Nafn: _____ Dagsetning: _____ Stig: _____

Öryggi ProtonVPN

Greining á öryggisarkitektúr ProtonVPN, þar á meðal Secure Core-netþjónum, NetShield DNS-síun, svissneskri persónuverndarlögsögu, endurskoðuðum forritum með opnum frumkóða og Stealth-samskiptareglu.

YFIRLIT UM NÁMSEFNI: ÖRYGGI PROTONVPN

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 Proton VPN. Þú kynnist Secure Core-byrgisnetþjónum, DNS-lokun NetShield, svissneskum persónuverndarlögum og Stealth-dulbúningi.

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/protonvpn/oryggi/

Námsvegvísir þinn: öryggi ProtonVPN

- Greindu tæknilega uppbyggingu og stillingarreglur varðandi öryggi hjá ProtonVPN.
- 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 PROTONVPN

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á Secure Core-tvöfalt hopp í leiðarvali og svissneska persónuverndarstjórnsýslu. Ljúktu með aukaverkefninu Hugsaðu hratt.

SECURE CORE TVÖFALDUR HOPPARKITEKTÚR OG SVISSNESK PERSÓNUVERNDARLÖGSAGA

Proton VPN ver umferð notenda með Secure Core-netþjónum í eigu Proton í Sviss, á Íslandi og í Svíþjóð, forritum með opnum kóða og óháðum úttektum, og Stealth-dulbúningssamskiptareglunum sem eru hannaðar til að komast framhjá djúpri pakkaskoðun.

(INNGANGUR)

Proton VPN ver umferð notenda með Secure Core-netþjónum í eigu Proton í Sviss, á Íslandi og í Svíþjóð, forritum með opnum kóða og óháðum úttektum, og Stealth-dulbúningssamskiptareglunum sem eru hannaðar til að komast framhjá djúpri pakkaskoðun.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hvers konar aðstaða hýsir Secure Core netþjóna Proton?**

- A) Sýndarvélar í opinberu skýi
- B) Staðir með mikla öryggisgæslu
- C) Opinberar gagnaver
- D) Sameiginlegir rekkar

2 **2. Hvaða samskiptareglur hjálpa til við að komast framhjá strangri ríkisritskoðun?**

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

3 **3. Hvert er hlutverk NetShield-eiginleika Proton VPN?**

- A) Speed Booster
- B) DNS-blokkun auglýsinga og spilliforrita
- C) Skýjageymsla
- D) Portaframsending

4 **4. Undir hvaða lands persónuverndarlögum starfar Proton AG?**

- A) Bandaríkin
- B) Bretland
- C) Sviss
- D) Panama

5 **5. Hvernig staðfesta sérfræðingar VPN-biðlaraforrit Proton?**

- A) Leynikóði
- B) Úttektir á opnum hugbúnaði
- C) Séreignarleyfi
- D) Opinber yfirferð

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Secure Core beinir umferð um lönd sem eru vinsamleg persónuvernd áður en hún fer út.

○ Satt ○ Ósatt

7 Spurning 7

7. Sviss er aðili að leyniþjónustueftirlitsbandalaginu 14 Eyes.

○ Satt ○ Ósatt

8 Spurning 8

8. NetShield lokar á auglýsingar og skaðleg lén beint á DNS-stigi.

○ Satt ○ Ósatt

9 Spurning 9

9. Proton VPN-forrit eru 100% með opnum kóða og undir opinberri úttekt.

○ Satt ○ Ósatt

10 Spurning 10

10. Stealth-samskiptareglan notar hefðbundna WireGuard-hausa án dulbúnings.

○ Satt ○ Ósatt

Áfangi 3: Lykilhugtök fyllt inn

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

1. Fjölstökksleiðarval um netþjóna í eigu Proton í löndum sem eru vinsamleg friðhelgi kallast _____ arkitektúr.

2. Til að sigrast á djúpri pakkaskoðun og netveggjum virkja notendur _____ ham.

3. Lén með spilliforritum, rekjarar og auglýsingaforskriftir eru síuð með _____ DNS.

4. Proton segir að því sé ekki skylt að halda skrár um virkni notenda, þar sem í gildi eru _____ .

5. Ef VPN-göngin rofna óvænt er netumferð stöðvuð af _____ vörninni.

6. Óháðir öryggisrannsakendur staðfesta heilleika biðlara því forritin eru gefin út sem _____ .

