Emri: _____ Data: _____ Pikët: _____

Siguria e Surfshark

Shqyrtimi i veçorive të sigurisë së Surfshark, përfshirë bllokimin e reklamave CleanWeb, rrugëzimin dinamik MultiHop, arkitekturën SDN Nexus, flotën e serverëve vetëm me RAM dhe modalitetin Camouflage.

PËRMBLEDHJE MËSIMORE: SIGURIA E SURFSHARK

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 Surfshark. Do të eksplorosh harduerin e serverëve vetëm me RAM, rotacionin dinamik të IP-ve me Nexus SDN, bllokuesit e reklamave CleanWeb dhe rrugëzimin MultiHop.

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/surfshark/siguria/

Udhërrëfyesi yt mësimor për sigurinë e Surfshark

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

UDHËZIMET E UDHËZUESIT TË SIGURISË SURFSHARK

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 infrastrukturën vetëm me RAM, Nexus SDN dhe CleanWeb. Përfundo me aktivitetin bonus Mendo shpejt.

FLOTA E SERVERËVE VETËM ME RAM, NEXUS SDN DHE ARKITEKTURA CLEANWEB (HYRJE)

Surfshark mbron privatësinë e përdoruesve me një flotë serverësh vetëm me RAM, rrjet të përcaktuar nga softueri Nexus me IP Rotator, bllokim reklamash CleanWeb dhe shtigje enkriptimi Dynamic MultiHop.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Si quhet bllokuesi i integruar i reklamave dhe malware-it i Surfshark?
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. Cilën arkitekturë harduerike përdor Surfshark në të gjithë serverët?
   - A) Disqe të ngurtë (HDD)
   - B) 100% vetëm me RAM
   - C) Ruajtje optike
   - D) Shirit magnetik

3. Cila veçori e kalon trafikun përmes dy serverëve të ndryshëm VPN?
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) Rrjeti Nexus
   - D) IP statike

4. Cila veçori fshehjeje e maskon trafikun VPN si të dhëna normale web?
   - A) Kill Switch
   - B) Modaliteti i kamuflimit
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. Cili është funksioni i mjetit Surfshark Bypasser?
   - A) Speed Booster
   - B) Split Tunneling
   - C) Menaxheri i fjalëkalimeve
   - D) Zgjidhës DNS

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

6 Pyetja 6

6. Serverët vetëm me RAM i fshijnë të gjitha të dhënat operative menjëherë pas rinisjes së serverit.

- E vërtetë
- E gabuar

7 Pyetja 7

7. Camouflage Mode i pengon ISP-të të zbulojnë se po përdor VPN.

- E vërtetë
- E gabuar

8 Pyetja 8

8. CleanWeb 2.0 vepron brenda zgjerimeve të shfletuesit për të bllokuar dritaret e pëlqimit për cookie.

- E vërtetë
- E gabuar

9 Pyetja 9

9. Surfshark mban vula kohore të përkohshme të lidhjeve dhe regjistra të përdorimit të brezit.

- E vërtetë
- E gabuar

10 Pyetja 10

10. Rrjeti Nexus i rrotullon periodikisht adresat IP të përdoruesve pa u shkëputur.

- 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. Reklamat e bezdisshme, skriptet e gjurmimit dhe lidhjet phishing bllokohen nga filtrat _____ .

2. Aktiviteti i përdoruesit nuk lë gjurmë forenzike sepse serverët funksionojnë me konfigurim _____ .

3. Rrugëzimi i të dhënave përmes dy hapave të veçantë të serverëve të enkriptuar arrihet me tunele _____ .

4. Për të fshehur përdorimin e VPN-së nga ofruesit e shërbimit të internetit, përdoruesit aktivizojnë modalitetin _____ .

