Nafn: _____ Dagsetning: _____ Stig: _____

Öryggi ExpressVPN

Mat á öryggisinnviðum ExpressVPN, sérsniðnu opnu Lightway-samskiptareglunni, TrustedServer-tækni eingöngu með vinnsluminni, óháðum öryggisúttektum og Network Lock kill switch.

YFIRLIT NÁMS UM ÖRYGGI EXPRESSVPN

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 öryggiseiginleika ExpressVPN. Þú munt kanna opnar samskiptareglur, netþjónahnúta með eingöngu RAM, dulmál og Network Lock kill switch.

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/expressvpn/oryggi/

Námsvegvísir þinn: öryggi ExpressVPN

- Greindu tæknilega uppbyggingu og stillingarreglur varðandi öryggi hjá ExpressVPN.
- 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 EXPRESSVPN

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

NETÞJÓNASÖFN EINGÖNGU Í VINNSLUMINNI OG SAMSKIPTAREGLUR MEÐ OPNUM FRUMKÓÐA

ExpressVPN notar TrustedServer-tækni eingöngu með vinnsluminni til að koma í veg fyrir staðbundnar skrár, ásamt sérsniðnu opnu Lightway-samskiptareglunni og Internet Kill Switch til að veita gagnaöryggi notenda frá enda til enda.

(INNGANGUR)

ExpressVPN notar TrustedServer-tækni eingöngu með vinnsluminni til að koma í veg fyrir staðbundnar skrár, ásamt sérsniðnu opnu Lightway-samskiptareglunni og Internet Kill Switch til að veita gagnaöryggi notenda frá enda til enda.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hver eru sérsniðnu opnu samskiptareglur ExpressVPN?**

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

2 **2. Hvaða netþjónatækni keyrir eingöngu í rokgjörnu vinnsluminni?**

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

3 **3. Hvað gerist ef VPN-tenging slitnar óvænt?**

- A) Kill switch lokar fyrir umferð
- B) Umferð lekur til netþjónustuaðilans
- C) Kerfið endurræsir sig
- D) Gögn verða ódulkóðuð

4 **4. Hvar er ExpressVPN skráð til að vernda persónuvernd?**

- A) Bresku Jómfrúaeyjar
- B) Sviss
- C) Panama
- D) Rúmenía

5 **5. Hvaða samhverfa dulmál er notað sjálfgefið?**

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

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. TrustedServer tæknin geymir netþjónaannála á hörðum diskum.

