Nafn: _____ Dagsetning: _____ Stig: _____

Hvað er VPN Verkefnablað

Verklegar æfingar í netsamskiptareglum, göngum og öryggisstýringum.

YFIRLIT NÁMSEFNIS UM VPN

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 grundvallarreglur sýndareinkaneta (VPN). Þú munt kynnast því hvernig dulkóðuð göng vernda gögnin þín, hvernig netsamskiptareglur virka og hvernig á að greina og draga úr lekum á friðhelgi.

ÁFANGAR VERKEFNABLAÐSINS

- [ ] **Hluti 1-4: Náðu tökum á VPN-hugtökum og samskiptareglum.**
- [ ] **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 VPN-leiðarvísi VPN.com

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

Námsvegvísir þinn: VPN

- Útskýrðu hugtakið gagnagöngun og innhjúpun.
- Greindu hefðbundnar stillingar samskiptareglna og dulkóðunaraðferðir.
- Greindu hlutverk netþjóna og IP-grímunar í sýndareinkanetum.
- Skildu hvernig netþjónustuveitur fylgjast með vafri og hvernig VPN kemur í veg fyrir það.
- Gerðu greinarmun á rekstrarlegum mörkum sýndarnetsuppbyggingar.

LEIÐBEININGAR: HVAÐ ER VPN?

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á raunveruleg dæmi í dæmisöguhlutanum. Ljúktu með aukaverkefninu Hugsaðu hratt.

HVAÐ ER VPN? (INNGANGUR)

Sýndareinkanet er meira en bara persónuverndarrofi. Það eru dulkóðuð göng sem beina netumferð þinni í gegnum fjarnetþjón. Þetta felur IP-töluna þína, kemur í veg fyrir að netþjónustuveitan þín safni skrám um aðgerðir þínar á netinu og tryggir gögnin þín á opnum netum. Skilningur á hugtökunum er nauðsynlegur til að viðhalda stafrænu öryggi.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1. Hvert er meginhlutverk sýndareinkanets (VPN)?

- A. Til að auka birtingarhraða vafrans
- B. Til að dulkóða gagnapakka og fela opinberu IP-töluna þína
- C. Til að geyma vefkökugagnagrunna staðbundið
- D. Til að koma í stað líkamlegs tölvubúnaðar þíns

2. Hvað eru netgöng (tunneling) í tengslum við VPN?

- A. Að eyða tvíteknum netskrám
- B. Að setja upp gagnagrunnsskrár á staðnum
- C. Að deila skrám með öðrum staðbundnum tölvum
- D. Að pakka einum netpakka inn í annan öruggan pakka

3. Hvaða dulkóðunarstaðall er víða notaður til að verja VPN-umferð?

- A. Úrelt DES-dulkóðun
- B. Nútímalegi AES-256 staðallinn
- C. Base64-kóðun í ódulkóðuðum texta
- D. Venjuleg rot13-dulritun

4. Hvaða hluti netumferðar þinnar er dulkóðaður af VPN?

- A. Aðeins prentverk á staðarneti tækisins
- B. Leiðin sem ethernet-kapallinn liggur
- C. Allur gagnahluti netpakkans
- D. Aðeins leitarsaga þín í vafranum

5. Hvað merkir hugtakið „dulkóðun“ í netkerfum?

- A. Að breyta ódulkóðuðum gögnum í ólæsilegan dulmálstexta
- B. Að eyða gömlum samskiptaskrám
- C. Að hækka hámark staðbundinnar bandbreiddar
- D. Að deila aðgangslyklum að gagnagrunni opinberlega

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. VPN dulkóðar umferðina þína til að koma í veg fyrir hleranir á staðnum á opnu Wi-Fi.

