Emri: _____ Data: _____ Pikët: _____

Siguria e ProtonVPN

Analizimi i arkitekturës së sigurisë së ProtonVPN, përfshirë serverët Secure Core, filtrimin DNS NetShield, jurisdiksionin zviceran të privatësisë, aplikacionet me burim të hapur të audituara dhe protokollin Stealth.

PËRMBLEDHJE MËSIMORE PËR SIGURINË E PROTONVPN

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 arkitekturës së sigurisë së Proton VPN. Do të eksplorosh serverët bunker Secure Core, bllokimin DNS NetShield, ligjet zvicerane të privatësisë dhe errësimin Stealth.

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/protonvpn/siguria/

Udhërrëfyesi yt mësimor për sigurinë e ProtonVPN

- Analizo arkitekturën teknike dhe rregullat e konfigurimit të sigurisë së ProtonVPN.
- 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 PROTONVPN

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 rrugëzimin me dy kërcime Secure Core dhe qeverisjen zviceriane të privatësisë. Përfundo me aktivitetin bonus Mendo shpejt.

ARKITEKTURA E DYFISHTË SECURE CORE DHE JURIDIKSIONI ZVICERAN I PRIVATËSISË

Proton VPN e mbron trafikun e përdoruesve me serverë Secure Core në pronësi të Proton në Zvicër, Islandë dhe Suedi, aplikacione me burim të hapur të audituara dhe protokollin e maskimit Stealth të projektuar për të kapërcyer inspektimin e thellë të paketave.

(HYRJE)

Proton VPN e mbron trafikun e përdoruesve me serverë Secure Core në pronësi të Proton në Zvicër, Islandë dhe Suedi, aplikacione me burim të hapur të audituara dhe protokollin e maskimit Stealth të projektuar për të kapërcyer inspektimin e thellë të paketave.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Çfarë lloj objektesh strehojnë serverët Secure Core të Proton?**

- A) VM publike cloud
- B) Vende me siguri të lartë
- C) Qendra publike të dhënash
- D) Raftë të përbashkët

2 **2. Cili protokoll ndihmon të kapërcehet censura e rreptë qeveritare?**

- A) PPTP
- B) Protokolli Stealth
- C) OpenVPN UDP
- D) IKEv2

3 **3. Cili është funksioni i veçorisë NetShield të Proton VPN-së?**

- A) Speed Booster
- B) Bllokim DNS i reklamave dhe malware-it
- C) Ruajtje në cloud
- D) Përcjellja e porteve

4 **4. Sipas ligjeve të privatësisë të cilit shtet vepron Proton AG?**

- A) Shtetet e Bashkuara
- B) Mbretëria e Bashkuar
- C) Zvicra
- D) Panamaja

5 **5. Si verifikohen nga ekspertët aplikacionet klient të Proton VPN?**

- A) Kod sekret
- B) Auditime me burim të hapur
- C) Licencë pronare
- D) Rishikim qeveritar

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

6 Pyetja 6

6. Secure Core e drejton trafikun përmes vendeve miqësore ndaj privatësisë përpara daljes.

○ E vërtetë ○ E gabuar

7 Pyetja 7

7. Zvicra është anëtare e aleancës së survejimit të inteligjencës 14-Eyes.

○ E vërtetë ○ E gabuar

8 Pyetja 8

8. NetShield bllokon reklamat dhe domenet keqdashëse drejtpërdrejt në nivel DNS.

○ E vërtetë ○ E gabuar

9 Pyetja 9

9. Aplikacionet e Proton VPN janë 100% me burim të hapur dhe të audituara publikisht.

○ E vërtetë ○ E gabuar

10 Pyetja 10

10. Protokolli Stealth përdor kokat standarde të WireGuard pa errësim.

○ 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. Rrugëzimi multi-hop përmes serverëve në pronësi të Proton në vende miqësore ndaj privatësisë quhet arkitekturë _____ .

2. Për të mposhtur inspektimin e thellë të paketave dhe firewall-et e rrjetit, përdoruesit aktivizojnë modalitetin _____ .