○ Satt ○ Ósatt

7 Spurning 7

7. ExpressVPN hefur gengist undir öryggisúttektir þriðju aðila.

○ Satt ○ Ósatt

8 Spurning 8

8. Lightway-samskiptareglurnar eru byggðar ofan á OpenVPN-kóðagrunninn.

○ Satt ○ Ósatt

9 Spurning 9

9. Kill switch er sjálfgefið virkur í skjáborðsforritum.

○ Satt ○ Ósatt

10 Spurning 10

10. ExpressVPN rekur einka-DNS á hverjum einasta þjóni.

○ Satt ○ Ósatt

Áfangi 3: Lykilhugtök fyllt inn

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

1. Hraðvirka samskiptareglan sem ExpressVPN hannaði sjálft heitir _____ .

2. Til að koma í veg fyrir gagnageymslu byggir netþjónakerfið á _____ netþjónum sem nota eingöngu vinnsluminni.

3. Kill switch ExpressVPN hét áður Network _____ .

4. Lögsagnarumdæmi ExpressVPN eru Bresku _____ .

5. Gögn eru varin með öflugu samhverfu dulmáli, _____ .

6. Stefnan um engar skrár hefur sætt óháðri _____ leiðandi fyrirtækja.

ORÐABANKI

AES-256 JÓMFRÚAREYJAR LEKI LIGHTWAY LOCK NAFNAÞJÓNN TRUSTED SERVER ÚTTEKT

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um VPN og net

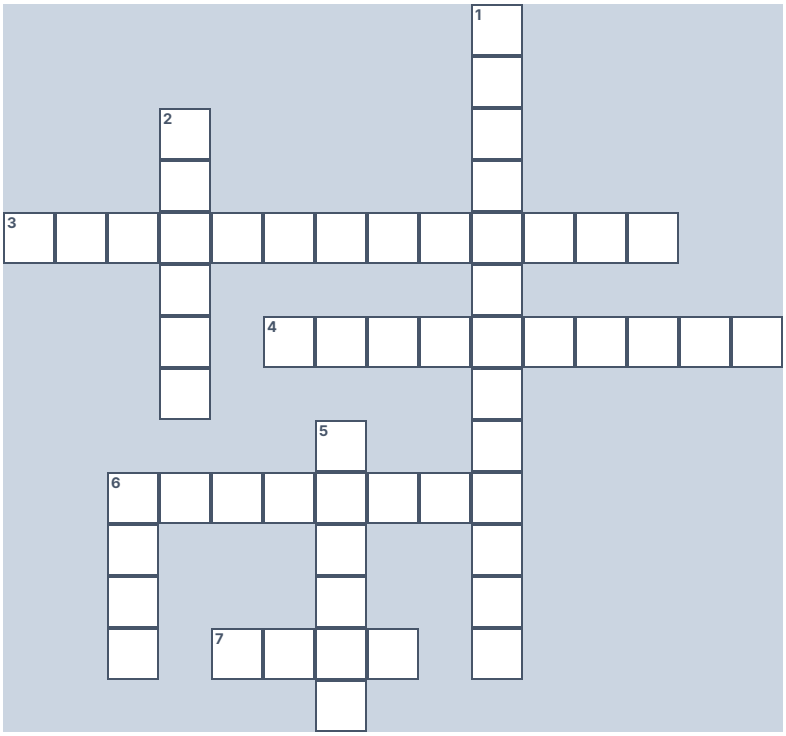
PÖRUN SKILGREININGA

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

☐	1. LIGHTWAY	A	Lögsaga Bresku Jómfrúaeyja sem býður upp á sterka persónuvernd
☐	2. TRUSTED SERVER	B	Óviljandi afhjúpun á einka-IP-tölu, DNS- eða WebRTC-gögnum
☐	3. LÁS	C	Leysiþjónar lénakerfisins (DNS) keyra á einkaþjóni á hverjum þjónshnút
☐	4. EYJAR	D	Staðfest óháð af öryggisfyrirtækjum þriðju aðila
☐	5. AES-256	E	Netþjónaarkitektúr eingöngu í vinnsluminni sem kemur í veg fyrir gagnageymslu á diski
☐	6. ÚTTEKIN	F	Síðasta orðið í Network Lock, fyrra heiti kill switch
☐	7. LEKI	G	Létt, opin tengisamskiptaregla ExpressVPN
☐	8. DNS	H	Samhverfur dulkóðunarstaðall sem ver gagnaflutning

Áfangi 5: Krossgáta

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



LÁRÉTT

3. Netþjónaarkitektúr sem notar eingöngu vinnsluminni og kemur í veg fyrir gagnageymslu á diski (13)

4. DNS-nafnaþjónar (lénakerfið) sem eru reknir í einkaeigu á hverjum netþjónahnúti (10)

6. Létt, opin tengisamskiptaregla ExpressVPN (8)

7. Óviljandi birting einkaupplýsinga um IP, DNS eða WebRTC (4)

LÓÐRÉTT

1. Lögsagnarumdæmi bresku Jómfrúareyja sem býður upp á sterka friðhelgi (13)

2. Samhverfur dulkóðunarstaðall sem ver gagnaflutning (6)

5. Sjálfstæð sannprófun öryggisfyrirtækja þriðja aðila (6)

6. Síðasta orðið í Network Lock, fyrra heiti kill switch (4)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

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

LÁRÉTT

3 lárétt: Netþjónaarkitektúr sem notar eingöngu vinnsluminni og kemur í veg fyrir gagnageymslu á diski (13 stafir):

4 lárétt: DNS-nafnaþjónar (lénakerfið) sem eru reknir í einkaeigu á hverjum netþjónahnúti (10 stafir):

6 lárétt: Létt, opin tengisamskiptaregla ExpressVPN (8 stafir):

7 lárétt: Óviljandi birting einkaupplýsinga um IP, DNS eða WebRTC (4 stafir):

LÓÐRÉTT

1 lóðrétt: Lögsagnarumdæmi bresku Jómfrúareyja sem býður upp á sterka friðhelgi (13 stafir):

2 lóðrétt: Samhverfur dulkóðunarstaðall sem ver gagnaflutning (6 stafir):

5 lóðrétt: Sjálfstæð sannprófun öryggisfyrirtækja þriðja aðila (6 stafir):

6 lóðrétt: Síðasta orðið í Network Lock, fyrra heiti kill switch (4 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.