5. Lejimi i aplikacioneve bankare të anashkalojnë tunelin VPN menaxhohet nga cilësimet _____ .

6. Arkitektura SDN e gjeneratës së radhës që lidh flotën e serverëve është sistemi _____ .

BANKA E FJALËVE TË LEKSIKUT

BYPASSER | CAMOUFLAGE | CLEANWEB | IP ROTATIVE | KILL SWITCH | MULTI-HOP | NEXUS | VETËM RAM

Shkruaj përgjigjet e tua këtu:

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

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

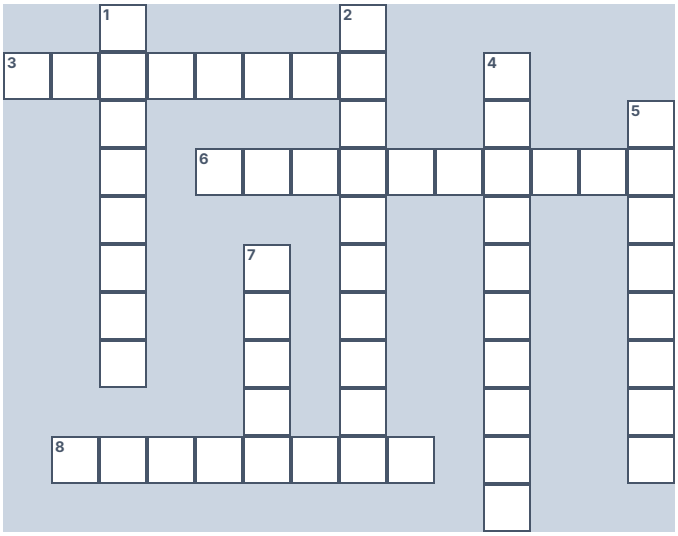
PËRPUTHJA E PËRKUFIZIMEVE

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. CLEANWEB	A	Një veçori automatike sigurie që bllokon trafikun e rrjetit kur VPN-ja bie.
☐	2. VETËM RAM	B	Funksionalitet split-tunneling që lejon aplikacione të zgjedhura të anashkalojnë VPN-në.
☐	3. MULTI-HOP	C	Një filtër i avancuar që bllokon reklamat, malware-in dhe banerat e pëlqimit për cookie.
☐	4. KAMUFLIM	D	Harduer serveri me memorie të paqëndrueshme që fshin të gjitha të dhënat në çdo cikël energjie.
☐	5. ANASHKALUESI	E	Një veçori që ndryshon rregullisht adresën tënde të jashtme IP pa ndërprerë tunelet.
☐	6. KILL SWITCH	F	Teknologji maskimi që fsheh nënshkrimet e VPN-së për të imituar trafikun e zakonshëm HTTPS.
☐	7. RRJETI NEXUS	G	Një veçori drejtimi double-VPN që enkripton trafikun përmes dy nyjeve të ndryshme të serverit.
☐	8. ROTULLIM	H	Një rrjet pronësor i përcaktuar nga softueri që lidh të gjithë serverët në një mesh të unifikuar.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

3. Veçori rrugëzimi me VPN të dyfishtë që enkripton trafikun nëpër dy nyje serveri të dallueshme (8)

6. Teknologji errësimi që fsheh nënshkrimet e VPN-së për të imituar trafikun e zakonshëm HTTPS (10)

8. Funksionalitet split-tunneling që lejon aplikacione të zgjedhura të anashkalojnë VPN-në (8)

VERTIKALISHT

1. Filtër i avancuar që bllokon reklamat, malware dhe banerët e pëlqimit për cookies (8)

2. Veçori që ndryshon rregullisht adresën tënde të jashtme IP pa ndërprerë tunelet (10)

4. Veçori automatike sigurie që bllokon trafikun e rrjetit kur VPN-ja bie (10)

5. Hardware serveri me memorie të paqëndrueshme që fshin të gjitha të dhënat në çdo cikël energjie (8)

7. Rrjet pronësor i përcaktuar nga softueri që lidh të gjithë serverët në një rrjetë të unifikuar (5)

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

3 horizontalisht: Veçori rrugëzimi me VPN të dyfishtë që enkripton trafikun nëpër dy nyje serveri të dallueshme (8 shkronja):