Satt Ósatt

7 Spurning 7

7. VPN breytir vélbúnaðarstillingum beinisins þíns líkamlega.

Satt Ósatt

8 Spurning 8

8. Gangasamskiptareglur pakka gagnapökkum inn í dulkóðað flutningslag.

Satt Ósatt

9 Spurning 9

9. Samhverf dulkóðun notar sama lykil til að dulkóða og afkóða umferð.

Satt Ósatt

10 Spurning 10

10. Notkun VPN gerir nettenginguna þína líkamlega ónæma fyrir rafmagnsleysi án nettengingar.

Satt Ósatt

Áfangi 3: Lykilhugtök fyllt inn

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

1. Til að tryggja umferð þína vefur VPN gagnapökkunum inn í aðra samskiptareglu, ferli sem kallast _____ .

2. Ef niðurhal er hægt við streymi gæti það stafað af takmarkaðri _____ á netinu.

3. Streymisþjónusta sem er aðeins í boði í tilteknu landi beitir takmörkun sem kallast _____ gegn notendum annars staðar.

4. Tengireglur sem skilgreina dulkóðun og tengibreytur eru kallaðar _____ VPN.

5. Tölvan þín notar staðbundinn _____ til að fylgjast með netumferð og loka á óörugga tengingar.

6. Þegar þú tengist VPN fer umferðin um fjartengda tölvu sem nefnist _____ til að fela opinbera IP-tölu þína.

ORÐABANKI

BANDBREIDD ELDVEGGUR FRIÐHELGI HJÚPUN LANDLÆSING NETVEITA NETÞJÓNN SAMSKIPTAREGLA

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um net

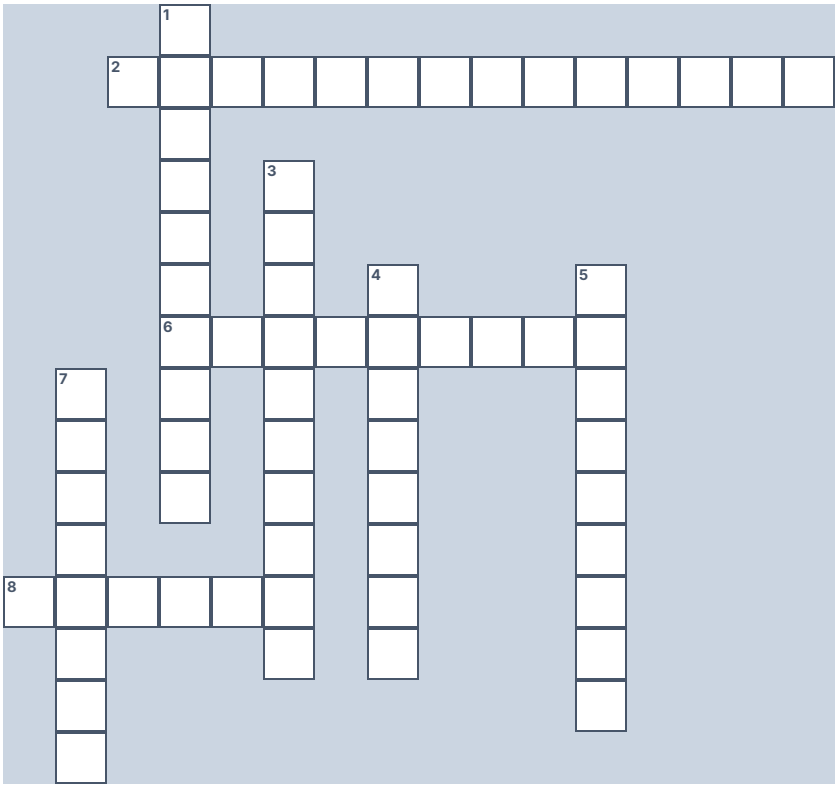
PÖRUN SKILGREININGA

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

☐	1. Göng	A	Fjartölva sem beinir umferðinni þinni og felur IP-töluna þína.
☐	2. Samskiptaregla	B	Netþjónustuveitan sem flytur umferð þína og getur séð ódulkóðaða virkni.
☐	3. Bandvídd	C	Takmörkun sem kemur í veg fyrir vefaðgang út frá líkamlegri staðsetningu.
☐	4. Netþjónn	D	Öryggiskerfi sem fylgist með og lokar á óheimila umferð.
☐	5. Landfræðileg lokun	E	Safn reglna sem ákvarða hvernig gögn eru send um netið.
☐	6. Eldveggur	F	Það að vera laus við rakningu eða opinbert eftirlit.
☐	7. Persónuvernd	G	Mesti hraði gagnaflutnings yfir tengingu.
☐	8. Netþjónustuveita	H	Gagnapakkar settir inn í annan pakka til öruggs flutnings.

