Nafn: _____ Dagsetning: _____ Stig: _____

# Leiðbeiningar um öruggasta VPN

Tæknileg greining á hönnun VPN með mikið öryggi, netþjónum eingöngu í rokgjörnu vinnsluminni, Zero Trust-aðgangsöryggi, vörnum gegn DNS-leka með dulkóðuðu einka-DNS og úttektum á WireGuard-stillingum.

## YFIRLIT UM ÖRUGGASTA 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 tæknilega staðla mjög öruggra VPN-þjónusta. Þú munt kynnast vélbúnaði netþjóna með eingöngu RAM, Zero Trust-aðgangsöryggi, einka-dulkóðuðum DNS-upplausnarþjónum og endurskoðuðum WireGuard-stillingum.

### 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/oruggasta-vpn/

# Námsvegvísir þinn: öruggasta VPN-ið

- Greindu tæknilega uppbyggingu og dulkóðunarstaðla í leiðarvísinum Most Secure VPN.
- Stilltu stillingar biðlara til að koma í veg fyrir leka á IP-tölu, DNS og WebRTC-umferð.
- Berðu saman séreignarsamskiptareglur fyrir göng við hefðbundnar útfærslur.

### LEIÐBEININGAR UM ÖRUGGASTA VPN

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á netþjónabúnað sem notar eingöngu vinnsluminni (RAM) og Zero Trust-kerfi. Ljúktu með aukaverkefninu Hugsaðu hratt.

### INNVIÐIR EINGÖNGU Í VINNSLUMINNI OG ZERO TRUST-NET (INNGANGUR)

Raunverulega öruggt VPN byggir á Zero Trust-ramma, netþjónum eingöngu með vinnsluminni til að koma í veg fyrir að upptaka diska afhjúpi skrár, einka-dulkóðuðum DNS-nafnaþjónum og endurskoðuðum samskiptareglum eins og WireGuard. Þessar samtvinnuðu varnir verja verðmætar stafrænar eignir gegn hlerunarógnum.

**LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.**

# Áfangi 1: Fjölvalsáskorun

**1** **1. Hvaða arkitektúr er grundvallaratriði til að tryggja hæsta öryggi í nútíma VPN-netþjónum?**

- A) Netþjónainnviðir eingöngu með vinnsluminni
- B) Diskageymsla
- C) Kvikt DNS-leiðarval
- D) Virkjun portaframsendingar

**2** **2. Hvaða samskiptareglum er víða mælt með fyrir öruggustu og nútímalegustu VPN-stillingarnar?**

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

**3** **3. Hvaða öryggisrammi krefst þess að hver tenging sé staðfest stöðugt án undantekninga?**

- A) Zero Trust-arkitektúr
- B) Jaðareldveggir
- C) Kvikt leiðarval
- D) Sameiginlegir leynilyklar

**4** **4. Hvert er meginhlutverk DNS-lekavarnar í VPN-forriti?**

- A) Beinir öllum DNS-beiðnum í gegnum einka-dulkóðaða nafnaþjóna
- B) Torkenna IP-pakka
- C) Geyma DNS-fyrirspurnir í skyndiminni á staðnum
- D) Slökkva á nafnaþjónum

**5** **5. Hvernig eykur fjölþrepa leiðing (Multi-Hop) heildaröryggi VPN-ganga?**

- A) Beinir gögnum í gegnum tvo aðskilda netþjóna í röð
- B) Eykur þjöppunarhraða
- C) Dulkóðar gögn með veikum dulmálum
- D) Sniðgengur eldveggi

## Áfangi 2: Satt eða ósatt

### 6 Spurning 6

6. Netþjónar eingöngu í vinnsluminni geyma skrár í skammvinnu minni sem þurrkast út við endurræsingu.

Satt Ósatt

### 7 Spurning 7

7. WireGuard notar nútímaleg dulritunaralgrím sem eru síður viðkvæm fyrir hraðaflöskuhálsum.

Satt Ósatt

### 8 Spurning 8

8. Kill switch í VPN virkar þannig að hann lokar á alla netumferð ef göngin falla niður.

Satt Ósatt

### 9 Spurning 9

9. Óháðar úttektir þriðju aðila skipta engu máli við að staðfesta öryggisskuldbindingar.