6 horizontalisht: Teknologji errësimi që fsheh nënshkrimet e VPN-së për të imituar trafikun e zakonshëm HTTPS (10 shkronja):

8 horizontalisht: Funksionalitet split-tunneling që lejon aplikacione të zgjedhura të anashkalojnë VPN-në (8 shkronja):

VERTIKALISHT

1 vertikalisht: Filtër i avancuar që bllokon reklamat, malware dhe banerët e pëlqimit për cookies (8 shkronja):

2 vertikalisht: Veçori që ndryshon rregullisht adresën tënde të jashtme IP pa ndërprerë tunelet (10 shkronja):

4 vertikalisht: Veçori automatike sigurie që bllokon trafikun e rrjetit kur VPN-ja bie (10 shkronja):

5 vertikalisht: Hardware serveri me memorie të paqëndrueshme që fshin të gjitha të dhënat në çdo cikël energjie (8 shkronja):

7 vertikalisht: Rrjet pronësor i përcaktuar nga softueri që lidh të gjithë serverët në një rrjetë të unifikuar (5 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.

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

LISTA E FJALËVE TË LEKSIKUT

CLEANWEB VETËMRAM MULTIHOP NEXUS CAMOUFLAGE IPROTATIVE BYPASSER KILLSWITCH

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. CLEANWEB

B. VETËMRAM

C. MULTIHOP

D. CAMOUFLAGE

E. BYPASSER

F. KILLSWITCH

G. NEXUS

H. IPROTATIVE

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

_____ 1. Teknologji errësimi që fsheh nënshkrimet e VPN-së për të imituar trafikun e zakonshëm HTTPS.

_____ 2. Veçori automatike sigurie që bllokon trafikun e rrjetit kur VPN-ja bie.

_____ 3. Filtër i avancuar që bllokon reklamat, malware dhe banerët e pëlqimit për cookies.

_____ 4. Funksionalitet split-tunneling që lejon aplikacione të zgjedhura të anashkalojnë VPN-në.

_____ 5. Hardware serveri me memorie të paqëndrueshme që fshin të gjitha të dhënat në çdo cikël energjie.

_____ 6. Veçori që ndryshon rregullisht adresën tënde të jashtme IP pa ndërprerë tunelet.

_____ 7. Veçori rrugëzimi me VPN të dyfishtë që enkripton trafikun nëpër dy nyje serveri të dallueshme.

_____ 8. Rrjet pronësor i përcaktuar nga softueri që lidh të gjithë serverët në një rrjetë të unifikuar.

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. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. MREMËVAT
6. GUOLACAFEM
7. ILKIWTCHSL
8. VOAEITPTIR

Aktivitet bonus: Mendo shpejt

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

1	Veçori sigurie te Surfshark			
2	Shenja që lidhja jote VPN është e ngadaltë			
3	Protokolle VPN që njeh			
4	Gjëra që mbron enkriptimi			
5	Kërcënime në Wi-Fi publik			
6	Vende të njohura për ligje të forta privatësie			
7	Mënyra për të krijuar një fjalëkalim të fortë			
8	Pajisje ku do ta instaloje Surfshark			
9	Pyetje për mbështetjen e klientëve të Surfshark			
10	Cilësime që i aktivizon për siguri shtesë			
11	Gjëra që Surfshark mund t'i fshehë nga rrjeti yt			
12	Lloje rrjedhjesh të VPN-së			
13	Të dhëna që një VPN nuk duhet t'i ruajë kurrë			
14	Fjalë që përshkruajnë një aplikacion të mirë VPN			
15	Gjëra që mund të kontrollojë një auditim			

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 FILTRAVE TË KAMPUSIT DHE VENDIT TË PUNËS



Skenari: Një student gjen se Wi-Fi-ja e kampusit të universitetit të tij bllokon të gjitha portat standarde OpenVPN dhe WireGuard.