ORÐABANKI

AES-GCM | KILL SWITCH | NETSHIELD | OPINN KÓÐI | SECURE CORE | STEALTH | SVISSNESK LÖG | WIREGUARD

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um VPN og net

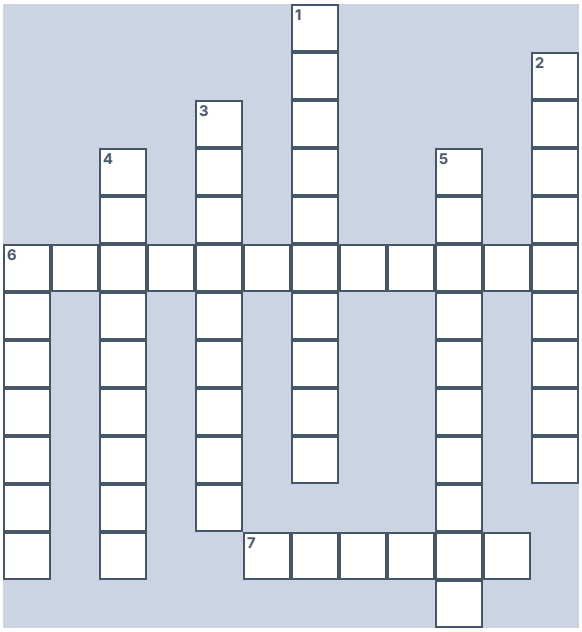
PÖRUN SKILGREININGA

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

☐	1. SECURE CORE	A	Opinberlega aðgengilegur biðlarahugbúnaður sem er undir óháðri úttekt.
☐	2. STEALTH	B	Samhverfur dulmálsstaðall sem dulkóðar gagnapakka VPN.
☐	3. NETSHIELD	C	Strangar svissneskar persónuverndarreglur utan lögsagnarumdæma 14 Eyes.
☐	4. SVISSNESK LÖG	D	Dulbúin göngusamskiptaregla sem er dulbúin sem venjuleg HTTPS-vefumferð.
☐	5. KILL SWITCH	E	Nútímaleg, létt samskiptaregla sem veitir öfluga dulritun og mikinn hraða.
☐	6. OPINN KÓÐI	F	DNS-byggð sía sem lokar á auglýsingar, rakningarbúnað og spilliforrit.
☐	7. WIREGUARD	G	Fjölstökkshönnun sem leiðir umferð í gegnum fyrstu stökksnetþjóna í eigu Proton.
☐	8. AES-GCM	H	Öryggisvörn sem stöðvar netsendingar þegar tenging rofnar.

Áfangi 5: Krossgáta

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



LÁRÉTT

6. Ströng lagaákvæði um friðhelgi í Sviss utan lögsögu 14-Eyes (12)

7. Hernaðargráðu samhverft dulmál sem ver alla hjúpaða VPN-gagnapakka (6)

LÓÐRÉTT

1. Fjölstökkshönnun sem beinir umferð um fyrstu stökk netþjóna í eigu Proton (10)

2. Nútímaleg og létt samskiptaregla með öflugri dulritun og miklum hraða (9)

3. DNS-byggð sía sem lokar á auglýsingar, mælingarrekjara og spilliforrit (9)

4. Opinberlega aðgengilegur og óháð ryndur hugbúnaður biðlaraforrita (9)

5. Öryggisbúnaður sem stöðvar netflutning þegar tenging fellur (10)

6. Dulin göngusamskiptaregla sem dulbýr sig sem venjulega HTTPS-vefumferð (7)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

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

LÁRÉTT

6 lárétt: Ströng lagaákvæði um friðhelgi í Sviss utan lögsögu 14-Eyes (12 stafir):

7 lárétt: Hernaðargráðu samhverft dulmál sem ver alla hjúpaða VPN-gagnapakka (6 stafir):

LÓÐRÉTT

1 lóðrétt: Fjölstökkshönnun sem beinir umferð um fyrstu stökk netþjóna í eigu Proton (10 stafir):

2 lóðrétt: Nútímaleg og létt samskiptaregla með öflugri dulritun og miklum hraða (9 stafir):

3 lóðrétt: DNS-byggð sía sem lokar á auglýsingar, mælingarrekjara og spilliforrit (9 stafir):

4 lóðrétt: Opinberlega aðgengilegur og óháð rýndur hugbúnaður biðlaraforrita (9 stafir):

5 lóðrétt: Öryggisbúnaður sem stöðvar netflutning þegar tenging fellur (10 stafir):

6 lóðrétt: Dulin göngusamskiptaregla sem dulbýr sig sem venjulega HTTPS-vefumferð (7 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.