3. Domenet me malware, gjurmuesit dhe skriptet reklamuese filtrohen nga DNS-ja _____ .

4. Proton thotë se sipas _____ nuk është i detyruar të mbajë regjistra të aktivitetit të përdoruesve.

5. Nëse tuneli VPN shkëputet papritur, trafiku i internetit bllokohet nga mbrojtja _____ .

6. Studiues të pavarur të sigurisë verifikojnë integritetin e klientit sepse aplikacionet janë me kod _____ .

BANKA E FJALËVE TË LEKSIKUT

AES-GCM BURIM I HAPUR KILL SWITCH LIGJ ZVICERAN NETSHIELD SECURE CORE STEALTH WIREGUARD

Shkruaj përgjigjet e tua këtu:

1. **2.**

3. **4.**

5. **6.**

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

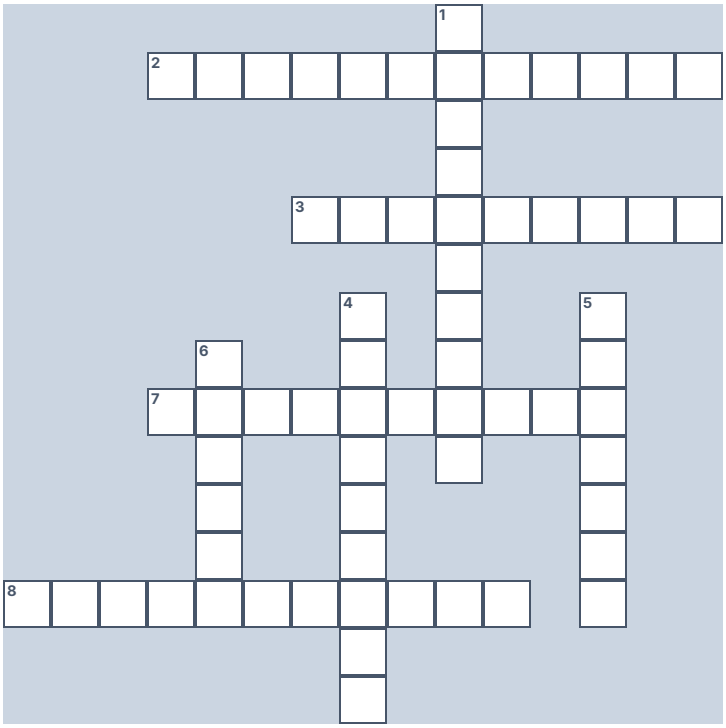
PËRPUTHJA E PËRKUFIZIMEVE

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. SECURE CORE	A	Softuer klienti i aksesueshëm publikisht dhe i audituar në mënyrë të pavarur.
☐	2. STEALTH	B	Standard simetrik shifre që enkripton paketat e të dhënave të VPN-së.
☐	3. NETSHIELD	C	Statute strikte ligjore të privatësisë në Zvicër jashtë juridiksionit 14-Eyes.
☐	4. LIGJ ZVICERAN	D	Një protokoll tunelimi i errësuar, i maskuar si trafik i zakonshëm uebi HTTPS.
☐	5. KILL SWITCH	E	Një protokoll modern i lehtë që ofron kriptografi të fuqishme dhe shpejtësi të larta.
☐	6. BURIM I HAPUR	F	Një filtër i bazuar në DNS që bllokon reklamat, gjurmuesit e telemetrisë dhe malware-in.
☐	7. WIREGUARD	G	Një dizajn multi-hop që e drejton trafikun përmes serverëve të hopit të parë në pronësi të Proton.
☐	8. AES-GCM	H	Një mbrojtje sigurie që ndalon transmetimin e rrjetit gjatë ndërprerjeve të lidhjes.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

2. Statute të rrepta ligjore të privatësisë në Zvicër, jashtë juridiksionit 14-Eyes (12)

3. Filtër i bazuar në DNS që bllokon reklamat, gjurmuesit e telemetrisë dhe malware (9)

7. Dizajn multi-hop që rrugëzon trafikun përmes serverëve të hapit të parë në pronësi të Proton (10)

8. Softuer aplikacioni klient i aksesueshëm publikisht dhe i audituar në mënyrë të pavarur (11)

VERTIKALISHT

1. Mbrojtje sigurie që ndalon transmetimin e rrjetit gjatë ndërprerjeve të lidhjes (10)

4. Protokoll modern i lehtë që ofron kriptografi të fortë dhe shpejtësi të larta (9)

5. Protokoll tunelimi i errësuar, i maskuar si trafik standard uebi HTTPS (7)

6. Shifër simetrike e nivelit ushtarak që siguron të gjitha paketat e të dhënave VPN të kapsuluara (6)

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: Statute të rrepta ligjore të privatësisë në Zvicër, jashtë juridiksionit 14-Eyes (12 shkronja):