Pyetje për diskutim: Cila veçori e Surfshark i lejon studentit të lidhet pa u zbuluar nga administratorët e rrjetit?

STUDIMI I RASTIT 2: HETIMI GAZETARESK ME RREZIK TË LARTË



Skenari: Një gazetar hetimor ka nevojë për mbrojtje shtesë ndaj survejimit ndërsa kërkon regjistra të ndjeshëm korporativë.

Pyetje për diskutim: Si ofron Dynamic MultiHop privatësi superiore krahasuar me drejtimin përmes një serveri të vetëm?

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	23	20	8	21	10	1	20	13		16	6	25	23	21		5	10	6

11	18		20	17	22	1	22	11	24	6

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 Surfshark CleanWeb?

CleanWeb është një veçori e integruar e sigurisë që bllokon reklamat, gjurmuesit, malware-in dhe faqet e phishing-ut.

Q2: Çfarë janë serverët vetëm me RAM?

Serverët vetëm me RAM funksionojnë në memorie të paqëndrueshme, që do të thotë se të dhënat e mbajtura në memorie fshihen sa herë që serverët riniset.

Q3: Çfarë është Surfshark MultiHop?

MultiHop (Double VPN) e rutuon dhe e enkripton lidhjen tënde të internetit përmes dy vendndodhjeve të ndryshme të serverëve.

Q4: Si funksionon Camouflage Mode?

Camouflage Mode e errëson trafikun VPN, që ISP-ja jote të mos dallojë se po përdor VPN.

Q5: Çfarë është veçoria Bypasser?

Bypasser është mjeti i split tunneling i Surfshark që lejon aplikacione ose faqe interneti të caktuara të anashkalojnë VPN-në.

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 ka Surfshark një Kill Switch?

Po, Kill Switch të shkëput nga interneti nëse VPN-ja bie papritur.

Q7: Çfarë standardi enkriptimi përdor Surfshark?

Surfshark përdor AES-256-GCM dhe ChaCha20, plus AEGIS-256X2 në protokollin e tij të ri Dausos.

Q8: A është audituar politika no-logs e Surfshark?

Po, Deloitte verifikoi politikën e Surfshark pa regjistra në vitin 2023 dhe përsëri në 2025.

Q9: Çfarë është Surfshark Nexus?

Nexus është një arkitekturë e avancuar SDN që i lidh të gjithë serverët në një rrjet të unifikuar për rutim më të qetë.

Q10: Çfarë është funksioni IP Rotator?

IP Rotator ndryshon automatikisht adresën tënde IP çdo disa minuta pa e shkëputur seancën tënde VPN.

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 ndryshon Dynamic MultiHop nga Double VPN tradicional?

Dynamic MultiHop të lejon të personalizosh çdo kombinim serverësh hyrës dhe dalës në mbarë botën.

Q2: A funksionon CleanWeb 2.0 në shtesat e shfletuesit?

Po, CleanWeb 2.0 bllokon reklamat video, dritaret e pëlqimit për cookie dhe banerat e alarmeve brenda Chrome/Firefox.

Q3: Çfarë është Alternative ID në paketën e sigurisë?

Alternative ID gjeneron pseudonime unike personale, adresa emaili dhe maska telefoni.

Q4: Si i parandalon Surfshark rrjedhjet e DNS-së?

Surfshark i rrugëzon të gjitha kërkesat e domeneve përmes serverëve të vet privatë DNS në çdo nyje.

Q5: A e mbështet Surfshark enkriptimin ChaCha20 në celular?

Po, WireGuard në Android dhe iOS përdor ChaCha20-Poly1305 për efikasitet superior në celular.

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: Çfarë është modaliteti NoBorders në Surfshark?

NoBorders zbulon automatikisht mjediset e kufizuara të rrjetit dhe ofron serverë të specializuar.

Q7: Kush i kreu auditimet e sigurisë për shtesat e shfletuesit të Surfshark?

Firma e pavarur e sigurisë kibernetike Cure53 përfundoi auditime në shtesat e shfletuesit dhe në sistemet e serverëve.

