Nafn: _____ Dagsetning: _____ Stig: _____

Öryggi Surfshark

Skoðun á öryggiseiginleikum Surfshark, þar á meðal CleanWeb-auglýsingalokun, MultiHop-kvikri leiðarstýringu, Nexus SDN-arkitektúr, þjónaflota eingöngu með vinnsluminni og Camouflage-ham.

YFIRLIT NÁMS UM ÖRYGGI SURFSHARK

NEMANDI
NÁMSMANNASTAÐA
Ferill netverndarsérfræðings

ÖRUGGT
STAÐA TENGINGAR
Að verja gagnapakka

VIRKT
LEKAVÖRN
Vörn gegn DNS- og IPv6-leka

Velkomin! Þetta verkefnahefti leiðir þig í gegnum öryggisarkitektúr Surfshark. Þú kynnist netþjónavélbúnaði með eingöngu vinnsluminni, kvikri IP-skiptingu með Nexus SDN, CleanWeb-auglýsingasíum og MultiHop-leiðarstýringu.

ÁFANGAR VERKEFNABLAÐSINS

- [ ] **Hluti 1-4: Náðu tökum á VPN og öryggisstillingum netkerfa.**
- [ ] **Hluti 5-7: Leystu krossgátur og orðaleitarþrautir.**
- [ ] **Hluti 8-9: Leystu dæmisögur og dulmálsáskorun.**
- [ ] **Hluti 10: Farðu yfir síður með algengum spurningum, grunnstig og framhaldsstig.**
- [ ] **Hluti 11: Kannaðu 10 áhugaverðar staðreyndir úr raunheimum.**
- [ ] **Auka: áskorunin Hugsaðu hratt.**

Opnaðu leiðarvísi VPN.com um bestu VPN-þjónusturnar

URL: https://www.vpn.com/is/vpn/surfshark/oryggi/

Námsvegvísir þinn: öryggi Surfshark

- Greindu tæknilega uppbyggingu og stillingarreglur varðandi öryggi hjá Surfshark.
- Stilltu stillingar biðlara til að koma í veg fyrir leka á IP-tölu, DNS og WebRTC-umferð.
- Berðu saman sérsniðið verð, prufur og afkastaeiginleika við hefðbundin líkön.

LEIÐBEININGAR UM ÖRYGGI SURFSHARK

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á innviði sem nota eingöngu vinnsluminni (RAM), Nexus SDN og CleanWeb. Ljúktu með aukaverkefninu Hugsaðu hratt.

NETÞJÓNAFLOTI EINGÖNGU Í VINNSLUMINNI, NEXUS SDN OG CLEANWEB-UPPBYGGING (INNGANGUR)

Surfshark ver persónuvernd notenda með netþjónaflota sem er eingöngu í vinnsluminni, Nexus hugbúnaðarskilgreindu neti með IP Rotator, CleanWeb-auglýsingalokun og Dynamic MultiHop-dulkóðunarleiðum.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hvað heitir samþætta auglýsinga- og spilliforritablokkun Surfshark?**

- A) AdGuard
- B) CleanWeb
- C) ThreatShield
- D) NetBlocker

2 **2. Hvaða vélbúnaðararkitektúr notar Surfshark á öllum netþjónum?**

- A) Harðir diskar
- B) 100% eingöngu vinnsluminni (RAM)
- C) Sjóngeymsla
- D) Segulband

3 **3. Hvaða eiginleiki beinir umferð í gegnum tvo ólíka VPN-netþjóna?**

- A) Bypasser
- B) MultiHop (tvöfalt VPN)
- C) Nexus-net
- D) Föst IP-tala

4 **4. Hvaða hulningareiginleiki (obfuscation) dular VPN-umferð sem venjuleg vefgögn?**

- A) Kill switch
- B) Felugervi (Camouflage Mode)
- C) CleanWeb 2.0
- D) Skiptigöng

5 **5. Hvert er hlutverk Surfshark Bypasser-tólsins?**

- A) Speed Booster
- B) Split Tunneling
- C) Lykilorðastjóri
- D) DNS-lausnari

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Netþjónar eingöngu í vinnsluminni eyða öllum rekstrargögnum strax við endurræsingu netþjónsins.