Satt Ósatt

### 10 Spurning 10

10. Zero Trust-líkön gera ráð fyrir að allar innri nettengingar séu öruggar sjálfgefið.

Satt Ósatt

## Áfangi 3: Lykilhugtök fyllt inn

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

1. Stjórnendur framfylgja öryggi með því að innleiða strangan _____ ramma.
2. Að beina pökkum um marga inngangspunkta krefst öruggrar _____ uppsetningar.
3. Gagnaleki úr stolnum netþjónum er útilokaður þar sem _____ hönnun er notuð.
4. Dregið er úr yfirtöku netþjónustuveitu með því að stilla innbyggða eiginleika á borð við _____ .
5. Til að loka á umferð þegar tenging bilar skaltu virkja _____ búnaðinn.
6. Til að lágmarka geymdar skrár í gagnagrunnum skaltu velja veitu sem býr yfir fullu _____ .

**ORÐABANKI**

DISKALAUS DNS-VÖRN DULKÓÐUN KILL SWITCH MULTI-HOP SAMSKIPTAREGLA ÚTTEKTARKERFI ZERO TRUST

**Skrifaðu svörin þín hér:**

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

# Áfangi 4: Pörun hugtaka um VPN og net

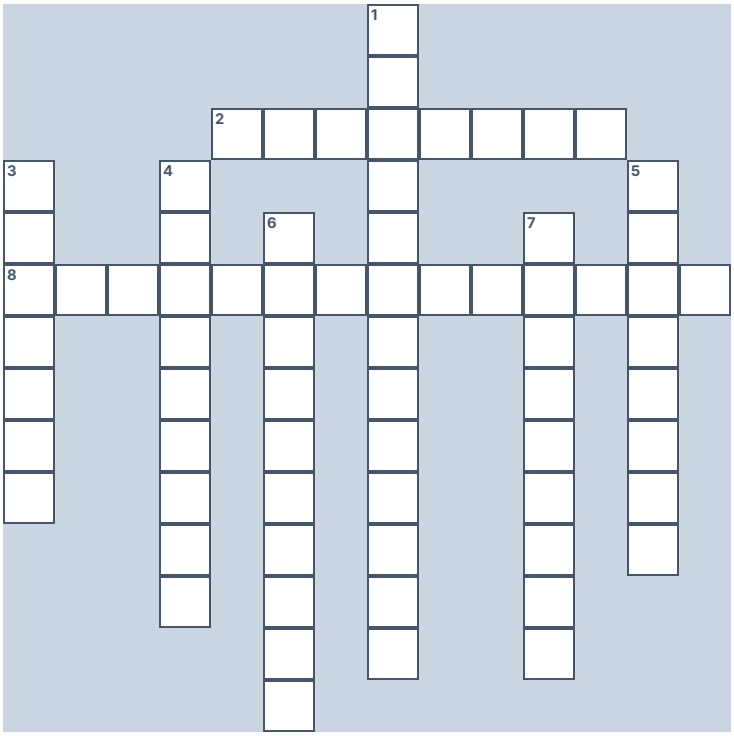
**PÖRUN SKILGREININGA**

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

| | | | |
|---|---|---|---|
| ☐ | 1. Zero Trust | A | Óháð skoðuð uppsetning sem staðfestir að engar skrár eru geymdar. |
| ☐ | 2. Multi-Hop | B | Dulritunarbrengling á gögnum til að tryggja flutning. |
| ☐ | 3. Netþjónn eingöngu í vinnsluminni | C | Öryggisrammi sem krefst stöðugrar auðkenningar allra notenda. |
| ☐ | 4. DNS-vörn | D | Safn tæknilegra reglna sem ákvarða hvernig gögn eru pökkuð og send. |
| ☐ | 5. Kill Switch | E | VPN-leiðarstýring í röð sem tengir saman tvo netþjónahnúta. |
| ☐ | 6. Úttektarsannað kerfi | F | Netþjónaarkitektúr sem notar rokgjarnt minni til að geyma gagnafarma. |
| ☐ | 7. Dulkóðun | G | Að framfylgja einka-DNS-fyrirspurnum til að vernda uppflettingar nafnaþjóna. |
| ☐ | 8. Samskiptaregla | H | Öryggisbúnaður sem lokar á umferð ef VPN bilar. |

# Áfangi 5: Krossgáta

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



## LÁRÉTT

**2. Raðtengt VPN-leiðarval sem tengir saman tvo netþjónshnúta (8)**

**8. Safn tæknilegra reglna sem ákvarða hvernig gögn eru pökkuð og send (14)**

## LÓÐRÉTT

**1. Óháð rýnd uppsetning sem staðfestir að engar skrár séu geymdar (13)**

**3. Að framfylgja einkafyrirspurnum DNS til að vernda nafnaleit (7)**

**4. Netþjónaarkitektúr sem notar rokgjarnt minni til að geyma gagnahleðslu (9)**

**5. Dulmálsfelun gagnahleðslu til að tryggja gagnaflutning (8)**

**6. Öryggisbúnaður sem lokar á umferð ef VPN bilar (10)**

**7. Öryggisrammi sem krefst stöðugrar auðkenningar allra notenda (9)**

# 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: Raðtengt VPN-leiðarval sem tengir saman tvo netþjónshnúta (8 stafir):**