3 horizontalisht: Filtër i bazuar në DNS që bllokon reklamat, gjurmuesit e telemetrisë dhe malware (9 shkronja):

7 horizontalisht: Dizajn multi-hop që rrugëzon trafikun përmes serverëve të hapit të parë në pronësi të Proton (10 shkronja):

8 horizontalisht: Softuer aplikacioni klient i aksesueshëm publikisht dhe i audituar në mënyrë të pavarur (11 shkronja):

VERTIKALISHT

1 vertikalisht: Mbrojtje sigurie që ndalon transmetimin e rrjetit gjatë ndërprerjeve të lidhjes (10 shkronja):

4 vertikalisht: Protokoll modern i lehtë që ofron kriptografi të fortë dhe shpejtësi të larta (9 shkronja):

5 vertikalisht: Protokoll tunelimi i errësuar, i maskuar si trafik standard uebi HTTPS (7 shkronja):

6 vertikalisht: Shifër simetrike e nivelit ushtarak që siguron të gjitha paketat e të dhënave VPN të kapsuluara (6 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.

G D Ç Q P K D K G Q Z R E P U

R R E A A P N I L O N S X P I

U A Q S Q Ç L L Y B E Ë Q X V

P U H A A Q Z L Y Y T J Ë G L

A G P I E K K S S N S F O S P

H E F Z S A N W U Ë H T C E Y

I R Q Y G B F I K Z I Ë I C M

M I O M C V C T K Z E Y Ë U Y

I W N V M T J C T O L B M R U

R S K F T Ç Y H T I D Q B E V

U L I G J Z V I C E R A N C Z

B Y K Q P X G N Ç A Ç I P O U

V V S T E A L T H J H G S R G

Ë B E G J S Q U P Z D G E E Q

C A J O C Z K I U Q T A R V I

LISTA E FJALËVE TË LEKSIKUT

SECURECORE STEALTH NETSHIELD LIGJZVICERAN KILLSWITCH

BURIMIHAPUR WIREGUARD AESGCM

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. SECURECORE

B. STEALTH

C. NETSHIELD

D. LIGJZVICERAN

E. KILLSWITCH

F. BURIMIHAPUR

G. WIREGUARD

H. AESGCM

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

_____ 1. Protokoll tunelimi i errësuar, i maskuar si trafik standard uebi HTTPS.

_____ 2. Protokoll modern i lehtë që ofron kriptografi të fortë dhe shpejtësi të larta.

_____ 3. Statute të rrepta ligjore të privatësisë në Zvicër, jashtë juridiksionit 14-Eyes.

_____ 4. Dizajn multi-hop që rrugëzon trafikun përmes serverëve të hapit të parë në pronësi të Proton.

_____ 5. Shifër simetrike e nivelit ushtarak që siguron të gjitha paketat e të dhënave VPN të kapsuluara.

_____ 6. Mbrojtje sigurie që ndalon transmetimin e rrjetit gjatë ndërprerjeve të lidhjes.

_____ 7. Filtër i bazuar në DNS që bllokon reklamat, gjurmuesit e telemetrisë dhe malware.

_____ 8. Softuer aplikacioni klient i aksesueshëm publikisht dhe i audituar në mënyrë të pavarur.

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. RCERESOEUC
2. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. NZERVACLIIGJ
7. AMBUHRPURII
8. SMACGE