○ Satt ○ Ósatt

7 Spurning 7

7. Camouflage Mode kemur í veg fyrir að netþjónustur geti greint að þú notir VPN.

○ Satt ○ Ósatt

8 Spurning 8

8. CleanWeb 2.0 starfar innan vafraviðbóta og lokar á samþykkisglugga fyrir vefkökur.

○ Satt ○ Ósatt

9 Spurning 9

9. Surfshark geymir tímabundna tímastimpla tenginga og annála um bandvíddarnotkun.

○ Satt ○ Ósatt

10 Spurning 10

10. Nexus-netið skiptir reglulega um IP-tölur notenda án þess að aftengjast.

○ Satt ○ Ósatt

Áfangi 3: Lykilhugtök fyllt inn

Lestu hverja setningu hér að neðan og fylltu í eyðuna með réttu hugtaki úr orðabankanum.

1. Hvimleiðar vefauglýsingar, rekjaraforskriftir og vefveiðatenglar eru stöðvaðir af _____ síum.

2. Virkni notenda skilur eftir engin réttarrannsóknarspor því _____ hönnun netþjóna starfar eingöngu í minni.

3. Að beina gögnum um tvö aðskilin dulkóðuð netþjónsstökk fæst með _____ göngum.

4. Til að fela VPN-notkun fyrir netþjónustuveitum virkja notendur _____ ham.

5. Að leyfa bankaforritum að fara framhjá VPN-göngunum er stýrt með _____ stillingum.

6. Næstu kynslóðar SDN-arkitektúrinn sem tengir netþjónaflotann er _____ kerfið.

ORÐABANKI

BYPASSER CAMOUFLAGE CLEANWEB DISKALAUS KILL SWITCH MULTI-HOP NEXUS WIREGUARD

Skrifaðu svörin þín hér:

1. 2.

3. 4.

5. 6.

Áfangi 4: Pörun hugtaka um VPN og net

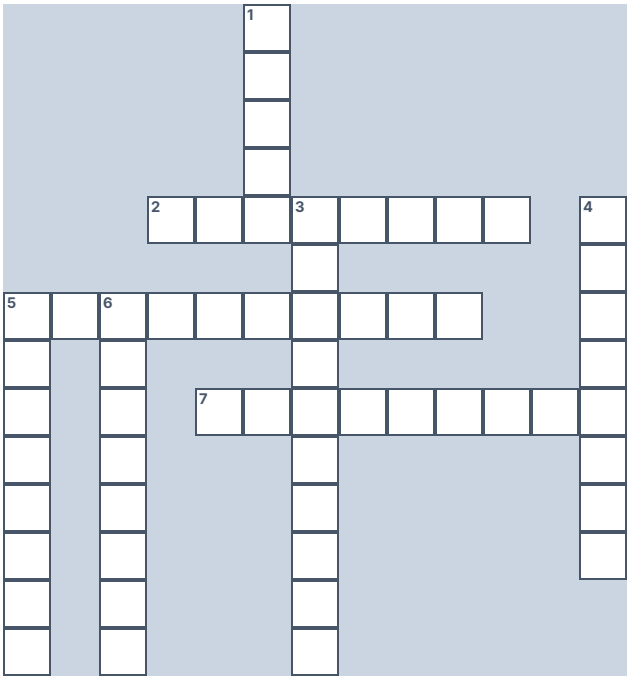
PÖRUN SKILGREININGA

Paraðu hvert hugtak til vinstri við rétta skilgreiningu til hægri með því að skrifa samsvarandi bókstaf (A-H) í útfyllanlega reitinn.

☐	1. CLEANWEB	A	Sjálfvirkur öryggiseiginleiki sem lokar á netumferð þegar VPN dettur út.
☐	2. DISKALAUS	B	Split-tunneling-virkni sem leyfir völdum forritum að sneiða hjá VPN.
☐	3. MULTI-HOP	C	Háþróuð sía sem lokar á auglýsingar, spilliforrit og kökusamþykkisborða.
☐	4. CAMOUFLAGE	D	Netþjónabúnaður með rokgjörnu minni sem eyðir öllum gögnum í hvert sinn sem slökkt er á honum og kveikt aftur.
☐	5. SNIÐGANGARI	E	Eiginleiki sem breytir ytri IP-tölu þinni reglulega án þess að rjúfa göng.
☐	6. KILL SWITCH	F	Dulbúningstækni sem felur VPN-einkenni svo umferðin líkist venjulegri HTTPS-umferð.
☐	7. NEXUS	G	Tvöfalt VPN-leiðarval sem dulkóðar umferð yfir tvo aðskilda netþjóna.
☐	8. SKIPTANDI	H	Hugbúnaðarskilgreint séreignarnet sem tengir alla netþjóna í eitt sameinað möskvanet.