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

ORÐALISTI

SECURECORE STEALTH NETSHIELD SVISSNESKLÖG KILLSWITCH OPINNKÓÐI WIREGUARD AESGCM

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. SECURECORE
B. STEALTH
C. NETSHIELD
D. SVISSNESKLÖG
E. KILLSWITCH
F. OPINNKÓÐI
G. WIREGUARD
H. AESGCM

SKILGREININGAR OG PÖRUNARREITIR

1. Dulin göngusamskiptaregla sem dulbýr sig sem venjulega HTTPS-vefumferð.
2. Nútímaleg og létt samskiptaregla með öflugri dulritun og miklum hraða.
3. Ströng lagaákvæði um friðhelgi í Sviss utan lögsögu 14-Eyes.
4. Fjölstökkshönnun sem beinir umferð um fyrstu stökk netþjóna í eigu Proton.
5. Hernaðargráðu samhverft dulmál sem ver alla hjúpaða VPN-gagnapakka.
6. Öryggisbúnaður sem stöðvar netflutning þegar tenging fellur.
7. DNS-byggð sía sem lokar á auglýsingar, mælingarrekjara og spilliforrit.
8. Opinberlega aðgengilegur og óháð rýndur hugbúnaður biðlaraforrita.

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. **RCERESOEUC** _____
2. **DNLSEIEHT** _____
3. **KWCIISHLTL** _____
4. **GDREAUWIR** _____
5. **LHAESTT** _____
6. **GSKLNÖSSVEIS** _____
7. **KOÐIÓNPNI** _____
8. **SMACGE** _____

Aukaverkefni: Hugsaðu hratt

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

1	Hlutir sem þú gerir á netinu á hverjum degi			
2	Lönd sem eru þekkt fyrir sterk persónuverndarlög			
3	Öryggiseiginleikar í Proton VPN			
4	Tegundir VPN-leka			
5	Aðstæður þar sem kill switch hjálpar			
6	Hlutir sem úttekt getur kannað			
7	Stillingar sem þú kveikir á fyrir aukið öryggi			
8	Hlutir sem dulkóðun ver			
9	Orð sem lýsa góðu VPN-forriti			
10	Ástæður fyrir því að velja Proton VPN			
11	Hnappar eða valmyndir í VPN-forriti			
12	Streymisveitur sem þú horfir á			
13	Ógnir á opinberu Wi-Fi			
14	Leiðir til að búa til sterkt lykilorð			
15	Lönd þar sem þú vilt hafa netþjóna frá Proton VPN			

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 STRANGA ELDVEGGI



Aðstæður: Notandi ferðast til lands þar sem venjuleg VPN-umferð á borð við OpenVPN og WireGuard er lokuð með DPI.

Umræðuspurning: Hvaða stilling á samskiptareglu Proton VPN gerir notandanum kleift að sniðganga skoðun á ríkisstigi?

DÆMISAGA 2: VERND GEGN ÞRAUTREYNDUM ÓVINUM



Aðstæður: Fjármálaendurskoðandi grunar að útgönguhnútur netþjónustuaðila hans gæti verið í hættu vegna háþróaðra viðvarandi ógna.

Umræðuspurning: Hvernig ver Secure Core auðkenni endurskoðandans gegn því að útgönguhnútur sé í hættu?

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	7	4	26	23	7		4	19	23	7		11	7	23	25	12	23

18	7	25	34	14	20	18	1	23		28	7	23	18	5	1		10	36	10	18

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 Proton VPN Secure Core?

Secure Core beinir umferð um marga netþjóna í löndum sem eru vinsamleg persónuvernd áður en hún fer út.

Q2: Hvað eru Stealth-samskiptareglurnar?

Stealth er yfirhulin samskiptaregla sem felur VPN-tengingar sem venjulega TLS/HTTPS-umferð.

Q3: Hvernig verndar NetShield notendur?

NetShield er DNS-byggt verkfæri sem lokar sjálfkrafa á auglýsingar, rekjara og spilliforritalén.

Q4: Nýtur Proton VPN lagaverndar í Sviss?