Áfangi 5: Krossgáta

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



LÁRÉTT

2. Safn reglna sem ákvarða hvernig gögn eru send yfir netið (14)

6. Öryggiskerfi sem vaktar og lokar á óheimila umferð (9)

8. Að vefja gagnapökkum inn í annan pakka fyrir örugga flutninga (6)

LÓÐRÉTT

1. Hámarkshraði gagnaflutnings yfir tengingu (10)

3. Takmörkun sem hindrar vefaðgang eftir líkamlegri staðsetningu (10)

4. Netþjónustuveita sem skráir umferð þína nema hún sé dulkóðuð (8)

5. Það að vera laus við rakningu eða opinbert eftirlit (9)

7. Fjartengd tölva sem beinir umferð þinni og felur IP-töluna þína (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: Safn reglna sem ákvarða hvernig gögn eru send yfir netið (14 stafir):

6 lárétt: Öryggiskerfi sem vaktar og lokar á óheimila umferð (9 stafir):

8 lárétt: Að vefja gagnapökkum inn í annan pakka fyrir örugga flutninga (6 stafir):

LÓÐRÉTT

1 lóðrétt: Hámarkshraði gagnaflutnings yfir tengingu (10 stafir):

3 lóðrétt: Takmörkun sem hindrar vefaðgang eftir líkamlegri staðsetningu (10 stafir):

4 lóðrétt: Netþjónustuveita sem skráir umferð þína nema hún sé dulkóðuð (8 stafir):

5 lóðrétt: Það að vera laus við rakningu eða opinbert eftirlit (9 stafir):

7 lóðrétt: Fjartengd tölva sem beinir umferð þinni og felur IP-töluna þína (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.

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

ORÐALISTI

HJÚPUN · SAMSKIPTAREGLA · BANDBREIDD · NETÞJÓNN · LANDLÆSING
ELDVEGGUR · FRIÐHELGI · NETVEITA

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. HJÚPUN
B. SAMSKIPTAREGLA
C. BANDBREIDD
D. NETÞJÓNN
E. LANDLÆSING
F. ELDVEGGUR
G. FRIÐHELGI
H. NETVEITA

SKILGREININGAR OG PÖRUNARREITIR

1. Safn reglna sem ákvarða hvernig gögn eru send yfir netið.
2. Takmörkun sem hindrar vefaðgang eftir líkamlegri staðsetningu.
3. Öryggiskerfi sem vaktar og lokar á óheimila umferð.
4. Það að vera laus við rakningu eða opinbert eftirlit.
5. Netþjónustuveita sem skráir umferð þína nema hún sé dulkóðuð.
6. Að vefja gagnapökkum inn í annan pakka fyrir örugga flutninga.
7. Fjartengd tölva sem beinir umferð þinni og felur IP-töluna þína.
8. Hámarkshraði gagnaflutnings yfir tengingu.

Áfangi 7: Áskorun með ruglaðum orðum

Raðaðu stöfunum hér að neðan í rétta röð til að afhjúpa lykilhugtök um VPN. Skrifaðu svörin þín í útfyllanlegu reitina.

1. ÚHPUNJ
2. DDBABDEIRN
3. LÆNSALGDIN
4. HIGÐLEFRI
5. RMGATAKAIE PSLS
6. NNÞÓNJET
7. GEURGVLED
8. VEEANTIT

Aukaverkefni: Hugsaðu hratt

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

1	Hlutir sem IP-tala getur afhjúpað			
2	Mýtur um VPN			
3	Hlutir sem ferðast um netið			
4	Loforð sem góð VPN-þjónusta gefur			
5	Leyndarmál sem þú myndir dulkóða			
6	Hlutir sem VPN getur ekki verndað þig fyrir			
7	Leiðir til að þekkja falskt Wi-Fi net			
8	Orð tengd friðhelgi			
9	Tæki sem geta notað VPN			
10	Hlutir sem gerast þegar þú ýtir á „Tengjast“			
11	Staðir þar sem þú myndir nota VPN			
12	Ástæður fyrir því að nota VPN á ferðalögum			
13	Hlutir í raunheimum sem líta út eins og göng			
14	Orð úr þessu verkefnablaði sem þú vilt muna			
15	Orð til að útskýra VPN fyrir barni			