Áfangi 5: Krossgáta

Leystu krossgátuna með því að slá stafi inn í virku hvítu reitina. Tölurnar vísa til vísbendinganna hér að neðan.



LÁRÉTT

2. Eiginleiki sem breytir ytri IP-tölu þinni reglulega án þess að rjúfa göng (8)

5. Hulningartækni sem felur VPN-undirskriftir svo umferðin líki eftir venjulegri HTTPS-umferð (10)

7. Netþjónauppsetning með rokgjörnu minni sem þurrkar öll gögn við hverja endurræsingu (9)

LÓÐRÉTT

1. Sérsmíðað hugbúnaðarskilgreint net sem tengir alla netþjóna í eitt samþætt möskvanet (5)

3. Sjálfvirkur öryggiseiginleiki sem lokar á netumferð þegar VPN fellur (10)

4. Virkni skiptra ganga sem leyfir völdum forritum að fara framhjá VPN (8)

5. Háþróuð sía sem lokar á auglýsingar, spilliforrit og borða um samþykki fyrir vafrakökum (8)

6. Tvöfalt VPN-leiðarval sem dulkóðar umferð yfir tvo ólíka netþjónshnúta (8)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

Notendur skjálesara og lyklaborðs geta slegið svör krossgátunnar beint inn í textareitina hér að neðan.

LÁRÉTT

2 lárétt: Eiginleiki sem breytir ytri IP-tölu þinni reglulega án þess að rjúfa göng (8 stafir):

5 lárétt: Hulningartækni sem felur VPN-undirskriftir svo umferðin líki eftir venjulegri HTTPS-umferð (10 stafir):

7 lárétt: Netþjónauppsetning með rokgjörnu minni sem þurrkar öll gögn við hverja endurræsingu (9 stafir):

LÓÐRÉTT

1 lóðrétt: Sérsmíðað hugbúnaðarskilgreint net sem tengir alla netþjóna í eitt samþætt möskvanet (5 stafir):

3 lóðrétt: Sjálfvirkur öryggiseiginleiki sem lokar á netumferð þegar VPN fellur (10 stafir):

4 lóðrétt: Virkni skiptra ganga sem leyfir völdum forritum að fara framhjá VPN (8 stafir):

5 lóðrétt: Háþróuð sía sem lokar á auglýsingar, spilliforrit og borða um samþykki fyrir vafrakökum (8 stafir):

6 lóðrétt: Tvöfalt VPN-leiðarval sem dulkóðar umferð yfir tvo ólíka netþjónshnúta (8 stafir):

Áfangi 6: Falið orð í orðaleit

Finndu 8 lykilhugtök sem eru falin í reitnum hér að neðan. Orð geta verið lárétt, lóðrétt eða á ská.

Ú	T	U	E	K	Í	B	M	A	Á	B	Ó	Þ	K	J
Þ	K	Ý	Ú	J	Đ	R	U	M	Í	B	Đ	I	N	N
H	K	R	P	G	M	M	L	R	S	Y	T	Ú	Ú	G
C	B	T	P	O	H	T	T	B	Y	P	Đ	U	Æ	V
T	S	D	Ö	Y	C	F	I	J	G	A	Ö	Đ	D	N
I	U	Đ	R	Ý	A	P	H	B	V	S	Á	A	I	Ö
W	X	O	Đ	K	M	A	O	C	Đ	S	O	Đ	S	É
S	E	G	I	Đ	O	S	P	L	I	E	R	M	K	E
L	N	I	T	Ö	U	U	É	E	P	R	R	X	A	É
L	A	A	R	Ó	F	N	P	A	S	Ú	Þ	R	L	J
I	S	Ú	T	D	L	N	Æ	N	K	B	F	T	A	Ý
K	Y	Í	A	S	A	Ö	Æ	W	I	Æ	K	F	U	I
M	S	J	L	L	G	U	Ó	E	P	G	P	R	S	G
Ö	A	O	X	F	E	V	B	B	T	Æ	T	Æ	Á	G
L	Ö	G	J	O	P	N	Ý	B	I	L	Ö	Æ	F	Þ

ORÐALISTI

CLEANWEB DISKALAUS MULTIHOP CAMOUFLAGE BYPASSER KILLSWITCH NEXUS IPSKIPTI

Áfangi 6, valkostur: Aðgengileg orðaforðapörun

Paraðu hvert af hugtökunum 8 úr orðaleitinni við rétta skilgreiningu með því að skrifa bókstafinn (A-H) í eyðuna.