Já, Sviss hefur ströng persónuverndarlög og er utan lögsögu Bandaríkjanna og ESB/14-Eyes. [4]

Q5: Eru Proton VPN-forritin opinn hugbúnaður?

Já. Forrit Proton VPN eru með opnum kóða og hafa gengist undir birtar öryggisúttektir.

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

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

Q6: Hvaða dulmál eru notuð?

Proton VPN notar AES-256-GCM eða ChaCha20-Poly1305 með HMAC-SHA384 og RSA-4096 handaböndum.

Q7: Er Proton VPN með Kill Switch?

Já, Proton VPN inniheldur venjulegan og varanlegan Kill Switch til að koma í veg fyrir ódulkóðaðan leka.

Q8: Getur Proton VPN lekið DNS-fyrirspurnum?

Nei, allar DNS-fyrirspurnir fara um dulkóðaða einkaþjóna DNS sem Proton á.

Q9: Heldur Proton VPN tengiskrár?

Nei, Proton VPN heldur stranga stefnu um enga skráningu, staðfesta með árlegum úttektum Securitum. [3]

Q10: Er Proton VPN berskjaldað fyrir WebRTC-leka?

Nei, Proton-biðlarar innihalda innbyggðar eldveggsreglur og leiðarvalsstefnur sem loka á WebRTC-leka.

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

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

Q1: Hvar eru Secure Core-gagnaver staðsett í raun?

Þeir eru í Sviss, í fyrrverandi herstöð á Íslandi og á neðanjarðarstað í Svíþjóð. [1]

Q2: Hvernig virkar Perfect Forward Secrecy í Proton VPN?

Einkvæmur skammlífur dulkóðunarlykill er myndaður fyrir hverja lotu, sem kemur í veg fyrir afturvirka afkóðun.

Q3: Hvað er Permanent Kill Switch á Windows/Linux?

Varanlegur Kill Switch lokar á alla netumferð jafnvel þótt VPN-forritinu sé alveg lokað eða það hrynji.

Q4: Styður Proton VPN IPv6-leiðarval og vörn gegn leka?

Proton VPN beinir IPv6-umferð að fullu um göngin eða gerir hana óvirka á öruggan hátt til að koma í veg fyrir leka.

Q5: Hvernig meðhöndlar DNS-síun NetShield HTTPS-skoðun?

NetShield starfar eingöngu á DNS-uppflettistigi án þess að krefjast ágengrar TLS-afkóðunar.

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

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

Q6: Hver framkvæmdi úttektir þriðja aðila á kóða Proton VPN?

SEC Consult endurskoðaði forritin og Securitum endurskoðar forritin og stefnuna um skráningarleysi.

Q7: Hvernig er Stealth-samskiptareglan í samanburði við OpenVPN XOR eða Shadowsocks?

Stealth gengur með WireGuard um yfirhulið TLS og skilar betri árangri en eldri yfirhylming byggð á OpenVPN. [5]

Q8: Geta svissnesk yfirvöld skyldað Proton VPN til að skrá umferð?

Proton segir að samkvæmt svissneskum lögum sé fyrirtækinu ekki skylt að geyma skrár yfir virkni eða gögn notenda.

Q9: Hvernig eru Proton VPN-netþjónar varðir gegn upptöku?

Allir Proton VPN-netþjónar eru vélar án sýndarvæðingar sem eru varðar með fullri diskdulkóðun. [2]

Q10: Styður Proton VPN sérsniðnar stillingar DNS-netþjóna?

Já, greiðandi áskrifendur geta stillt eigin DNS-netþjóna beint í stillingum forritsins.

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. Proton á og setur sjálft upp Secure Core netþjóna sína á öruggum stöðum í Sviss, Íslandi og Svíþjóð. [1]