Áfangi 8: Dæmisögur um VPN

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

SARAH (NEMANDI Á KAFFIHÚSI)

👩‍💻 „Halló! Ég sit á Coffee & Bytes. Þar er óvarið almenningsnet sem heitir ‚Free_Wi-Fi_No_Password'. Ég vil skrá mig inn á skólapóstinn minn og skila verkefninu mínu, en ég hef áhyggjur af tölvuþrjótum. Hverjar eru áhætturnar af því að nota þetta net án VPN og hvernig tryggir VPN gögnin mín?"

ALEX (FERÐALANGUR OG NEMANDI)

👩‍💻 „Æ nei! Ég er á ferðalagi erlendis vegna verkefnis og er að reyna að horfa á líffræðiheimildarmynd sem hýst er á netþjóni í heimalandi mínu. En vefsvæðið segir ‚This video is not available in your current location.' Hvers vegna er ég útilokuð/aður og hvernig getur VPN hjálpað mér að horfa á hana?"

Áfangi 9: Leystu dulmálið

VPN dulkóðar umferðina þína til að tryggja hana. Notaðu lykilinn „bókstafur í tölu“ hér að neðan til að afkóða öryggisskilaboðin 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

28	7	23	18	5	1	6	26		9	23	12	6	11	7	16	10	12

34	13	18	1		17	7	6		36	23	26	10	10	26	17

10	36	18	10	26	17

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 sem væntanlegir viðskiptavinir hafa um sýndareinkanet.

Q1: Hvað er VPN og hvernig virkar það?

Sýndareinkanet (VPN) dulkóðar nettenginguna þína og beinir umferðinni í gegnum öruggan fjarnetþjón. Þetta felur opinberu IP-töluna þína og takmarkar það sem eftirlitsaðilar á staðarneti og netþjónustuveitan þín geta séð um umferð sem fer um VPN-göngin.

Q2: Hvers vegna ætti ég að nota VPN?

VPN verndar stafræna persónuvernd þína, tryggir tenginguna á opnum Wi-Fi netum (eins og á kaffihúsum eða flugvöllum), getur dregið úr hraðatakmörkunum sem byggjast á virkni þegar netþjónustuveitan getur ekki greint hvers konar dulkóðuð umferð er um að ræða, fer framhjá landfræðilegum takmörkunum til að nálgast efni um allan heim og hjálpar til við að tryggja auðlindir í fjarvinnu.

Q3: Gerir VPN mig algerlega nafnlausan á netinu?

Nei. Þótt VPN feli IP-töluna þína og dulkóði umferð er enn hægt að rekja þig með vafrakökum, virkum reikningum (eins og Google eða Facebook), fingrafaragreiningu vafra eða ef VPN-þjónustuveitan skráir gögnin þín.

Q4: Hægir VPN á nethraðanum mínum?

Já, örlítið. Dulkóðunarferlið og líkamleg fjarlægð að VPN-netþjóninum bæta við seinkun og álagi. Áhrifin eru breytileg eftir þjónustuveitu, samskiptareglu, fjarlægð að netþjóni, tæki og netaðstæðum.

Q5: Er löglegt að nota VPN?

Notkun VPN er lögleg í mörgum löndum, en sum lögsagnarumdæmi takmarka, stýra eða loka á VPN-þjónustu. Notendur ættu að kanna gildandi staðbundin lög áður en þeir nota VPN. Nánari upplýsingar er að finna í leiðbeiningum um lögmæti á VPN.com.

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

Farðu yfir algengustu spurningar og svör sem væntanlegir viðskiptavinir hafa um sýndareinkanet.

Q6: Get ég notað ókeypis VPN?

Ókeypis VPN geta reitt sig á auglýsingar, takmarkaða eiginleika, notkunargreiningu, gagnahámark eða önnur tekjulíkön. Notendur ættu að kynna sér persónuverndarstefnu þjónustuveitunnar, eignarhald, úttektir og viðskiptalíkan áður en þeir nota hana.