R D Ö Y N F J 6 G Ö Đ N Đ R Ý
A Y P B V N 5 Á A Ö O Đ K A Đ
J A O Đ É 2 Ó G I Đ S R M E I
Y W T Ö S U É J R X É A A R Ó
E T N E P Ú Þ R Þ J S Ú T T D
R H A N Æ B F T Ý A Y Í K A S
A G Ö Æ Æ K F I M S N E J L L
Ú I U Ó G P R G Ö A T F O X F
R L V B Æ T Æ Á G T L Ö A G J
F O P N Ý B L Ö Ú Æ F Þ Ó N Y
M T R U S T E D S E R V E R V
Ó K V L P Á O X Ú L G X I D Þ
J V O J S Á Ý Ö Þ M T R K Ý I
Ó C Đ A D J R Y Ý Ý K Í E H Ú
K H F Á É I K U T Y S Ö L E H

ORÐALISTI

LIGHTWAY TRUSTEDSERVER LOCK JÓMFRÚAREYJAR AES256 ÚTTEKT LEKI NAFNAÞJÓNN

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. LIGHTWAY
B. TRUSTEDSERVER
C. LOCK
D. JÓMFRÚAREYJAR
E. AES256
F. ÚTTEKT
G. LEKI
H. NAFNAÞJÓNN

SKILGREININGAR OG PÖRUNARREITIR
1. Óviljandi birting einkaupplýsinga um IP, DNS eða WebRTC.
2. Lögsagnarumdæmi bresku Jómfrúareyja sem býður upp á sterka friðhelgi.
3. DNS-nafnaþjónar (lénakerfið) sem eru reknir í einkaeigu á hverjum netþjónahnúti.
4. Létt, opin tengisamskiptaregla ExpressVPN.
5. Síðasta orðið í Network Lock, fyrra heiti kill switch.
6. Samhverfur dulkóðunarstaðall sem ver gagnaflutning.
7. Netþjónaarkitektúr sem notar eingöngu vinnsluminni og kemur í veg fyrir gagnageymslu á diski.
8. Sjálfstæð sannprófun öryggisfyrirtækja þriðja aðila.

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. AHTLWIYG
2. LCKO
3. AS265E
4. IKLE
5. EVRUSTRERDTES
6. RYAÚJMAEJÓRRF
7. KÚETTT
8. NNÞNNAAJÓF

Aukaverkefni: Hugsaðu hratt

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

1	Eiginleikar sem þú leitar að í ExpressVPN			
2	Ógnir á opinberu Wi-Fi			
3	Tegundir VPN-leka			
4	Leiðir til að búa til sterkt lykilorð			
5	Hnappar eða valmyndir í VPN-forriti			
6	Hlutir sem þú gerir á netinu á hverjum degi			
7	Fólk sem þú myndir mæla með ExpressVPN við			
8	Lönd sem eru þekkt fyrir sterk persónuverndarlög			
9	VPN-samskiptareglur sem þú þekkir			
10	Hlutir sem úttekt getur kannað			
11	Öryggiseiginleikar í ExpressVPN			
12	Hlutir til að athuga áður en þú kaupir VPN			
13	Stillingar sem þú kveikir á fyrir aukið öryggi			
14	Hlutir sem dulkóðun ver			
15	Hlutir sem ExpressVPN getur falið fyrir netinu þínu			

Áfangi 8: Dæmisögur um VPN og net

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

DÆMISAGA 1: AÐ FRAMFYLGJA VERND MEÐ AÐEINS VINNSLUMINNI



Aðstæður: Ríkisstofnun leggur hald á ExpressVPN-netþjón til að ná í notendaskrár og tengingarsögu.

Umræðuspurning: Hvaða upplýsingar munu þau finna á þjóninum og hvers vegna?

DÆMISAGA 2: ÓSTÖÐUG GÖNG Á WI-FI-TENGINGU



Aðstæður: Starfsmaður í fjarvinnu notar opinbert Wi-Fi á hóteli sem slitnar á nokkurra mínútna fresti meðan hann breytir skjölum.