HUGTÖK
A. CLEANWEB
B. DISKALAUS
C. MULTIHOP
D. CAMOUFLAGE
E. BYPASSER
F. KILLSWITCH
G. NEXUS
H. IPSKIPTI

	SKILGREININGAR OG PÖRUNARREITIR
	1. Hulningartækni sem felur VPN-undirskriftir svo umferðin líki eftir venjulegri HTTPS-umferð.
	2. Sjálfvirkur öryggiseiginleiki sem lokar á netumferð þegar VPN fellur.
	3. Háþróuð sía sem lokar á auglýsingar, spilliforrit og borða um samþykki fyrir vafrakökum.
	4. Virkni skiptra ganga sem leyfir völdum forritum að fara framhjá VPN.
	5. Netþjónauppsetning með rokgjörnu minni sem þurrkar öll gögn við hverja endurræsingu.
	6. Eiginleiki sem breytir ytri IP-tölu þinni reglulega án þess að rjúfa göng.
	7. Tvöfalt VPN-leiðarval sem dulkóðar umferð yfir tvo ólíka netþjónshnúta.
	8. Sérsmíðað hugbúnaðarskilgreint net sem tengir alla netþjóna í eitt samþætt möskvanet.

Áfangi 7: Áskorun með ruglaðum orðum

Raðaðu stöfunum hér að neðan í rétta röð til að afhjúpa lykilhugtök um sýndareinkanet (VPN). Skrifaðu svörin þín í reitina sem fylgja.

1. **EANCWLBE** _____
2. **TMPUOHIL** _____
3. **AYBSSREP** _____
4. **XSUNE** _____
5. **AAISLKDUS** _____
6. **GUOLACAFEM** _____
7. **ILKIWTCHSL** _____
8. **KPIIITPS** _____

Aukaverkefni: Hugsaðu hratt

3 SVÖR Í HVERJUM FLOKKI. SÁ VINNUR SEM FYLLIR FYRST ÚT LISTANN.

1	Öryggiseiginleikar í Surfshark			
2	Merki þess að VPN-tengingin þín sé hæg			
3	VPN-samskiptareglur sem þú þekkir			
4	Hlutir sem dulkóðun ver			
5	Ógnir á opinberu Wi-Fi			
6	Lönd sem eru þekkt fyrir sterk persónuverndarlög			
7	Leiðir til að búa til sterkt lykilorð			
8	Tæki sem þú myndir setja Surfshark upp á			
9	Spurningar til þjónustuvers Surfshark			
10	Stillingar sem þú kveikir á fyrir aukið öryggi			
11	Hlutir sem Surfshark getur falið fyrir netinu þínu			
12	Tegundir VPN-leka			
13	Gögn sem VPN ætti aldrei að geyma			
14	Orð sem lýsa góðu VPN-forriti			
15	Hlutir sem úttekt getur kannað			

Áfangi 8: Dæmisögur um VPN og net

Nýttu hugtökin sem þú hefur lært til að leysa raunveruleg dæmi hér að neðan.

DÆMISAGA 1: AÐ SNIÐGANGA SÍUR Í SKÓLUM OG Á VINNUSTÖÐUM

👷

Aðstæður: Nemandi kemst að því að Wi-Fi á háskólasvæðinu lokar á öll venjuleg OpenVPN- og WireGuard-tengi.

Umræðuspurning: Hvaða eiginleiki Surfshark gerir nemandanum kleift að tengjast án þess að netstjórnendur greini það?

DÆMISAGA 2: ÁHÆTTUSÖM BLAÐAMENNSKURANNSÓKN

👷

Aðstæður: Rannsóknarblaðamaður þarf aukna vernd gegn eftirliti meðan hann rannsakar viðkvæm fyrirtækjaskjöl.

Umræðuspurning: Hvernig veitir Dynamic MultiHop betri friðhelgi en leið um einn netþjón?