Q7: Hvað er stefna um „engar skrár“ („no-logs“)?

Stefna um engar skrár lýsir því hvaða virkni og tengigögn þjónustuveita segist ekki varðveita. Umfangið er mismunandi, svo lesendur ættu að fara yfir stefnuna og niðurstöður óháðra úttekta.

Q8: Hvernig vel ég besta VPN-ið?

Leitaðu að úttektuðum stefnum um enga skráningu, sterkum samskiptareglum (WireGuard, OpenVPN), öruggum staðsetningum netþjóna, miklum hraða, netþjónum með eingöngu vinnsluminni, kill switch-eiginleika og lögsögu utan leyniþjónustusamstarfs (eins og 5/9/14 Eyes).

Q9: Get ég notað VPN í símanum og snjallsjónvarpinu?

Já. Nútímalegar VPN-þjónustuveitur bjóða sérstök forrit fyrir iOS, Android, macOS, Windows, Linux og snjallsjónvörp, auk beinauppsetninga sem vernda öll tæki á heimilisnetinu.

Q10: Hvað er Kill Switch?

Kill switch er öryggiseiginleiki sem aftengir tækið þitt sjálfkrafa frá netinu ef VPN-tengingin rofnar. Þetta kemur í veg fyrir að ódulkóðuð gögn þín eða raunveruleg IP-tala leki út.

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

Kannaðu tæknilega og uppbyggingarlega þætti sýndareinkaneta og öruggra göngusamskiptareglna.

Q1: Hver er munurinn á WireGuard, OpenVPN og IKEv2?

WireGuard eru nútímalegar, léttar samskiptareglur (aðeins um 4.000 kóðalínur) sem bjóða upp á mikinn hraða og stuttan tengitíma. OpenVPN eru mjög öruggar og margreyndar opnar samskiptareglur. IKEv2 hentar vel fyrir farsíma því það getur tengst fljótt aftur þegar skipt er um net. [4]

Q2: Hvað er tvöfalt VPN eða Multi-Hop-leiðarval?

Multi-Hop beinir umferð þinni í gegnum tvo eða fleiri VPN-netþjóna í röð. Það bætir við öðru lagi dulkóðunar og hjálpar til við að halda raunverulegri IP-tölu þinni falinni fyrir öðru hoppinu ef einn netþjónn er í hættu.

Q3: Hvað er WebRTC-leki og hvernig kemur VPN í veg fyrir hann?

WebRTC er samskiptaregla í vöfrum sem getur afhjúpað raunverulegar staðar- og opinberar IP-tölur þínar jafnvel þegar VPN er virkt. Vönduð VPN loka á eða afvegaleiða WebRTC-beiðnir í forritum fyrir borðtölvur og síma og í vafraviðbótum.

Q4: Hvað eru netþjónar sem keyra eingöngu í vinnsluminni og hvers vegna skipta þeir máli?

Hefðbundnir netþjónar skrifa gögn á harða diska sem hægt er að leggja hald á eða brjótast inn í. Netþjónar eingöngu með vinnsluminni (RAM) án diska keyra alfarið í rokgjörnu minni (RAM). Þegar netþjónninn er endurræstur eða slökkt er á honum eyðast gögnin í minninu.

Q5: Hvernig kemst dulbúningur (Obfuscation) framhjá VPN-lokunum?

Dulbúningur (eða „Stealth VPN“) lætur VPN-umferð líta út eins og venjulega HTTPS-umferð (gátt 443). Það getur hjálpað henni að komast framhjá djúpri pakkaskoðun (DPI), sem stjórnvöld eða skóla- og skrifstofunet nota til að loka á VPN.

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

Kannaðu tæknilega og uppbyggingarlega þætti sýndareinkaneta og öruggra göngusamskiptareglna.

Q6: Hvað er skipting umferðar (Split Tunneling) og hvenær ætti ég að nota hana?

Split Tunneling leyfir þér að velja hvaða forrit fara um dulkóðuðu VPN-göngin og hver tengjast beint við internetið. Notaðu það til að beina viðkvæmum bankaforritum um VPN meðan staðbundnir leikir tengjast beint og forðast þannig svartíma sem VPN bætir við.