**8 lárétt: Safn tæknilegra reglna sem ákvarða hvernig gögn eru pökkuð og send (14 stafir):**

## LÓÐRÉTT

**1 lóðrétt: Óháð rýnd uppsetning sem staðfestir að engar skrár séu geymdar (13 stafir):**

**3 lóðrétt: Að framfylgja einkafyrirspurnum DNS til að vernda nafnaleit (7 stafir):**

**4 lóðrétt: Netþjónaarkitektúr sem notar rokgjarnt minni til að geyma gagnahleðslu (9 stafir):**

**5 lóðrétt: Dulmálsfelun gagnahleðslu til að tryggja gagnaflutning (8 stafir):**

**6 lóðrétt: Öryggisbúnaður sem lokar á umferð ef VPN bilar (10 stafir):**

**7 lóðrétt: Öryggisrammi sem krefst stöðugrar auðkenningar allra notenda (9 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 T P T H Æ Á G L Ö G J O P N
F S O Ý B C L Ö Æ F Þ Ó Y V D
R U H K V P T Á O X Ú L G N X
E R I D Þ V J I S Á Ý Ö S Þ M
K T T T R Ý I Ó W Đ A V D J R
R O L Y Ý Ý K Í H S Ö Ú H F Á
A R U É I K U T Y R L S Ö E H
T E M É T D A L N P B L Ö M J
K Z X S V A T Ý J M M G I H N
E H S F N U Đ Ó K L U D K K U
T S A M S K I P T A R E G L A
T L S Ý H B V É Þ O Æ Ý T H Ú
Ú Ý D I S K A L A U S A P V N
O Æ Ó I P U H Ó X Ú Ó V Ú J A
E Ó M K Á O X F G P R Ý Æ Í J

**ORÐALISTI**

ZEROTRUST MULTIHOP DISKALAUS DNSVÖRN KILLSWITCH ÚTTEKTARKERFI DULKÓÐUN SAMSKIPTAREGLA

# 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. ZEROTRUST |
| B. MULTIHOP |
| C. DISKALAUS |
| D. DNSVÖRN |
| E. KILLSWITCH |
| F. ÚTTEKTARKERFI |
| G. DULKÓÐUN |
| H. SAMSKIPTAREGLA |

| SKILGREININGAR OG PÖRUNARREITIR | |
| --- | --- |
| | 1. Öryggisbúnaður sem lokar á umferð ef VPN bilar. |
| | 2. Að framfylgja einkafyrirspurnum DNS til að vernda nafnaleit. |
| | 3. Raðtengt VPN-leiðarval sem tengir saman tvo netþjónshnúta. |
| | 4. Safn tæknilegra reglna sem ákvarða hvernig gögn eru pökkuð og send. |
| | 5. Dulmálsfelun gagnahleðslu til að tryggja gagnaflutning. |
| | 6. Netþjónaarkitektúr sem notar rokgjarnt minni til að geyma gagnahleðslu. |
| | 7. Óháð rýnd uppsetning sem staðfestir að engar skrár séu geymdar. |
| | 8. Öryggisrammi sem krefst stöðugrar auðkenningar allra notenda. |

## 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. **RTOEZUSTR** _____
2. **SDUKILAAS** _____
3. **KWCIISHLTL** _____
4. **KUNÐÓDUL** _____
5. **IHUPTMOL** _____
6. **RSÖDVNN** _____
7. **ERRTÚTKKIFTAE** _____
8. **STGIARAASPMLEK** _____

# Aukaverkefni: Hugsaðu hratt

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

| | | | | |
|---|---|---|---|---|
| 1 | Lásar eða lyklar sem þú notar daglega | | | |
| 2 | Hlutir sem VPN getur falið | | | |
| 3 | Hlutir sem gera VPN öruggt | | | |
| 4 | Mýtur um VPN | | | |
| 5 | Ástæður fyrir því að nota VPN á ferðalögum | | | |
| 6 | Öruggir staðir í raunheimum | | | |
| 7 | Orð sem þýða „varinn“ | | | |
| 8 | Loforð sem góð VPN-þjónusta gefur | | | |
| 9 | Orð tengd friðhelgi | | | |
| 10 | Tegundir úttekta eða skoðana | | | |
| 11 | Orð úr þessu verkefnablaði sem þú vilt muna | | | |
| 12 | Hlutir sem tölvuþrjótur vill stela | | | |
| 13 | Leiðir til að þekkja falskt Wi-Fi net | | | |
| 14 | Staðir þar sem þú myndir nota VPN | | | |
| 15 | Hlutir sem netþjónustuaðilinn þinn getur séð | | | |