Umræðuspurning: Hvernig ver ExpressVPN gögn hans gegn leka þegar tengingin slitnar?

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 Ð=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

25 23 26 24 25 7 5 24 7 23 28 7 23   7 31 6 12 23

36 16 16 26 17   18 19 25 7 18 5 1 24 15 23 2 17

5 1 10 16 7 10 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: Hvaða dulkóðun notar ExpressVPN?

ExpressVPN notar AES-256-GCM samhverfa dulkóðun sjálfgefið.

Q2: Hvað eru Lightway-samskiptareglurnar?

Lightway er sérsmíðaðar samskiptareglur ExpressVPN, byggðar fyrir hraða, öryggi og stöðugleika.

Q3: Skráir ExpressVPN leitarferilinn minn?

Nei, ExpressVPN framfylgir strangri stefnu um enga skráningu sem hefur verið úttekt óháð.

Q4: Hvað er Internet Kill Switch?

Það er innbyggður kill switch ExpressVPN sem lokar á netumferð ef tengingin rofnar.

Q5: Er Lightway-samskiptareglan með opnum frumkóða?

Já, kjarnakóði Lightway-samskiptareglunnar er með opnum kóða og aðgengilegur á GitHub. [9]

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

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

Q6: Rekur ExpressVPN einkarekið DNS?

Já, ExpressVPN rekur eigin einka-DNS með dulkóðun á hverjum netþjóni. [7]

Q7: Hvað er TrustedServer-tæknin?

Það er netþjónauppsetning þar sem stýrikerfið og forritin keyra alfarið í rokgjörnu vinnsluminni.

Q8: Hefur ExpressVPN verið úttekið?

Já, ExpressVPN hefur verið tekið út af fyrirtækjum eins og PwC, Cure53 og F-Secure. [1]

Q9: Ver ExpressVPN gegn DNS- og IPv6-leka?

Já, Internet Kill Switch lokar á IPv4-, IPv6- og DNS-umferð utan ganganna.

Q10: Hvar er ExpressVPN staðsett?

ExpressVPN er skráð á Bresku Jómfrúareyjum (BVI).

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

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

Q1: Hvernig eykur uppbygging með eingöngu vinnsluminni öryggi?

Gögn eru ekki skrifuð á harða diska og gögn í minni eru þurrkuð út í hvert sinn sem slökkt er á þjóninum.

Q2: Hvers vegna skiptir BVI-lögsagnarumdæmið máli fyrir friðhelgi einkalífs?

ExpressVPN hefur aðsetur á BVI, þannig að lagakröfur um gögn lúta lögum BVI.

Q3: Styður ExpressVPN fullkomið framvirkt leynd (perfect forward secrecy)?

Já, Lightway notar kvika lykla sem er reglulega eytt og búnir til upp á nýtt.

Q4: Hvernig kemur Network Lock í veg fyrir IP-leka?

Það lokar á alla umferð á kerfisstigi hvenær sem VPN-tengingin rofnar.

Q5: Ver Lightway gegn skammtafræðiárásum?

Já, Lightway býður upp á vernd gegn skammtatölvum (post-quantum) með NIST ML-KEM staðlinum.

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

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

Q6: Geta ríkisstofnanir hlerað Lightway-umferð?

Þeir geta numið hana en geta ekki afkóðað hana vegna AES-256/ChaCha20 dulkóðunar.

Q7: Hvernig ver einka-DNS leitarskrár notenda?

Það vinnur allar DNS-fyrirspurnir innan dulkóðuðu ganganna og kemur í veg fyrir vöktun netþjónustuveitu.

Q8: Til hvers er Lightway Turbo notað?

Það notar fjölbrautagöng til að senda meira af gögnum í einu fyrir meiri hraða.

Q9: Hver er kosturinn við Lightway umfram WireGuard?

Lightway er sérsmíðað til að takast hratt á við netskipti (eins og úr Wi-Fi yfir í farsímanet) án þess að tengingin falli niður.

Q10: Hversu oft er netþjónahugbúnaðurinn settur upp aftur?

Með TrustedServer er allt hugbúnaðarsafnið endurhlaðið úr öruggri skrifvarinni mynd við hverja endurræsingu.