Q8: Si mbron Surfshark nga rrjedhjet e IPv6?

Surfshark e rrugëzon trafikun IPv6 në mënyrë të sigurt ose e kufizon me siguri për të parandaluar çdo rrjedhje të paenkriptuar.

Q9: Ku bazohet juridiksioni ligjor i Surfshark?

Surfshark operon sipas ligjit të Holandës, duke respektuar standardet strikte evropiane të privatësisë GDPR.

Q10: A mbështet Surfshark vërtetimin me dy faktorë (2FA)?

Po, dhe Surfshark One shton një bllokim 2FA që vetëm ti të mund të ndryshosh cilësimet e veçorive.

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. Surfshark thotë se e gjithë rrjeti i tij me mbi 4,500 serverë funksionon në harduer të paqëndrueshëm vetëm me RAM, pa disk.

2. PERSPEKTIVË PËR VPN-NË

2. Firma e Katërshes së Madhe Deloitte verifikoi politikën pa regjistrim të Surfshark në 2023 dhe përsëri në nëntor 2025.

3. PERSPEKTIVË PËR VPN-NË

3. Arkitektura pronësore Nexus i lidh të gjithë serverët global në një rrjet dinamik të përcaktuar nga softueri.

4. PERSPEKTIVË PËR VPN-NË

4. IP-ja rrotulluese e ndryshon adresën tënde IP afërsisht çdo pesë minuta pa e ndërprerë lidhjen VPN.

5. PERSPEKTIVË PËR VPN-NË

5. CleanWeb 2.0 bllokon dritaret ndërhyrëse të pëlqimit për cookie dhe reklamat video drejtpërdrejt në shfletues.

6. PERSPEKTIVË PËR VPN-NË

6. Dynamic MultiHop u lejon përdoruesve të krijojnë shtigje të personalizuara enkriptimi me dy serverë nëpër 100 vende.

7. NJOHURI PËR VPN-NË

7. Modaliteti Camouflage heq nënshkrimet e kokës së VPN-së, duke e bërë trafikun të padallueshëm nga HTTPS-ja e zakonshme.

8. NJOHURI PËR VPN-NË

8. Alternative ID gjeneron pseudonime të njëpërdorshme dhe maska emaili për t'i mbrojtur përdoruesit nga rrjedhjet e bazave të të dhënave.

9. NJOHURI PËR VPN-NË

9. Surfshark zbaton enkriptimin simetrik AES-256-GCM krahas ChaCha20 në protokollet WireGuard.

10. PERSPEKTIVË PËR VPN-NË

10. Modaliteti NoBorders aktivizohet automatikisht në rrjetet e kufizuara për të ofruar qasje tunelimi të qëndrueshme.

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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

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

1 **Bllokues i integruar i përmbajtjes** MBROJTJA NGA REKLAMAT DHE MALWARE Përgjigjja e saktë: B

SHËNIM PËR MËSUESIN

CleanWeb është filtri i integruar i sigurisë i Surfshark që bllokon reklamat, domenet e gjurmuesve, faqet e phishing-ut dhe skriptet keqdashëse të URL-ve në nivel rrjeti. Citim: CleanWeb Security Specs.

2 **Infrastrukturë 100% vetëm me RAM** ARKITEKTURA RAM Përgjigjja e saktë: B

SHËNIM PËR MËSUESIN

Surfshark operon serverë vetëm me RAM, ndaj të dhënat e mbajtura në memorien e serverit fshihen kur serveri fiket ose riniset. Burimi: Cure53 Infrastructure Audit.

3 **Tunelim i dyfishtë MultiHop** VPN MULTIHOP Përgjigjja e saktë: B

SHËNIM PËR MËSUESIN

MultiHop (Double VPN) e enkripton trafikun përmes dy nyjeve të veçanta serverësh në vende të ndryshme për të parandaluar sulmet e korrelacionit të trafikut. Citim: Surfshark MultiHop Guide.