Áfangi 9: Leystu dulmálið

Netverkfræðingur tryggir leiðarrásir og göng biðlara. Notaðu lykilinn „bókstafur í tölu“ hér að neðan til að afkóða skilaboðin með því að skrifa samsvarandi bókstafi í auðu reitina.

DULMÁLSLYKILL: STAFIR Í TÖLUR

A=1 Á=2 B=3 C=4 D=5 Đ=6 E=7 É=8 F=9 G=10 H=11 I=12

Í=13 J=14 K=15 L=16 M=17 N=18 O=19 Ó=20 P=21 Q=22 R=23 S=24

T=25 U=26 Ú=27 V=28 W=29 X=30 Y=31 Ý=32 Z=33 Þ=34 Æ=35 Ö=36

24	26	23	9	24	11	1	23	15		18	7	30	26	24

24	15	12	21	25	12	23		26	17		12	21		25	36	16	26

18	19	25	7	18	5	1

Afkóðuð skilaboð:

ÁBENDING: HVER TALA STENDUR FYRIR STÖÐU STAFSINS Í STAFRÓFINU (T.D. 1 = A, 2 = B, 36 = Ö).

Áfangi 10: Algengar spurningar um VPN – grunnstig (Hluti A)

Farðu yfir algengustu spurningar og svör um sýndareinkanet (VPN) og göng.

Q1: Hvað er Surfshark CleanWeb?

CleanWeb er innbyggður öryggiseiginleiki sem lokar á auglýsingar, rekjara, spilliforrit og vefveiðasíður.

Q2: Hvað eru netþjónar sem nota eingöngu vinnsluminni?

Netþjónar eingöngu í vinnsluminni keyra á rokgjörnu minni, sem þýðir að gögn í minni þurrkast út í hvert sinn sem netþjónar eru endurræstir.

Q3: Hvað er Surfshark MultiHop?

MultiHop (Double VPN) beinir og dulkóðar netsambandið þitt í gegnum tvær ólíkar netþjónastaðsetningar.

Q4: Hvernig virkar Camouflage Mode?

Camouflage Mode dulbýr VPN-umferð þannig að netþjónustan þín geti ekki séð að þú notir VPN.

Q5: Hvað er Bypasser-eiginleikinn?

Bypasser er split-tunneling-tól Surfshark sem gerir tilteknum forritum eða vefsvæðum kleift að sniðganga VPN.

Áfangi 10: Algengar spurningar um VPN – grunnstig (Hluti B)

Farðu yfir algengustu spurningar og svör um sýndareinkanet (VPN) og göng.

Q6: Er Surfshark með Kill Switch?

Já, Kill Switch aftengir þig frá netinu ef VPN rofnar óvænt.

Q7: Hvaða dulkóðunarstaðal notar Surfshark?

Surfshark notar AES-256-GCM og ChaCha20, auk AEGIS-256X2 á nýju Dausos-samskiptareglunni.

Q8: Hefur stefna Surfshark um að engar skrár séu haldnar verið úttekin?

Já, Deloitte staðfesti stefnu Surfshark um enga annála árið 2023 og aftur árið 2025.

Q9: Hvað er Surfshark Nexus?

Nexus er háþróaður SDN-arkitektúr sem tengir alla netþjóna í eina netheild fyrir mýkra leiðarval.

Q10: Hvað er IP Rotator-eiginleikinn?

IP Rotator breytir IP-tölunni þinni sjálfkrafa á nokkurra mínútna fresti án þess að rjúfa VPN-lotuna.

Áfangi 10: Algengar spurningar um VPN – framhaldsstig (Hluti C)

Kannaðu ítarlega tæknilega þætti VPN-göngusamskiptareglna, samþættingar við farsímabiðlara og uppsetningar í fyrirtækjum.

Q1: Í hverju er Dynamic MultiHop frábrugðið hefðbundnu tvöföldu VPN?

Dynamic MultiHop gerir þér kleift að sérsníða hvaða samsetningu inngangs- og útgangsþjóna sem er um allan heim.

Q2: Virkar CleanWeb 2.0 í vafraviðbótum?

Já, CleanWeb 2.0 lokar á myndbandsauglýsingar, samþykkisglugga fyrir vafrakökur og tilkynningaborða í Chrome/Firefox.

Q3: Hvað er Alternative ID í öryggispakkanum?

Alternative ID býr til einkvæm persónuleg gervinöfn, netföng og símagrímur.