# Áfangi 8: Dæmisögur um VPN og net

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

### DÆMISAGA 1: STYRKING INNVIÐA FYRIRTÆKJA



**Aðstæður:** Banki endurhannar tengingarskipulag fjaraðgangs. Hann krefst Zero Trust-arkitektúrs sem tengir öll biðlaratæki við örugga netþjóna.

**Umræðuspurning:** Hver er helsti ávinningur örskiptingar nets (micro-segmentation) samkvæmt Zero Trust VPN-líkani?

### DÆMISAGA 2: VÖRN NETÞJÓNA MEÐ AÐEINS VINNSLUMINNI



**Aðstæður:** VPN-þjónustuaðili með áherslu á öryggi uppfærir netþjóna sína til að koma í veg fyrir að líkamleg haldlagning netþjóns afhjúpi notendaskrár.

**Umræðuspurning:** Útskýrðu hvernig vélbúnaðaruppsetningar eingöngu með vinnsluminni koma í veg fyrir réttarfræðilega gagnaöflun við líkamlega haldlagningu netþjóna.

# 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**

| 36 | 23 | 26 | 10 | | 28 | 21 | 18 | | 28 | 7 | 23 | 18 | 5 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | |

| 28 | 7 | 23 | 6 | 17 | 35 | 25 | 1 | 23 | | 24 | 25 | 1 | 9 | 23 | 35 | 18 | 1 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | |

| 7 | 12 | 10 | 18 | 12 | 23 |
|---|---|---|---|---|---|
| | | | | | |

**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 gerir VPN „öruggast“?

Sambland af Zero Trust, netþjónum eingöngu með vinnsluminni og endurskoðuðum samskiptareglum.

### Q2: Hvað eru netþjónar sem nota eingöngu vinnsluminni?

Netþjónar sem keyra í rokgjörnu minni og eru hannaðir til að vista engar skrár á diski.

### Q3: Hvað er Zero Trust VPN?

Rammi sem sannreynir stöðugt hverja aðgangsbeiðni og tengingu.

### Q4: Hvers vegna er WireGuard talið öruggt?

Það hefur lítinn kóðagrunn sem auðvelt er að gera úttekt á og notar nútímadulmál.

### Q5: Hvernig koma öruggar VPN-þjónustur í veg fyrir DNS-leka?

Með því að beina öllum fyrirspurnum í gegnum einka, dulkóðaða DNS-uppflettiþjóna.

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

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

### Q6: Krefst öruggt VPN úttekta?

Já, óháðar úttektir staðfesta fullyrðingar um enga skráningu og öryggi kóðans.

### Q7: Hvert er hlutverk kill switch?

Það stöðvar netumferð tafarlaust ef VPN-tengingin rofnar.

### Q8: Hvaða dulkóðun er notuð í öruggum VPN?

AES-256 og ChaCha20 eru iðnaðarstaðlar fyrir dulkóðun.

### Q9: Er Multi-Hop-leiðarval öruggt?

Já, það tengir saman tvo eða fleiri netþjóna til að koma í veg fyrir umferðargreiningu.

### Q10: Hvernig hjálpar lögsaga á aflandssvæði?

Það getur takmarkað hvaða lög gilda en veitir ekki algjöra friðhelgi.

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

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

### Q1: Hvernig koma netþjónar sem nota eingöngu vinnsluminni í veg fyrir hættu á upptöku gagna?

Þar sem þeir keyra í vinnsluminni (RAM) þurrkar það út gögnin í minninu að kippa úr sambandi.

### Q2: Hvernig kemur Zero Trust í stað hefðbundins jaðaröryggis?

Það lítur á alla biðlara sem fjandsamlega og krefst stöðugrar auðkenningar.

### Q3: Hvað gerir WireGuard-kóðann auðveldari í yfirferð?

Linux-kóði þess er innan við 4,000 línur, mun minni en dæmigerðir VPN-staflar. [4]

### Q4: Hvernig ver DNSSEC DNS-fyrirspurnir?

Það undirritar DNS-færslur svo leysarar geti greint fölsuð eða breytt svör.