4 **Errësimi (obfuscation) me Camouflage Mode** MASKIM Përgjigjja e saktë: B

SHËNIM PËR MËSUESIN

Camouflage Mode modifikon kokat e paketave OpenVPN për ta maskuar trafikun VPN si trafik standard HTTPS, duke anashkaluar bllokimet e firewall-eve kufizuese. Citim: Surfshark Stealth Whitepaper.

5 **Split tunneling Bypasser** TUNELIM I NDARË Përgjigjja e saktë: B

SHËNIM PËR MËSUESIN

Bypasser është mjeti i split tunneling i Surfshark që u lejon përdoruesve të zgjedhin aplikacione ose faqe interneti të caktuara për t'i rrugëzuar drejtpërdrejt përmes lidhjes së tyre të zakonshme me ISP-në. Citim: Surfshark Client Features.

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

6 **Fshirja e të dhënave nga memoria e paqëndrueshme** SIGURIA E SERVERËVE Përgjigjja e saktë: E vërtetë

SHËNIM PËR MËSUESIN

Serverët vetëm me RAM nuk ruajnë asnjë të dhënë në disqe të përhershëm; rinisja e harduerit e pastron menjëherë gjithë memorien operative. Citim: RAM Server Architecture.

7 **Fshehja e ISP-së me Camouflage Mode** FSHEHJA E TRAFIKUT Përgjigjja e saktë: E vërtetë

SHËNIM PËR MËSUESIN

Camouflage Mode heq nënshkrimet e protokollit OpenVPN, duke i penguar ISP-të të zbulojnë se përdoruesi është lidhur me një tunel VPN. Citim: Deep Packet Inspection Guide.

8 **Zgjerimet e shfletuesit CleanWeb 2.0** EKSTENSION SHFLETUESI Përgjigjja e saktë: E vërtetë

SHËNIM PËR MËSUESIN

CleanWeb 2.0 vepron brenda zgjerimeve të shfletuesit për të bllokuar në kohë reale dritaret e pëlqimit për cookie, reklamat video dhe skriptet keqdashëse të ridrejtimit. Citim: CleanWeb 2.0 Release Notes.

9 **Zero ruajtje e regjistrave të lidhjes** POLITIKË PA REGJISTRA Përgjigjja e saktë: E gabuar

SHËNIM PËR MËSUESIN

Surfshark mban një politikë strikte zero-logs të audituar në mënyrë të pavarur, pa regjistruar adresa IP, vula kohore të lidhjeve ose regjistra të brezit. Burimi: Deloitte No-Logs Audit.

10 **Rotacioni dinamik i IP-së Nexus** RRJETI NEXUS Përgjigjja e saktë: E vërtetë

SHËNIM PËR MËSUESIN

Rrjeti i përcaktuar nga softueri Surfshark Nexus i rrotullon në mënyrë dinamike adresat IP të përdoruesve çdo disa minuta, pa e ndërprerë lidhjen aktive të VPN-së. Citim: Surfshark Nexus Architecture.

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

C 1. CLEANWEB	D 2. VETËM RAM	G 3. MULTI-HOP	F 4. KAMUFLIM
B 5. ANASHKALUESI	A 6. KILL SWITCH	H 7. RRJETI NEXUS	E 8. ROTULLIM

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 CLEANWEB	2 VETËM RAM	3 MULTI-HOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

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

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – VETËMRAM	6 H – IPROTATIVE	7 C – MULTIHOP	8 G – NEXUS

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë CLEANWEB, VETËM RAM dhe MULTI-HOP 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.