Q4: Hvernig kemur Surfshark í veg fyrir DNS-leka?

Surfshark beinir öllum lénabeiðnum um eigin einka-DNS-netþjóna á hverjum hnút.

Q5: Styður Surfshark ChaCha20-dulkóðun í farsímum?

Já, WireGuard á Android og iOS notar ChaCha20-Poly1305 fyrir framúrskarandi skilvirkni í farsímum.

Áfangi 10: Algengar spurningar um VPN – framhaldsstig (Hluti D)

Kannaðu ítarlega tæknilega þætti VPN-göngusamskiptareglna, samþættingar við farsímabiðlara og uppsetningar í fyrirtækjum.

Q6: Hvað er NoBorders-stillingin í Surfshark?

NoBorders greinir sjálfkrafa takmarkandi netumhverfi og útvegar sérhæfða netþjóna.

Q7: Hver framkvæmdi öryggisúttektir á vafraviðbótum Surfshark?

Óháða netöryggisfyrirtækið Cure53 lauk úttektum á vafraviðbótum og netþjónakerfum.

Q8: Hvernig ver Surfshark gegn IPv6-leka?

Surfshark beinir IPv6-umferð á öruggan hátt eða takmarkar hana á öruggan hátt til að koma í veg fyrir ódulkóðaðan leka.

Q9: Hvar er lögsagnarumdæmi Surfshark?

Surfshark starfar samkvæmt hollenskum lögum og fylgir ströngum evrópskum persónuverndarstöðlum GDPR.

Q10: Styður Surfshark tveggja þátta auðkenningu (2FA)?

Já, og Surfshark One bætir við 2FA-læsingu svo að aðeins þú getir breytt stillingum eiginleika.

Hluti 11: 10 staðreyndir um VPN og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um dulkóðunarhraða VPN, úttektir á samskiptareglum, farsímatengingar og fjarvinnu í fyrirtækjum.

1. INNSÝN Í VPN

1. Surfshark segir að allt net þess með yfir 4.500 netþjónum keyri á diskalausum og rokgjörnum vinnsluminnisbúnaði.

2. INNSÝN Í VPN

2. Fjórmenningarnir stóru, Deloitte, staðfestu stefnu Surfshark um enga skráningu árið 2023 og aftur í nóvember 2025.

3. INNSÝN Í VPN

3. Séreigna Nexus-arkitektúrinn tengir alla netþjóna um allan heim í kvikt hugbúnaðarskilgreint net.

4. INNSÝN Í VPN

4. Rotating IP breytir IP-tölu þinni á um það bil fimm mínútna fresti án þess að slíta VPN-tengingunni.

5. INNSÝN Í VPN

5. CleanWeb 2.0 lokar á uppáþrengjandi sprettiglugga um vefkökusamþykki og myndbandsauglýsingar beint í vöfrum.

6. INNSÝN Í VPN

6. Dynamic MultiHop gerir notendum kleift að búa til sérsniðnar tveggja netþjóna dulkóðunarleiðir í 100 löndum.

7. VPN-INNSÝN

7. Felustilling fjarlægir VPN-haussundirskriftir svo umferðin verður óaðgreinanleg frá venjulegu HTTPS.

8. VPN-INNSÝN

8. Alternative ID býr til einnota gervinöfn og tölvupóstgrímur til að vernda notendur gegn gagnaleka.

9. VPN-INNSÝN

9. Surfshark notar AES-256-GCM samhverfa dulkóðun ásamt ChaCha20 í WireGuard-samskiptareglum.

10. INNSÝN Í VPN

10. NoBorders-stilling virkjast sjálfkrafa á takmörkuðum netum til að veita seigan göngaaðgang.

Tæknilegar heimildir og tilvísanir

Námsleiðbeiningarnar og gagnvirku þrautirnar eru unnar úr alþjóðlegum tæknistöðlum, forskriftum og regluverki.

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[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

Lausnir: Áfangi 1 – Fjölval

1 **Innbyggður efnislokari** VÖRN GEGN AUGLÝSINGUM OG SPILLIFORRITUM **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

CleanWeb er innbyggð öryggissía Surfshark sem lokar á auglýsingar, rekjaralén, vefveiðasíður og skaðlegar slóðarskriftur á netstigi. Heimild: CleanWeb Security Specs.