Q7: Hvernig virkar framvirk leynd (Perfect Forward Secrecy)?

PFS tryggir að einstakur, tímabundinn dulkóðunarlykill sé búinn til fyrir hverja einustu lotu. Jafnvel þótt einkalykill komist í hættu síðar er ekki hægt að nota hann til að afkóða fyrri eða síðari lotur, því þær notuðu óháða lykla.

Q8: Hvað eru bandalögin 5/9/14 Eyes og hvers vegna ætti mér ekki að standa á sama?

Lögsaga getur haft áhrif á lagalegt ferli sem þjónustuveita gæti staðið frammi fyrir, en raunveruleg persónuverndaráhætta fer einnig eftir því hvaða gögn þjónustuveitan varðveitir, tæknilegri uppbyggingu, eignarhaldi, gagnsæisskýrslum og úttektarsögu.

Q9: Hvað er vörn gegn DNS-leka?

DNS-lekavörn lætur tækið þitt senda vefuppflettingar (DNS-fyrirspurnir) í gegnum dulkóðaða einka-DNS-þjóna VPN-þjónustunnar í stað þjóna netþjónustuveitunnar þinnar. Þetta kemur í veg fyrir að netþjónustuveitan þín geti fylgst með því hvaða vefsvæði þú heimsækir.

Q10: Getur VPN sneitt hjá hraðatakmörkunum netþjónustuveitu?

Stundum. VPN getur hjálpað þegar netþjónustuveita hægir sértækt á þekkjanlegri virkni, en það vinnur ekki bug á þrengslum, gagnamörkum, hraðatakmörkunum á reikningi eða lélegum netgæðum.

Hluti 11: 10 áhugaverðar staðreyndir um VPN og innsýn úr raunheimum

Farðu yfir þessar verðmætu, raunverulegu staðreyndir og innsýn um sögu, markað og tækni VPN.

1. FYRSTA VPN-SAMSKIPTAREGLAN

PPTP (Point-to-Point Tunneling Protocol) var þróað af hópi söluaðila, þar á meðal Microsoft, og gefið út sem RFC 2637 í júlí 1999 til að styðja VPN fyrir fjaraðgang. [6]

2. MARKAÐSVIRÐISMAT

Alþjóðlegur VPN-markaður hefur vaxið hratt, knúinn áfram af aukinni þörf fyrir fjarvinnu og öryggiskröfum fyrirtækja.

3. WIREGUARD-BYLTINGIN

WireGuard er með mjög straumlínulagaðan kóðagrunn sem er hannaður með skilvirkni í huga, sem gerir auðveldara að rýna í hann með tilliti til öryggisveikleika en hefðbundnar samskiptareglur. [4]

4. STRANGIR ÚTTEKTARSTAÐLAR

Fremstu VPN-þjónustuveitur ráða utanaðkomandi úttektaraðila (eins og Cure53 eða PwC) til að gera óháðar kóðarýnir og staðfesta að þær skrái enga notendavirkni.

5. UPPRUNI 5-EYES BANDALAGSINS

Five Eyes-bandalagið spratt úr UKUSA-samkomulaginu frá 1946 um merkjagreind milli Bandaríkjanna og Bretlands, sem Kanada, Ástralía og Nýja-Sjáland gengu síðar til liðs við.

6. DJÚP PAKKASKOÐUN

Dýptarskoðun gagnapakka (DPI) skoðar innihald pakka og umferðarmynstur, ekki bara hausa, og sumir eldveggir nota hana til að greina og loka á algengar VPN-samskiptareglur.

7. NOTKUN FYRIRTÆKJA

Stórt hlutfall starfsmanna fyrirtækja um allan heim notar örugg VPN til að skrá sig inn í innri gagnagrunna, sem gerir það að lykilöryggisstaðli.

8. DREIFSTÝRÐ VPN

Dreifstýrð VPN (dVPN) dreifa umferð yfir net hnúta sem jafningjar reka, sem dregur úr því að treyst sé á einn miðlægan þjónustuveitanda.