Aktivitet bonus: Mendo shpejt

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

1	Gjëra që bën çdo ditë në internet			
2	Vende të njohura për ligje të forta privatësie			
3	Veçori sigurie te Proton VPN			
4	Lloje rrjedhjesh të VPN-së			
5	Situata ku ndihmon një kill switch			
6	Gjëra që mund të kontrollojë një auditim			
7	Cilësime që i aktivizon për siguri shtesë			
8	Gjëra që mbron enkriptimi			
9	Fjalë që përshkruajnë një aplikacion të mirë VPN			
10	Arsye për të zgjedhur Proton VPN			
11	Butona ose menu në një aplikacion VPN			
12	Shërbime transmetimi që shikon			
13	Kërcënime në Wi-Fi publik			
14	Mënyra për të krijuar një fjalëkalim të fortë			
15	Vende ku do të dëshiroje serverë të Proton VPN			

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: ANASHKALIMI I FIREWALL-EVE KUFIZUESE

👷

Skenari: Një përdorues udhëton në një vend ku trafiku standard VPN si OpenVPN dhe WireGuard bllokohet nga DPI.

Pyetje për diskutim: Cili konfigurim i protokollit të Proton VPN e lejon përdoruesin të anashkalojë inspektimin në nivel shtetëror?

STUDIMI I RASTIT 2: MBROJTJA E AVANCUAR NGA KUNDËRSHTARËT

👷

Skenari: Një auditor financiar dyshon se nyja e daljes e ofruesit lokal të internetit mund të jetë kompromentuar nga kërcënime të avancuara të vazhdueshme.

Pyetje për diskutim: Si e mbron Secure Core identitetin e auditorit ndaj kompromentimit të nyjes së daljes?

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

21	6	3	23	20	6		3	17	20	6		15	2	20	17	16		22	7

5	10	7	16	1	22		6		18	7	20	5	17	20	23	6	21	11	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 për Rrjetet Private Virtuale (VPN) dhe tunelimin.

Q1: Çfarë është Proton VPN Secure Core?

Secure Core e drejton trafikun përmes serverëve të shumtë në vende miqësore ndaj privatësisë përpara daljes.

Q2: Çfarë është protokolli Stealth?

Stealth është një protokoll i obfuskuar që i fsheh lidhjet VPN si trafik i zakonshëm TLS/HTTPS.

Q3: Si i mbron përdoruesit NetShield?

NetShield është një mjet i bazuar në DNS që bllokon automatikisht reklamat, gjurmuesit dhe domenet e malware-it.

Q4: A është Proton VPN i mbrojtur ligjërisht në Zvicër?

Po, Zvicra ka ligje të rrepta për privatësinë dhe është jashtë jurisdiksionit të SHBA-së dhe BE-së/14-Eyes. [4]

Q5: A janë aplikacionet e Proton VPN me burim të hapur?

Po. Aplikacionet e Proton VPN janë me kod të hapur dhe kanë kaluar auditime sigurie të publikuara.

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: Cilat shifra enkriptimi përdoren?

Proton VPN përdor AES-256-GCM ose ChaCha20-Poly1305 me handshake-e HMAC-SHA384 dhe RSA-4096.

Q7: A ka Proton VPN një Kill Switch?

Po, Proton VPN përfshin një Kill Switch standard dhe një Permanent Kill Switch për të parandaluar rrjedhjet e paenkriptuara.

Q8: A mund t'i rrjedhë Proton VPN kërkesat DNS?

Jo, të gjitha kërkesat DNS rutohen përmes serverëve privatë të enkriptuar DNS që zotërohen nga Proton.

Q9: A mban Proton VPN regjistra të lidhjeve?

Jo, Proton VPN mban një politikë të rreptë pa regjistra, të konfirmuar nga auditime vjetore Securitum. [3]

Q10: A është Proton VPN i cenueshëm ndaj rrjedhjeve WebRTC?

Jo, klientët Proton përfshijnë rregulla të integruara firewall-i dhe politika rutimi që bllokojnë rrjedhjet WebRTC.

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: Ku ndodhen fizikisht qendrat e të dhënave Secure Core?

Ndodhen në Zvicër, në një ish-bazë ushtarake në Islandë dhe në një vend nëntokësor në Suedi. [1]

Q2: Si funksionon Perfect Forward Secrecy në Proton VPN?

Për çdo sesion gjenerohet një çelës unik enkriptimi kalimtar, duke parandaluar deshifrimin retroaktiv.