2. INNSÝN Í VPN

2. Proton VPN biðlaraforrit eru með opnum frumkóða og undirgangast endurteknar kóðaúttektir þriðja aðila.

3. INNSÝN Í VPN

3. Stealth dulbúningssamskiptareglan fer framhjá djúpri pakkaskoðun með því að líkja eftir venjulegri TLS-umferð.

4. INNSÝN Í VPN

4. Sviss er utan 5-Eyes, 9-Eyes og 14-Eyes alþjóðlegu leyniþjónustusamstarfsbandalaganna. [4]

5. INNSÝN Í VPN

5. NetShield starfar á DNS-úrlausnarstigi og kemur í veg fyrir auglýsingar og spilliforrit áður en farmur er sóttur.

6. INNSÝN Í VPN

6. Perfect Forward Secrecy tryggir að sprungnir lyklar geti ekki afkóðað áður fangaðar umferðarlotur. [7]

7. VPN-INNSÝN

7. Proton VPN notar fulla diskdulkóðun á netþjónum án sýndarvæðingar til að vernda stillingar netþjóna. [2]

8. VPN-INNSÝN

8. Varanlegur kill switch kemur í veg fyrir leka ódulkóðaðra gagna jafnvel við endurræsingu stýrikerfisins.

9. VPN-INNSÝN

9. Securitum hefur endurskoðað og staðfest stefnu Proton VPN um engar skrár í fimm árlegum úttektum í röð. [3]

10. INNSÝN Í VPN

10. Proton VPN var þróað af vísindamönnum sem kynntust hjá CERN (Evrópsku kjarnorkurannsóknastofnuninni). [4]

Tæknilegar heimildir og tilvísanir

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

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[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

Lausnir: Áfangi 1 – Fjölval

1 **Spurning 1** **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

Secure Core netþjónar eru á stöðum með mikla öryggisgæslu, þar á meðal í fyrrverandi herstöð á Íslandi og í neðanjarðargagnaveri í Svíþjóð.

2 **Stealth-yfirhylmingarsamskiptareglur** VÖRN GEGN RITSKOÐUN **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

Stealth-samskiptareglur Proton dulbúa WireGuard-tengingar sem venjulega TLS/HTTPS-umferð til að komast framhjá eldveggjum með djúpri pakkaskoðun (DPI). Heimild: Proton Stealth Protocol Whitepaper.

3 **NetShield DNS-auglýsingalokari** DNS-SÍUN **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

NetShield notar síun á DNS-stigi til að loka á spilliforritalén, njósnaforrit, ágengar auglýsingar og mæligagnarekjara áður en vefsíður hlaðast. Heimild: NetShield Security Specs.

4 **Svissnesk lögsaga** LÖGSAGA **Rétt svar: C**

ATHUGASEMD FYRIR KENNARA

Proton AG hefur höfuðstöðvar í Genf í Sviss og nýtur sterkra svissneskra persónuverndarlaga utan eftirlitsbandalaga Bandaríkjanna og ESB (14 Eyes). Heimild: Swiss Federal Data Protection Act. [4]

5 **Spurning 5** **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

Öll Proton VPN forrit eru með opnum frumkóða; SEC Consult og síðar Securitum hafa gert úttektir á þeim.

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Secure Core fjöllögsagnarumdæma** UPPBYGGING LEIÐARVALS **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Secure Core beinir umferð um lögsagnarumdæmi með sterka persónuvernd áður en hún fer út í áfangalandið, sem getur hjálpað til við að verjast útgangsnetþjóni sem hefur verið brotist inn á. Heimild: Secure Core Architecture.

7 **Svissneskt eftirlitsbandalag** EFTIRLITSBANDALÖG **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Sviss er ekki aðili að leyniþjónustusamstarfi 5-Eyes, 9-Eyes eða 14-Eyes og varðveitir þannig sjálfstætt löggjafarvald. Heimild: International Surveillance Treaties.

8 **Spurning 8** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

NetShield notar DNS-netþjóna Proton til að bera lén saman við lista yfir þekkt auglýsinga-, rekjara- og spilliforritalén.

9 **Úttekt á biðlara með opnum kóða** GAGNSÆI Í ÖRYGGISMÁLUM **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Proton hefur gert skjáborðs- og farsímaforrit sín opin og birtir úttektarskýrslur þriðju aðila. Heimild: SEC Consult Security Report.

10 **Spurning 10** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: Stealth pakkar WireGuard inn í duldan TLS yfir TCP þannig að umferðin lítur út eins og venjulegt HTTPS.

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

G 1. SECURE CORE	D 2. STEALTH	F 3. NETSHIELD	C 4. SVISSNESK LÖG
H 5. KILL SWITCH	A 6. OPINN KÓÐI	E 7. WIREGUARD	B 8. AES-GCM

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 SVISSNESK LÖG
5 KILL SWITCH	6 OPINN KÓÐI		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

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

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt SECURE CORE, STEALTH og NETSHIELD með eigin orðum og gefið dæmi um hvert hugtak.