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

Lightway notar AES-256-GCM, eða ChaCha20/Poly1305 á tækjum með litla orkunotkun. [6]

2. INNSÝN Í VPN

TrustedServer tæknin er hönnuð til að keyra alla netþjónastarfsemi í vinnsluminni (RAM). [4]

3. INNSÝN Í VPN

Bresku Jómfrúaeyjar (BVI) eru lögsagnarumdæmi fyrirtækisins. [8]

4. INNSÝN Í VPN

Lightway var endurskrifað úr C í Rust og úttektað af Cure53 og Praetorian. [3]

5. INNSÝN Í VPN

Internet Kill Switch lokar á umferð á kerfisstigi ef VPN rofnar. [5]

6. INNSÝN Í VPN

Allar DNS-fyrirspurnir eru leystar í gegnum einka-dulkóðaða DNS-netþjóna. [7]

7. VPN-INNSÝN

ExpressVPN hefur birt meira en 20 óháðar úttektir þriðju aðila. [1]

8. VPN-INNSÝN

Þjónustan skráir hvorki IP-tölur, vafrasögu né lýsigögn umferðar.

9. VPN-INNSÝN

Fullkomið framvirkt leynd (Perfect Forward Secrecy) er viðhaldið með kvikri skiptingu lotulykla. [1]

10. INNSÝN Í VPN

Lightway-samskiptareglan styður bæði UDP og TCP flutningslög.

Tæknilegar heimildir og tilvísanir

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

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

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

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

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

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

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

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

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

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

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

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

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

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

Lausnir: Áfangi 1 – Fjölval

1 **Spurning 1** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hver eru sérsniðnu opnu samskiptareglur ExpressVPN? → Lightway

2 **Spurning 2** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvaða netþjónatækni keyrir eingöngu í rokgjörnu vinnsluminni? → TrustedServer

3 **Spurning 3** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað gerist ef VPN-tenging slitnar óvænt? → A) Kill switch lokar fyrir umferð

4 **Spurning 4** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvar er ExpressVPN skráð til að vernda persónuvernd? → Bresku Jómfrúaeyjar

5 **Spurning 5** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvaða samhverfa dulmál er notað sjálfgefið? → AES-256-GCM

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

TrustedServer tæknin geymir netþjónaannála á hörðum diskum.

7 **Spurning 7** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

ExpressVPN hefur gengist undir öryggisúttektir þriðju aðila.

8 **Spurning 8** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Lightway-samskiptareglurnar eru byggðar ofan á OpenVPN-kóðagrunninn.

9 **Spurning 9** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Kill switch er sjálfgefið virkur í skjáborðsforritum.

10 **Spurning 10** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

ExpressVPN rekur einka-DNS á hverjum einasta þjóni. [7]

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. LIGHTWAY	E 2. TRUSTED SERVER	F 3. LÁS	A 4. EYJAR
H 5. AES-256	D 6. ÚTTEKIN	B 7. LEKI	C 8. DNS

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 LIGHTWAY	2 TRUSTED SERVER	3 LOCK	4 JÓMFRÚAREYJAR
5 AES-256	6 ÚTTEKT		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 G – LEKI	2 D – JÓMFRÚAREYJAR	3 H – NAFNAÞJÓNN	4 A – LIGHTWAY
5 C – LOCK	6 E – AES256	7 B – TRUSTEDSERVER	8 F – ÚTTEKT

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt LIGHTWAY, TRUSTED SERVER og LÁS með eigin orðum og gefið dæmi um hvert hugtak.

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

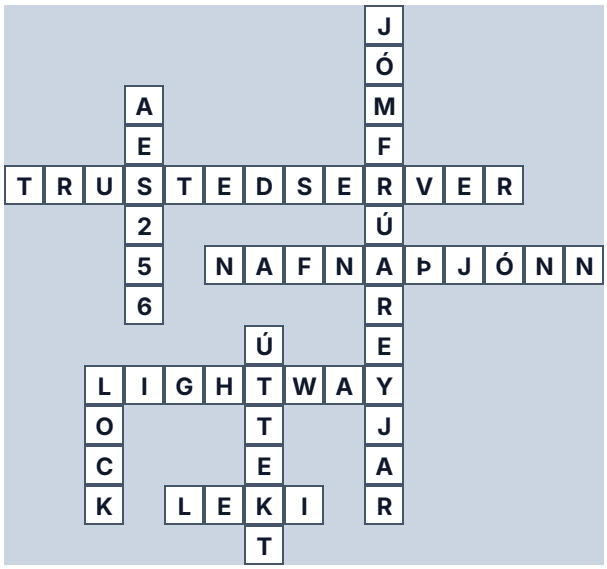
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

