.d.). Lightway Rust Open Source Workspace [GitHub repository].
https://github.com/expressvpn/lightway

[10] Cure53. (2024). Audit-Report ExpressVPN Lightway Protocol 10.-11.2024.
https://cure53.de/pentest-report_expressvpn-lightway_2024.pdf

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

[12] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Pyetja 1** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cili është protokolli i personalizuar me kod të hapur i ExpressVPN-së? → Lightway

2 **Pyetja 2** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cila teknologji serveri funksionon ekskluzivisht në RAM të paqëndrueshme? → TrustedServer

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

SHËNIM PËR MËSUESIN

Çfarë ndodh nëse një lidhje VPN ndërpritet papritur? → A) Kill switch e bllokon trafikun

4 **Pyetja 4** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Ku është themeluar ExpressVPN për të mbrojtur privatësinë? → Ishujt e Virgjër Britanikë

5 **Pyetja 5** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cila shifër simetrike e enkriptimit përdoret si parazgjedhje? → AES-256-GCM

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

6 **Pyetja 6**

Përgjigjja e saktë: E gabuar

SHËNIM PËR MËSUESIN

Teknologjia TrustedServer i ruan regjistrat e serverit në disqet e ngurtë.

7 **Pyetja 7**

Përgjigjja e saktë: E vërtetë

SHËNIM PËR MËSUESIN

ExpressVPN ka kaluar auditime sigurie nga palë të treta.

8 **Pyetja 8**

Përgjigjja e saktë: E gabuar

SHËNIM PËR MËSUESIN

Protokolli Lightway është ndërtuar mbi bazën e kodit të OpenVPN.

9 **Pyetja 9**

Përgjigjja e saktë: E vërtetë

SHËNIM PËR MËSUESIN

Kill switch është i aktivizuar si parazgjedhje në aplikacionet desktop.

10 **Pyetja 10**

Përgjigjja e saktë: E vërtetë

SHËNIM PËR MËSUESIN

ExpressVPN operon DNS privat në çdo server.

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

G 1. LIGHTWAY	E 2. TRUSTED SERVER	F 3. BRAVË	A 4. ISHUJT
H 5. AES-256	D 6. I AUDITUAR	B 7. RRJEDHJE	C 8. DNS

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 LIGHTWAY	2 TRUSTED SERVER	3 LOCK	4 ISHUJT E VIRGJËR
5 AES-256	6 AUDITUAR		

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

1 G – RRJEDHJE	2 D – ISHUJTEVIRGJËR	3 H – ZGJIDHËSDNS	4 A – LIGHTWAY
5 C – LOCK	6 E – AES256	7 B – TRUSTEDSERVER	8 F – AUDITUAR

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë LIGHTWAY, TRUSTED SERVER dhe BRAVË 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

A	U	D	I	T	U	A	R	G	Q	Z	R	E	P	U
E	Y	A	A	P	N	L	O	S	X	T	P	I	Q	S
S	A	Q	Ç	L	Y	B	Ë	Q	X	R	V	H	A	Q
N	W	Z	Y	A	Y	J	Ë	G	L	U	P	I	K	K
D	T	K	S	E	N	F	O	P	F	S	Z	A	N	U
S	H	C	Ë	S	T	C	Y	Q	Y	T	B	F	K	Z
Ë	G	O	Ë	2	I	M	O	M	V	E	C	K	Z	Y
H	I	L	Ë	5	Y	N	V	T	J	D	T	O	B	M
D	L	U	S	6	K	F	T	Ç	Y	S	T	I	Q	B
I	V	Z	Y	K	Q	P	X	G	N	E	Ç	A	Ç	I
J	I	S	H	U	J	T	E	V	I	R	G	J	Ë	R
G	P	U	V	V	J	H	G	S	G	V	Ë	B	E	G
Z	J	R	R	J	E	D	H	J	E	E	S	Q	U	P
Z	D	G	E	Q	C	A	J	O	C	R	Z	K	I	U
Q	T	A	R	V	I	K	K	F	F	L	G	P	Ë	J

ZGJIDHJA E FJALËKRYQIT

					T									
					R									
	A				U		Z			L	O	C	K	
	E		A		S		G			I				
I	S	H	U	J	T	E	V	I	R	G	J	Ë	R	
	2		D			D		D		H			R	
	5		I			S		H		T			J	
	6		T			E		Ë		W			E	
			U			R		S		A			D	
			A			V		D		Y			H	
			R			E		N					J	
						R		S					E	

UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

4 horizontalisht: LOCK Fjala e fundit e Network Lock, emrit të mëparshëm të kill switch-it (4 shkronja)

6 horizontalisht: ISHUJTEVIRGJËR Juridiksioni i Ishujve të Virgjër Britanikë, që ofron privatësi të fortë (14 shkronja)

VERTIKALISHT

1 vertikalisht: TRUSTEDSERVER Arkitekturë serverësh vetëm me RAM që parandalon ruajtjen e të dhënave në disk (13 shkronja)

2 vertikalisht: ZGJIDHËSDNS Zgjidhës të Sistemit të Emrave të Domeneve që funksionojnë privatisht në çdo nyje serveri (11 shkronja)

3 vertikalisht: AES256 Standard enkriptimi simetrik që siguron transmetimin e të dhënave (6 shkronja)

4 vertikalisht: LIGHTWAY Protokoll lidhjeje i lehtë dhe me burim të hapur i ExpressVPN (8 shkronja)

5 vertikalisht: AUDITUAR Verifikuar në mënyrë të pavarur nga firma sigurie të palëve të treta (8 shkronja)

7 vertikalisht: RRJEDHJE Ekspozim i paqëllimshëm i të dhënave private IP, DNS ose WebRTC (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.	AHTLWIYG	LIGHTWAY	5.	EVRUSTRERDTES	TRUSTEDSERVER
2.	LCKO	LOCK	6.	TEGJHJVËRISIRU	ISHUJTEVIRGJËR
3.	AS265E	AES256	7.	ARTUAUID	AUDITUAR
4.	EJEHDRRJ	RRJEDHJE	8.	DËSHJZDGNSI	ZGJIDHËSDNS

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"TRUSTEDSERVER FSHIN LOGET E PËRDORUESVE ÇDO DITË"

Çelësi i studimeve të rastit

A STUDIMI I RASTIT 1: ZBATIMI I MBROJTJEVE VETËM ME RAM

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një agjenci qeveritare sekuestron një server ExpressVPN për të nxjerrë regjistra përdoruesish dhe historikun e lidhjeve.
- Strategjia dhe zgjidhja e rekomanduar: Asgjë. Teknologjia TrustedServer e ExpressVPN funksionon tërësisht në RAM, kështu që të gjitha të dhënat fshihen menjëherë kur humbet energjia.

B STUDIMI I RASTIT 2: TUNELET E PAQËNDRUESHME TË LIDHJES WI-FI

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një punëtor në distancë po përdor Wi-Fi publik të hotelit që shkëputet çdo disa minuta ndërsa redakton dokumente.
- Strategjia dhe zgjidhja e rekomanduar: Internet Kill Switch bllokon automatikisht gjithë trafikun e internetit derisa tuneli VPN të rivendoset.