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

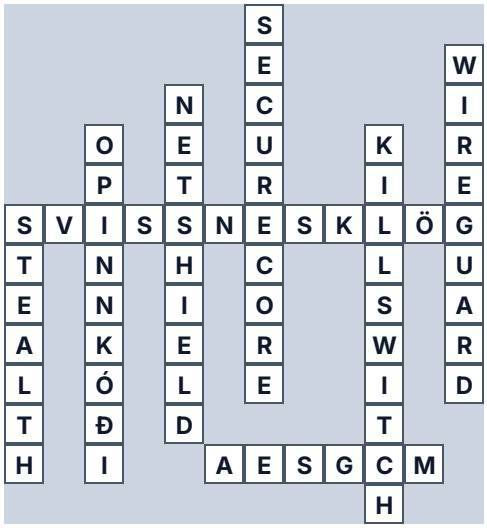
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

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

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

6 lárétt: SVISSNESKLÖG Ströng lagaákvæði um friðhelgi í Sviss utan lögsögu 14-Eyes (12 stafir)

7 lárétt: AESGCM Hernaðargráðu samhverft dulmál sem ver alla hjúpaða VPN-gagnapakka (6 stafir)

LÓÐRÉTT

1 lóðrétt: SECURECORE Fjölstökkshönnun sem beinir umferð um fyrstu stökk netþjóna í eigu Proton (10 stafir)

2 lóðrétt: WIREGUARD Nútímaleg og létt samskiptaregla með öflugri dulritun og miklum hraða (9 stafir)

3 lóðrétt: NETSHIELD DNS-byggð sía sem lokar á auglýsingar, mælingarrekjara og spilliforrit (9 stafir)

4 lóðrétt: OPINNKÓÐI Opinberlega aðgengilegur og óháð ryndur hugbúnaður biðlaraforrita (9 stafir)

5 lóðrétt: KILLSWITCH Öryggisbúnaður sem stöðvar netflutning þegar tenging fellur (10 stafir)

6 lóðrétt: STEALTH Dulin göngusamskiptaregla sem dulbýr sig sem venjulega HTTPS-vefumferð (7 stafir)

Lausnir: Stafaruglingur og dulmál

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

LYKILL ORÐARAÐAR

1. RCERESOEUC — SECURECORE
2. DNLSEIEHT — NETSHIELD
3. KWCIISHLTL — KILLSWITCH
4. GDREAUWIR — WIREGUARD
5. LHAESTT — STEALTH
6. GSKLNÖSSVEIS — SVISSNESKLÖG
7. KOÐIÓNPNI — OPINNKÓÐI
8. SMACGE — AESGCM

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"SECURE CORE HERTIR NETÞJÓNAR VERNDA GÖGN NOTENDA"

Lausnir dæmisagna

A DÆMISAGA 1: AÐ SNIÐGANGA STRANGA ELDVEGGI

Lausn fyrir kennara

EINKUNNAGJÖF OG LEIÐBEININGAR UM LAUSNIR

- Greining aðstæðna: Notandi ferðast til lands þar sem venjuleg VPN-umferð eins og OpenVPN og WireGuard er lokað með DPI.
- Lykilspurning: Hvaða stilling á samskiptareglu í Proton VPN gerir notandanum kleift að komast framhjá skoðun á vegum ríkisins?
- Ráðlögð aðferð og lausn: Notandinn ætti að virkja Stealth-samskiptaregluna, sem dulbýr VPN-pakkahausa sem venjulega TLS/HTTPS-vefumferð og smýgur framhjá DPI-síum.

B DÆMISAGA 2: VERND GEGN ÞRAUTREYNDUM ÓVINUM

Lausn fyrir kennara

EINKUNNAGJÖF OG LEIÐBEININGAR UM LAUSNIR

- Greining aðstæðna: Fjárhagsendurskoðandi grunar að útgangshnútur netþjónustuveitu hans gæti verið í hættu vegna þrálátra háþróaðra ógna.
- Lykilspurning: Hvernig ver Secure Core auðkenni úttektaraðilans ef útgönguhnútur er í hættu?
- Ráðlögð aðferð og lausn: Secure Core sendir umferð fyrst um netþjóna í eigu Proton í Sviss, Íslandi eða Svíþjóð, svo útgangsnetþjónn í hættu getur ekki rakið IP-tölu notandans.