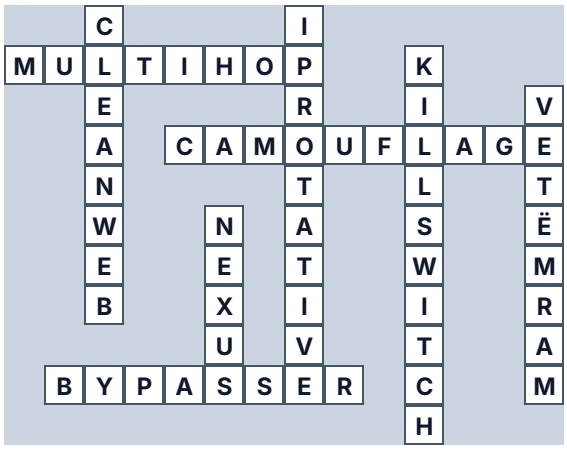
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

3 horizontalisht: MULTIHOP Veçori rrugëzimi me VPN të dyfishtë që enkripton trafikun nëpër dy nyje serveri të dallueshme (8 shkronja)

6 horizontalisht: CAMOUFLAGE Teknologji errësimi që fsheh nënshkrimet e VPN-së për të imituar trafikun e zakonshëm HTTPS (10 shkronja)

8 horizontalisht: BYPASSER Funksionalitet split-tunneling që lejon aplikacione të zgjedhura të anashkalojnë VPN-në (8 shkronja)

VERTIKALISHT

1 vertikalisht: CLEANWEB Filtër i avancuar që bllokon reklamat, malware dhe banerët e pëlqimit për cookies (8 shkronja)

2 vertikalisht: IPROTATIVE Veçori që ndryshon rregullisht adresën tënde të jashtme IP pa ndërprerë tunelet (10 shkronja)

4 vertikalisht: KILLSWITCH Veçori automatike sigurie që bllokon trafikun e rrjetit kur VPN-ja bie (10 shkronja)

5 vertikalisht: VETËMRAM Hardware serveri me memorie të paqëndrueshme që fshin të gjitha të dhënat në çdo cikël energjie (8 shkronja)

7 vertikalisht: NEXUS Rrjet pronësor i përcaktuar nga softueri që lidh të gjithë serverët në një rrjetë të unifikuar (5 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.	EANCWLBE	CLEANWEB	5.	MREMËVAT	VETËMRAM
2.	TMPUOHIL	MULTIHOP	6.	GUOLACAFEM	CAMOUFLAGE
3.	AYBSSREP	BYPASSER	7.	ILKIWTCHSL	KILLSWITCH
4.	XSUNE	NEXUS	8.	VOAEITPTIR	IPROTATIVE

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"SURFSHARK NEXUS DHE IP ROTATIVE"

Çelësi i studimeve të rastit

A STUDIMI I RASTIT 1: ANASHKALIMI I FILTRAVE TË KAMPUSIT DHE VENDIT TË PUNËS

Zgjidhja për mësuesin

RUBRIKË VLERËSIMI DHE UDHËZUES PËR ZGJIDHJET

- Analiza e skenarit: Një student gjen se Wi-Fi i kampusit të universitetit bllokon të gjitha portet standarde OpenVPN dhe WireGuard.
- Pyetje fokusi: Cila veçori e Surfshark i lejon studentit të lidhet pa u zbuluar nga administratorët e rrjetit?
- Strategjia dhe zgjidhja e rekomanduar: Aktivizo Camouflage Mode (OpenVPN), i cili fsheh metadatat e VPN-së që firewall-et të shohin shfletim normal HTTPS.

B STUDIMI I RASTIT 2: HETIMI GAZETARESK ME RREZIK TË LARTË

Zgjidhja për mësuesin

RUBRIKË VLERËSIMI DHE UDHËZUES PËR ZGJIDHJET

- Analiza e skenarit: Një gazetar hetimor ka nevojë për mbrojtje shtesë ndaj survejimit ndërsa heton dokumente të ndjeshme të korporatave.
- Pyetje fokusi: Si ofron Dynamic MultiHop privatësi më të lartë krahasuar me rrugëzimin përmes një serveri të vetëm?
- Strategjia dhe zgjidhja e rekomanduar: MultiHop dinamik e drejton trafikun përmes serverëve hyrës dhe dalës në dy vende, ndaj asnjë server i vetëm nuk mund ta ekspozojë përdoruesin.