Q3: Çfarë është Permanent Kill Switch në Windows/Linux?

Kill Switch i përhershëm bllokon të gjithë trafikun e rrjetit edhe nëse aplikacioni VPN mbyllet plotësisht ose prishet.

Q4: A e mbështet Proton VPN ruterimin IPv6 dhe mbrojtjen nga rrjedhjet?

Proton VPN e rrugëzon plotësisht trafikun IPv6 përmes tuneleve ose e çaktivizon në mënyrë të sigurt për të parandaluar rrjedhjet.

Q5: Si e trajton filtrimi DNS i NetShield inspektimin e HTTPS?

NetShield vepron thjesht në shtresën e zgjidhjes DNS, pa kërkuar deshifrim invaziv TLS.

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: Kush kreu auditimet e kodit nga palë të treta për Proton VPN?

SEC Consult i ka audituar aplikacionet, ndërsa Securitum i ka audituar aplikacionet dhe politikën pa regjistra.

Q7: Si krahasohet protokolli Stealth me OpenVPN XOR ose Shadowsocks?

Stealth e tunelon WireGuard mbi TLS të obfuskuar dhe i tejkalon obfuskimet më të vjetra të bazuara në OpenVPN. [5]

Q8: A mund ta detyrojnë autoritetet zvicerane Proton VPN të regjistrojë trafikun?

Proton thotë se sipas ligjit zviceran nuk është e detyruar të mbajë regjistra të aktivitetit ose të dhënave të përdoruesve.

Q9: Si mbrohen serverët e Proton VPN nga konfiskimi?

Të gjithë serverët e Proton VPN janë makina bare-metal të mbrojtura me enkriptim të plotë të diskut. [2]

Q10: A mbështet Proton VPN konfigurime të personalizuara të serverit DNS?

Po, abonentët me pagesë mund të konfigurojnë serverë të personalizuar upstream DNS drejtpërdrejt te preferencat e aplikacionit.

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

1. Proton i zotëron dhe i instalon vetë serverët e tij Secure Core, në vende me siguri të lartë në Zvicër, Islandë dhe Suedi. [1]

2. PERSPEKTIVË PËR VPN-NË

2. Aplikacionet e klientit të Proton VPN janë me kod të hapur dhe i nënshtrohen auditimeve të përsëritura të kodit nga palë të treta.

3. PERSPEKTIVË PËR VPN-NË

3. Protokolli i errësimit Stealth anashkalon inspektimin e thellë të paketave duke simuluar trafik standard TLS.

4. PERSPEKTIVË PËR VPN-NË

4. Zvicra është jashtë aleancave ndërkombëtare të ndarjes së inteligjencës 5-Eyes, 9-Eyes dhe 14-Eyes. [4]

5. PERSPEKTIVË PËR VPN-NË

5. NetShield vepron në nivelin e zgjidhësit DNS, duke parandaluar reklamat dhe malware-in përpara shkarkimit të ngarkesës.

6. PERSPEKTIVË PËR VPN-NË

6. Perfect Forward Secrecy siguron që çelësat e kompromentuar nuk mund t'i deshifrojnë seancat e trafikut të kapura më parë. [7]

7. NJOHURI PËR VPN-NË

7. Proton VPN përdor enkriptim të plotë të diskut në serverë bare-metal për të mbrojtur konfigurimet e serverëve. [2]

8. NJOHURI PËR VPN-NË

8. Permanent Kill Switch parandalon rrjedhjet e të dhënave të pa enkriptuara edhe gjatë riniseve të sistemit operativ.

9. NJOHURI PËR VPN-NË

9. Securitum ka audituar dhe konfirmuar politikën no-logs të Proton VPN në pesë auditime vjetore të njëpasnjëshme. [3]

10. PERSPEKTIVË PËR VPN-NË

10. Proton VPN u zhvillua nga shkencëtarë që u takuan në CERN (Organizata Evropiane për Kërkime Bërthamore). [4]

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] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

[7] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

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

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

SHËNIM PËR MËSUESIN

Serverët Secure Core ndodhen në vende me siguri të lartë, përfshirë një bazë të mëparshme ushtarake në Islandë dhe një qendër të dhënash nëntokësore në Suedi. [1]

2 **Protokolli i obfuskimit Stealth** MBROJTJA NGA CENZURA — **Përgjigjja e saktë: B**

SHËNIM PËR MËSUESIN

Protokolli Stealth i Proton i maskon lidhjet WireGuard si trafik standard TLS/HTTPS për të kapërcyer firewall-et e Inspektimit të Thellë të Paketave (DPI). Citim: Proton Stealth Protocol Whitepaper.