2 **100% innviðir eingöngu í vinnsluminni** UPPBYGGING VINNSLUMINNIS **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

Surfshark rekur netþjóna eingöngu í vinnsluminni, svo gögn í minni netþjóns eru þurrkuð út þegar slökkt er á honum eða hann endurræstur. Heimild: Cure53 Infrastructure Audit.

3 **MultiHop tvöföld göng** MULTIHOP VPN **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

MultiHop (Double VPN) dulkóðar umferð í gegnum tvo ólíka netþjónahnúta í sitt hvoru landinu til að koma í veg fyrir fylgniárásir á umferð. Heimild: Surfshark MultiHop Guide.

4 **Camouflage Mode: dulbúningur umferðar** DULBÚNINGUR **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

Camouflage Mode breytir hausum OpenVPN-pakka til að láta VPN-umferð líta út eins og venjulega HTTPS-umferð og sniðgengur þannig strangar lokanir eldveggja. Heimild: Surfshark Stealth Whitepaper.

5 **Bypasser Split Tunneling** SKIPTING GANGA **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

Bypasser er split-tunneling-tól Surfshark sem leyfir notendum að velja tiltekin forrit eða vefsvæði til að beina beint í gegnum venjulega tengingu netþjónustuveitu sinnar. Heimild: Surfshark Client Features.

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Eyðing gagna í rokgjörnu minni** ÖRYGGI NETÞJÓNA — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Netþjónar eingöngu í vinnsluminni geyma engin gögn á varanlegum hörðum diskum; endurræsing búnaðarins hreinsar strax allt rekstrarminni. Heimild: RAM Server Architecture.

7 **Camouflage Mode: dulning gagnvart netþjónustu** FELA UMFERÐ — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Camouflage Mode fjarlægir einkenni OpenVPN-samskiptareglunnar og kemur í veg fyrir að netþjónustur greini að notandinn sé tengdur við VPN-göng. Heimild: Deep Packet Inspection Guide.

8 **CleanWeb 2.0-vafraviðbætur** VAFRAVIÐBÓT — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

CleanWeb 2.0 starfar innan vafraviðbóta og lokar í rauntíma á samþykkisglugga fyrir vefkökur, myndbandsauglýsingar og skaðleg endurbeiningarskriftur. Heimild: CleanWeb 2.0 Release Notes.

9 **Engin geymsla tengiskráa** STEFNA UM ENGA SKRÁNINGU — **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Surfshark heldur uppi strangri stefnu um enga skráningu sem er óháð úttekin og skráir engar IP-tölur, tímastimpla tenginga eða bandvíddarannála. Heimild: Deloitte No-Logs Audit.

10 **Kvik IP-skipti í Nexus** NEXUS-NET — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Surfshark Nexus hugbúnaðarskilgreinda netið skiptir kvikt um IP-tölur notenda á nokkurra mínútna fresti án þess að rjúfa virku VPN-tenginguna. Heimild: Surfshark Nexus Architecture.

Orðalyklar og matskvarði

Einkunnaviðmið kennara: Gefðu 1 stig fyrir hverja rétta pörun (alls 8 stig) og hvert samhengishugtak (alls 6 stig).

ÁFANGI 4: LAUSNIR – PÖRUN HUGTAKA

C 1. CLEANWEB	D 2. DISKALAUS	G 3. MULTI-HOP	F 4. CAMOUFLAGE
B 5. SNIÐGANGARI	A 6. KILL SWITCH	H 7. NEXUS	E 8. SKIPTANDI

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

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

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

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

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt CLEANWEB, DISKALAUS og MULTI-HOP með eigin orðum og gefið dæmi um hvert hugtak.

Dæmisögur:
Biddu nemendur að styðja tillögur sínar með staðreyndum úr verkefnablaðinu en ekki ágiskunum.

Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

Ú	T	U	E	K	Í	B	M	A	Á	B	Ó	Þ	K	J
Þ	K	Ý	Ú	J	Đ	R	U	M	Í	B	Đ	I	N	N
H	K	R	P	G	M	M	L	R	S	Y	T	Ú	Ú	G
C	B	T	P	O	H	T	T	B	Y	P	Đ	U	Æ	V
T	S	D	Ö	Y	C	F	I	J	G	A	Ö	Đ	D	N
I	U	Đ	R	Ý	A	P	H	B	V	S	Á	A	I	Ö
W	X	O	Đ	K	M	A	O	C	Đ	S	O	Đ	S	É
S	E	G	I	Đ	O	S	P	L	I	E	R	M	K	E
L	N	I	T	Ö	U	U	É	E	P	R	R	X	A	É
L	A	A	R	Ó	F	N	P	A	S	Ú	Þ	R	L	J
I	S	Ú	T	D	L	N	Æ	N	K	B	F	T	A	Ý
K	Y	Í	A	S	A	Ö	Æ	W	I	Æ	K	F	U	I
M	S	J	L	L	G	U	Ó	E	P	G	P	R	S	G
Ö	A	O	X	F	E	V	B	B	T	Æ	T	Æ	Á	G
L	Ö	G	J	O	P	N	Ý	B	I	L	Ö	Æ	F	Þ

LAUSN KROSSGÁTUNNAR

					N									
					E									
					X									
					U									
			I	P	S	K	I	P	T	I			B	
						I							Y	
C	A	M	O	U	F	L	A	G	E				P	
L		U				L							A	
E		L		D	I	S	K	A	L	A	U		S	
A		T				W							S	
N		I				I							E	
W		H				T							R	
E		O				C								
B		P				H								

LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

2 lárétt: IPSKIPTI Eiginleiki sem breytir ytri IP-tölu þinni reglulega án þess að rjúfa göng (8 stafir)

5 lárétt: CAMOUFLAGE Hulningartækni sem felur VPN-undirskriftir svo umferðin líki eftir venjulegri HTTPS-umferð (10 stafir)

7 lárétt: DISKALAUS Netþjónauppsetning með rokgjörnu minni sem þurrkar öll gögn við hverja endurræsingu (9 stafir)

LÓÐRÉTT

1 lóðrétt: NEXUS Sérsmíðað hugbúnaðarskilgreint net sem tengir alla netþjóna í eitt samþætt möskvanet (5 stafir)

3 lóðrétt: KILLSWITCH Sjálfvirkur öryggiseiginleiki sem lokar á netumferð þegar VPN fellur (10 stafir)

4 lóðrétt: BYPASSER Virkni skiptra ganga sem leyfir völdum forritum að fara framhjá VPN (8 stafir)

5 lóðrétt: CLEANWEB Háþróuð sía sem lokar á auglýsingar, spilliforrit og borða um samþykki fyrir vafrakökum (8 stafir)

6 lóðrétt: MULTIHOP Tvöfalt VPN-leiðarval sem dulkóðar umferð yfir tvo ólíka netþjónshnúta (8 stafir)

Lausnir: Stafaruglingur og dulmál

Lausnalykill fyrir virkni um að raða orðaforða og Secret Cipher Challenge.

LYKILL ORÐARAÐAR

1. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. A A I S L K D U S — **DISKALAUS**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. K P I I I T P S — **IPSKIPTI**

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"SURFSHARK NEXUS SKIPTIR UM IP TÖLU NOTENDA"

Lausnir dæmisagna

A DÆMISAGA 1: AÐ SNIÐGANGA SÍUR Í SKÓLUM OG Á VINNUSTÖÐUM

Lausn fyrir kennara

EINKUNNAGJÖF OG LEIÐBEININGAR UM LAUSNIR

- Greining aðstæðna: Nemandi kemst að því að Wi-Fi háskólasvæðis hans lokar á allar venjulegar OpenVPN- og WireGuard-gáttir.
- Lykilspurning: Hvaða eiginleiki Surfshark gerir nemandanum kleift að tengjast án þess að netstjórar greini það?
- Ráðlögð aðferð og lausn: Virkjaðu Camouflage Mode (OpenVPN), sem felur lýsigögn VPN svo eldveggir sjái venjulega HTTPS-vafrun.

B DÆMISAGA 2: ÁHÆTTUSÖM BLAÐAMENNSKURANNSÓKN

Lausn fyrir kennara

EINKUNNAGJÖF OG LEIÐBEININGAR UM LAUSNIR

- Aðstæður til greiningar: Rannsóknarblaðamaður þarf aukna vernd gegn eftirliti meðan hann rannsakar viðkvæm fyrirtækjagögn.
- Lykilspurning: Hvernig veitir Dynamic MultiHop betra næði en leiðing um einn netþjón?
- Ráðlögð aðferð og lausn: Dynamic MultiHop beinir umferð um inn- og útgönguþjóna í tveimur löndum, þannig að enginn einn netþjónn getur afhjúpað notandann.