R	D	Ö	Y	N	F	J	6	G	Ö	Đ	N	Đ	R	Ý
A	Y	P	B	V	N	5	Á	A	Ö	O	Đ	K	A	Đ
J	A	O	Đ	É	2	Ó	G	I	Đ	S	R	M	E	I
Y	W	T	Ö	S	U	É	J	R	X	É	A	A	R	Ó
E	T	N	E	P	Ú	Þ	R	Þ	J	S	Ú	T	T	D
R	H	A	N	Æ	B	F	T	Ý	A	Y	Í	K	A	S
A	G	Ö	Æ	Æ	K	F	I	M	S	N	E	J	L	L
Ú	I	U	Ó	G	P	R	G	Ö	A	T	F	O	X	F
R	L	V	B	Æ	T	Æ	Á	G	T	L	Ö	A	G	J
F	O	P	N	Ý	B	L	Ö	Ú	Æ	F	Þ	Ó	N	Y
M	T	R	U	S	T	E	D	S	E	R	V	E	R	V
Ó	K	V	L	P	Á	O	X	Ú	L	G	X	I	D	Þ
J	V	O	J	S	Á	Ý	Ö	Þ	M	T	R	K	Ý	I
Ó	C	Đ	A	D	J	R	Y	Ý	Ý	K	Í	E	H	Ú
K	H	F	Á	É	I	K	U	T	Y	S	Ö	L	E	H

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

3 lárétt: TRUSTEDSERVER Netþjónaarkitektúr sem notar eingöngu vinnsluminni og kemur í veg fyrir gagnageymslu á diski (13 stafir)

4 lárétt: NAFNAÞJÓNN DNS-nafnaþjónar (lénakerfið) sem eru reknir í einkaeigu á hverjum netþjónahnúti (10 stafir)

6 lárétt: LIGHTWAY Létt, opin tengisamskiptaregla ExpressVPN (8 stafir)

7 lárétt: LEKI Óviljandi birting einkaupplýsinga um IP, DNS eða WebRTC (4 stafir)

LÓÐRÉTT

1 lóðrétt: JÓMFRÚAREYJAR Lögsagnarumdæmi bresku Jómfrúareyja sem býður upp á sterka friðhelgi (13 stafir)

2 lóðrétt: AES256 Samhverfur dulkóðunarstaðall sem ver gagnaflutning (6 stafir)

5 lóðrétt: ÚTTEKT Sjálfstæð sannprófun öryggisfyrirtækja þriðja aðila (6 stafir)

6 lóðrétt: LOCK Síðasta orðið í Network Lock, fyrra heiti kill switch (4 stafir)

Lausnir: Stafaruglingur og dulmál

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

LYKILL ORÐARAÐAR

1. AHTLWIYG — LIGHTWAY
2. LCKO — LOCK
3. AS265E — AES256
4. IKLE — LEKI
5. EVRUSTRERDTES — TRUSTEDSERVER
6. RYAÚJMAEJÓRRF — JÓMFRÚAREYJAR
7. KÚETTT — ÚTTEKT
8. NNÞNNAAJÓF — NAFNAÞJÓNN

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"TRUSTEDSERVER EYÐIR ÖLLUM NOTENDASKRÁM DAGLEGA"

Lausnir dæmisagna

A DÆMISAGA 1: AÐ FRAMFYLGJA VERND MEÐ AÐEINS VINNSLUMINNI

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Opinber stofnun leggur hald á ExpressVPN-netþjón til að ná í notendaskrár og tengingarsögu.
- Ráðlögð aðferð og lausn: Ekkert. TrustedServer-tækni ExpressVPN keyrir alfarið í vinnsluminni, svo öllum gögnum er eytt samstundis við rafmagnsleysi.

B DÆMISAGA 2: ÓSTÖÐUG GÖNG Á WI-FI-TENGINGU

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Fjarstarfsmaður notar opinbert Wi-Fi á hóteli sem slitnar á nokkurra mínútna fresti meðan hann breytir skjölum.
- Ráðlögð aðferð og lausn: Internet Kill Switch lokar sjálfkrafa á alla netumferð þar til VPN-göngin hafa verið endurreist.