3 **Bllokuesi i reklamave DNS NetShield** FILTRIMI I DNS — **Përgjigjja e saktë: B**

SHËNIM PËR MËSUESIN

NetShield përdor filtrim në nivel DNS për të bllokuar domenet e malware-it, spyware-in, reklamat ndërhyrëse dhe gjurmuesit e telemetrisë para se të ngarkohen faqet e uebit. Citim: NetShield Security Specs.

4 **Juridiksioni ligjor zviceran** JURIDIKSIONI — **Përgjigjja e saktë: C**

SHËNIM PËR MËSUESIN

Proton AG ka selinë në Gjenevë, Zvicër, duke përfituar nga ligjet e forta zvicerane të privatësisë, jashtë aleancave mbikëqyrëse 14-Eyes të SHBA-së dhe BE-së. Citim: Swiss Federal Data Protection Act.

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

SHËNIM PËR MËSUESIN

Të gjitha aplikacionet e Proton VPN janë me kod të hapur; SEC Consult dhe më vonë Securitum i kanë audituar.

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

6 **Secure Core me shumë juridiksione** ARKITEKTURA E RUTERIMIT — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Secure Core e drejton trafikun përmes juridiksioneve të forcuara për privatësi përpara se të dalë drejt vendit të destinacionit, duke ndihmuar në mbrojtjen nga një server dalës i kompromentuar. Burimi: Secure Core Architecture.

7 **Aleanca zvicerane e survejimit** ALEANCAT E SURVEJIMIT — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Zvicra nuk është anëtare e marrëveshjeve të ndarjes së inteligjencës 5-Eyes, 9-Eyes ose 14-Eyes, duke ruajtur sovranitetin e pavarur ligjor. Burimi: International Surveillance Treaties.

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

SHËNIM PËR MËSUESIN

NetShield përdor serverët DNS të Proton për të kontrolluar domenet kundrejt listave të domeneve të njohura të reklamave, gjurmuesve dhe malware-it.

9 **Auditimi i klientit me burim të hapur** TRANSPARENCA E SIGURISË — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Proton i ka bërë aplikacionet e desktopit dhe të celularit me burim të hapur dhe publikon raporte auditimi nga palë të treta. Citim: SEC Consult Security Report.

10 **Pyetja 10** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: Stealth i tunelon WireGuard brenda TLS-së së obfuskuar mbi TCP, ndaj trafiku duket si HTTPS i zakonshëm.

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. SECURE CORE	D 2. STEALTH	F 3. NETSHIELD	C 4. LIGJ ZVICERAN
H 5. KILL SWITCH	A 6. BURIM I HAPUR	E 7. WIREGUARD	B 8. AES-GCM

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 LIGJ ZVICERAN
5 KILL SWITCH	6 BURIM I HAPUR		

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

1 B – STEALTH	2 G – WIREGUARD	3 D – LIGJZVICERAN	4 A – SECURECORE
5 H – AESGCM	6 E – KILLSWITCH	7 C – NETSHIELD	8 F – BURIMIHAPUR

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë SECURE CORE, STEALTH dhe NETSHIELD 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.

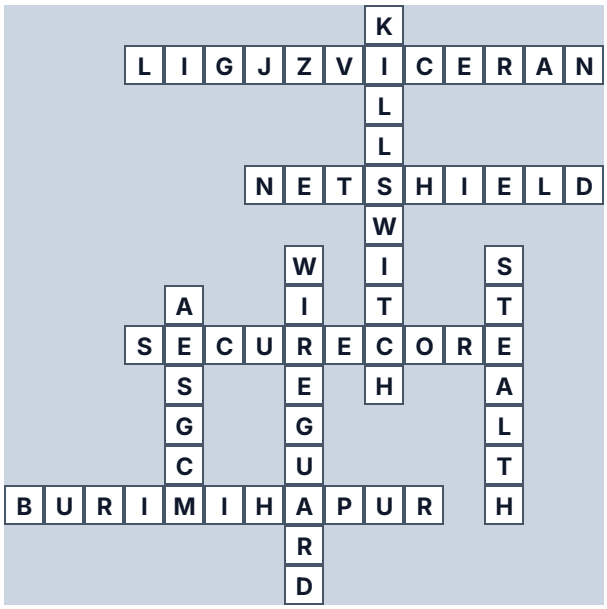
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