9. NAFNLEYND Í TOR OG VPN

VPN beinir umferð í gegnum eina þjónustuveitu, en Tor (The Onion Router) sendir umferð í gegnum þrjá sjálfboðaliðahnúta (inngangs-, milli- og útgönguhnút) svo enginn einn hnútur þekki báða enda.

10. KOSTNAÐUR VIÐ GAGNALEKA

Að nota öryggisaðgangslíkan með engu trausti (zero-trust) ásamt VPN hjálpar fyrirtækjum að vernda hugverk og draga úr fjárhagslegum áhrifum gagnaleka.

Tæknilegar heimildir og tilvísanir

Heimildir, dulritunarforskriftir og opinberir skjalastaðlar sem vísað er til í þessu verkefnablaði.

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Lausnir: Verkefnablað um hvað VPN er

1 **Aðalhlutverk** SAMSKIPTAREGLUR **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

Meginhlutverk VPN er að koma á dulkóðuðum göngum sem verja gagnahluta pakka og fela opinbera IP-tölu notandans. Heimild: IETF Tunnel RFC.

2 **Netgöng** SEINKUN **Rétt svar: D**

ATHUGASEMD FYRIR KENNARA

Gangasamskiptareglur hjúpa upprunalega gagnapakka innan ytri burðarpakka til að fara örugglega yfir opinber net. Heimild: IETF Tunnel RFC.

3 **Spurning 3** **Rétt svar: B**

ATHUGASEMD FYRIR KENNARA

Hvaða dulkóðunarstaðall er víða notaður til að verja VPN-umferð? → Nútímalegi AES-256 staðallinn

4 **Dulkóðaðir þættir** STÝRINGAR LEIÐARVALS **Rétt svar: C**

ATHUGASEMD FYRIR KENNARA

VPN dulkóðar allan gagnahluta IP-gagnapakka og heldur innihaldi sendingarinnar leyndu. Heimild: IETF Tunnel RFC.

5 **Spurning 5** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Dulkóðun notar reiknirit og lykil til að breyta ódulkóðuðum texta í ólæsilegan dulkóðaðan texta.

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Hlerunarvörn** GRÍMUN IP-TÖLU — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Dulkóðuð göng tryggja að pakkahlass séu ólæsileg þeim sem hlera gögn á staðbundnum Wi-Fi netum. Heimild: Deloitte Advisory.

7 **Breytingar á vélbúnaði** HRAÐI — **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

VPN eru hugbúnaðarbundin netgöng og breyta ekki efnislega vélbúnaði gáttarbeinisins þíns. Heimild: Cure53 Audit.

8 **Gangapakkar** HLERUNARHÆTTA — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Gangagerð virkar þannig að upprunalegum netpökkum er pakkað inn í flutningshausa á meðan þeir eru á leiðinni. Heimild: IETF Tunnel RFC.

9 **Samhverfir lyklar** ELDVEGGIR — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Samhverf dulritun nýtir sameiginlegan lykil bæði til að dulkóða og afkóða netstrauma. Heimild: WireGuard Project.

10 **Ónæmi gegn afli** ENGIN SKRÁNING — **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

VPN dulkóðar aðeins virk tengingarmerki; það getur ekki komið í veg fyrir truflanir á þjónustu vegna rafmagnsleysis á staðnum. Heimild: EDRi Retention Guidelines.

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

H 1. Göng	E 2. Samskiptaregla	G 3. Bandvídd	A 4. Netþjónn
C 5. Landfræðileg lokun	D 6. Eldveggur	F 7. Persónuvernd	B 8. Netþjónustuveita

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 HJÚPUN	2 BANDBREIDD	3 LANDLÆSING	4 SAMSKIPTAREGLA
5 ELDVEGGUR	6 NETÞJÓNN		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 B – SAMSKIPTAREGLA	2 E – LANDLÆSING	3 F – ELDVEGGUR	4 G – FRIÐHELGI
5 H – NETVEITA	6 A – HJÚPUN	7 D – NETÞJÓNN	8 C – BANDBREIDD

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt Göng, Samskiptaregla og Bandvídd með eigin orðum og gefið dæmi um hvert hugtak.