2 horizontalisht: LIGJZVICERAN Statute të rrepta ligjore të privatësisë në Zvicër, jashtë juridiksionit 14-Eyes (12 shkronja)

3 horizontalisht: NETSHIELD Filtër i bazuar në DNS që bllokon reklamat, gjurmuesit e telemetrisë dhe malware (9 shkronja)

7 horizontalisht: SECURECORE Dizajn multi-hop që rrugëzon trafikun përmes serverëve të hapit të parë në pronësi të Proton (10 shkronja)

8 horizontalisht: BURIMIHAPUR Softuer aplikacioni klient i aksesueshëm publikisht dhe i audituar në mënyrë të pavarur (11 shkronja)

VERTIKALISHT

1 vertikalisht: KILLSWITCH Mbrojtje sigurie që ndalon transmetimin e rrjetit gjatë ndërprerjeve të lidhjes (10 shkronja)

4 vertikalisht: WIREGUARD Protokoll modern i lehtë që ofron kriptografi të fortë dhe shpejtësi të larta (9 shkronja)

5 vertikalisht: STEALTH Protokoll tunelimi i errësuar, i maskuar si trafik standard uebi HTTPS (7 shkronja)

6 vertikalisht: AESGCM Shifër simetrike e nivelit ushtarak që siguron të gjitha paketat e të dhënave VPN të kapsuluara (6 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. RCERESOEUC — **SECURECORE**
2. DNLSEIEHT — **NETSHIELD**
3. KWCIISHLTL — **KILLSWITCH**
4. GDREAUWIR — **WIREGUARD**
5. LHAESTT — **STEALTH**
6. NZERVACLIIGJ — **LIGJZVICERAN**
7. AMBUHRPURII — **BURIMIHAPUR**
8. SMACGE — **AESGCM**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"SECURE CORE MBRON TË DHËNAT E PËRDORUESIT"

Çelësi i studimeve të rastit

A STUDIMI I RASTIT 1: ANASHKALIMI I FIREWALL-EVE KUFIZUESE

Zgjidhja për mësuesin

RUBRIKË VLERËSIMI DHE UDHËZUES PËR ZGJIDHJET

- Analiza e skenarit: Një përdorues udhëton në një vend ku trafiku standard VPN si OpenVPN dhe WireGuard bllokohet nga DPI.
- Pyetje fokusi: Cili konfigurim i protokollit të Proton VPN i lejon përdoruesit të anashkalojë inspektimin në nivel shteti?
- Strategjia dhe zgjidhja e rekomanduar: Përdoruesi duhet të aktivizojë protokollin Stealth, që i errëson kokat e paketave VPN si trafik i rregullt ueb TLS/HTTPS, duke kaluar filtrat DPI.

B STUDIMI I RASTIT 2: MBROJTJA E AVANCUAR NGA KUNDËRSHTARËT

Zgjidhja për mësuesin

RUBRIKË VLERËSIMI DHE UDHËZUES PËR ZGJIDHJET

- Analiza e skenarit: Një auditor financiar dyshon se nyja e daljes e ISP-së së tij lokale mund të jetë e kompromet uar nga kërcënime të avancuara të vazhdueshme.
- Pyetje fokusi: Si e mbron Secure Core identitetin e auditorit nga kompromentimi i nyjës dalëse?
- Strategjia dhe zgjidhja e rekomanduar: Secure Core e kalon trafikun fillimisht përmes serverëve në pronësi të Proton në Zvicër, Islandë ose Suedi, kështu që një server dalës i kompromet uar nuk mund ta gjurmojë IP-në e përdoruesit.