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

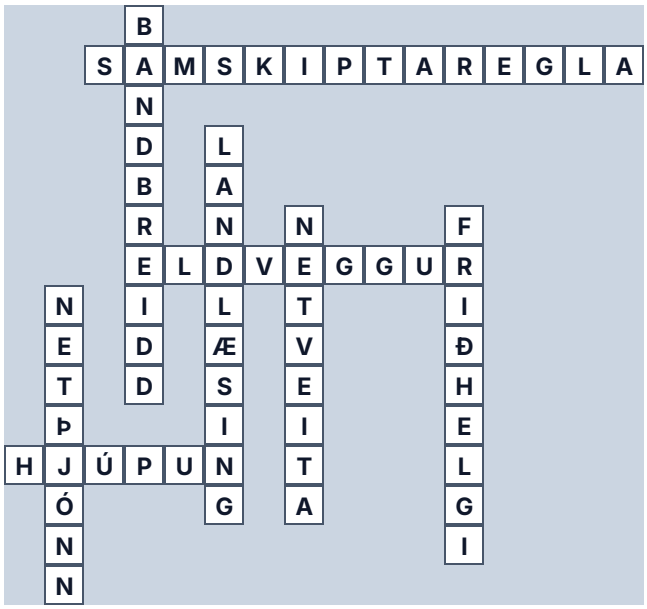
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

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

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

2 lárétt: SAMSKIPTAREGLA Safn reglna sem ákvarða hvernig gögn eru send yfir netið (14 stafir)

6 lárétt: ELDVEGGUR Öryggiskerfi sem vaktar og lokar á óheimila umferð (9 stafir)

8 lárétt: HJÚPUN Að vefja gagnapökkum inn í annan pakka fyrir örugga flutninga (6 stafir)

LÓÐRÉTT

1 lóðrétt: BANDBREIDD Hámarkshraði gagnaflutnings yfir tengingu (10 stafir)

3 lóðrétt: LANDLÆSING Takmörkun sem hindrar vefaðgang eftir líkamlegri staðsetningu (10 stafir)

4 lóðrétt: NETVEITA Netþjónustuveita sem skráir umferð þína nema hún sé dulkóðuð (8 stafir)

5 lóðrétt: FRIÐHELGI Það að vera laus við rakningu eða opinbert eftirlit (9 stafir)

7 lóðrétt: NETÞJÓNN Fjartengd tölva sem beinir umferð þinni og felur IP-töluna þína (8 stafir)

Lausnir: Stafaruglingur og dulmál

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

LYKILL ORÐARAÐAR

1. ÚHPUNJ — **HJÚPUN**
2. DDBABDEIRN — **BANDBREIDD**
3. LÆNSALGDIN — **LANDLÆSING**
4. HIGÐLEFRI — **FRIÐHELGI**
5. RMGATAKAIEPSLS — **SAMSKIPTAREGLA**
6. NNÞÓNJET — **NETÞJÓNN**
7. GEURGVLED — **ELDVEGGUR**
8. VEEANTIT — **NETVEITA**

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"VERNDAÐU FRIÐHELGI ÞÍNA MEÐ ÖRUGGUM GÖNGUM"

Lausnir dæmisagna

A Aðstæður A: Öryggi á opinberum netum

HLERUN OG DULKÓÐUN

Vandi Sarah

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Áhætta: Pakkahlerun, gagnahlerun og maður-í-miðjunni-árásir. Einhver á sama kaffihúsaneti gæti náð innskráningarupplýsingum hennar eða heimaverkefnisskrá.
- VPN-vörn: Dulkóðar innihald netpakka, sem gerir hleraða göngumferð ólæsilega hlutlausum hlerurum á staðarneti þegar VPN er rétt stillt.

B Aðstæður B: Aðgangur að lokuðum úrræðum

LANDFRÆÐILEGAR LOKANIR OG IP-TÖLUR

Vandi Alex

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Hvers vegna lokað: Streymisveitan notar landlæsingu, sem tengir staðbundna IP-tölu ferðalangsins við raunverulegt land hans og lokar á hana á grundvelli landsbundinna leyfa.
- Hvernig VPN hjálpar: Með því að fela raunverulega staðsetningu hans og leiða umferðina um netþjón í heimalandi hans. Vefsvæðið sér IP-tölu heimalandsins og veitir aðgang.