### Q5: Hvernig gerir Multi-Hop fylgnigreiningu umferðar erfiðari?

Með því að aðgreina komandi og útsendar IP-tölur á mismunandi hýsingarveitur.

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

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

### Q6: Hvers vegna eru lögsagnarumdæmi Five Eyes áhættusöm fyrir VPN?

Aðildarríki deila leyniþjónustuupplýsingum og geta notað lagalegar fyrirskipanir til að óska eftir notendagögnum.

### Q7: Hvernig er kill switch útfærður á stigi kjarna?

Það notar kerfiseldveggsreglur (eins og iptables eða WFP) til að loka á útleiðandi umferð.

### Q8: Hvað er framvirk leynd í VPN-handtökum?

Það býr til einstaka lotulykla þannig að ekki er hægt að afkóða fyrri lotur.

### Q9: Hvernig draga öruggar VPN-þjónustur úr WebRTC-leka?

Með því að loka á WebRTC-beiðnir eða beina þeim í gegnum göngin.

### Q10: Hvernig tryggja óháðar úttektir að persónuvernd sé virt?

Úttektaraðilar framkvæma skarpskyggnipróf og skoða stillingar netþjóna.

# 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**

Netþjónar eingöngu í vinnsluminni hlaða stýrikerfi sínu í minni við ræsingu, svo ekkert varðveitist á diski eftir endurræsingu.

**2. INNSÝN Í VPN**

WireGuard notar Noise-rammann með Curve25519, ChaCha20, Poly1305, BLAKE2s og HKDF. [3]

**3. INNSÝN Í VPN**

Zero Trust veitir aðgang eftir auðlindum og gefur ekkert ótilgreint traust á grundvelli staðsetningar í neti (NIST SP 800-207). [1]

**4. INNSÝN Í VPN**

Leyniþjónustubandalagið Five Eyes nær til Bandaríkjanna, Bretlands, Kanada, Ástralíu og Nýja-Sjálands.

**5. INNSÝN Í VPN**

WebRTC-lekar verða þegar vafrar afhjúpa raunverulega opinbera IP-tölu notandans í gegnum STUN-fyrirspurnir.

**6. INNSÝN Í VPN**

Fullkomið framvirkt leynd (PFS) tryggir að þótt langtímalykill komist í hættu afhjúpi það ekki fyrri lotulykla. [3]

**7. VPN-INNSÝN**

Cure53, öryggisfyrirtæki í Berlín, hefur birt úttektir á nokkrum VPN-þjónustuveitum.

**8. VPN-INNSÝN**

DNS-lekar verða þegar DNS-fyrirspurnir fara fram hjá VPN-göngunum og til nafnaþjóna netþjónustuveitunnar á staðnum.

**9. VPN-INNSÝN**

Rokgjarnir vinnsluminniskubbar þurfa stöðugt rafmagn til að halda gögnum og tapa innihaldi sínu þegar slökkt er á þeim.

**10. INNSÝN Í VPN**

Zero Trust-kerfi fyrir fyrirtæki framfylgja athugunum á stöðu tækja áður en tenging við örugg föng er leyfð. [1]

# Tæknilegar heimildir og tilvísanir

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

## FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

## Lausnir: Áfangi 1 – Fjölval

**1** **Netþjónn eingöngu í vinnsluminni** EINGÖNGU VINNSLUMINNI Rétt svar: A

### ATHUGASEMD FYRIR KENNARA

Netþjónar eingöngu í vinnsluminni geyma engar skrár á diski og gögnin þurrkast út við endurræsingu. Heimild: Most Secure VPN.

**2** **Spurning 2** Rétt svar: A

### ATHUGASEMD FYRIR KENNARA

WireGuard sameinar lítinn kóðagrunn sem auðvelt er að gera úttekt á og nútímaleg dulmál.

**3** **Zero Trust-líkanið** ZERO TRUST Rétt svar: A

### ATHUGASEMD FYRIR KENNARA

Zero Trust-líkön staðfesta stöðugt að tæki uppfylli kröfur áður en aðgangur er veittur. Tilvitnun: Most Secure VPN.

**4** **DNS-vörn** DNS-VÖRN Rétt svar: A

### ATHUGASEMD FYRIR KENNARA

DNS-lekavörn beinir uppflettingum í gegnum einkaþjóna. Heimild: Most Secure VPN.

**5** **Multi-Hop-göng** MULTI-HOP Rétt svar: A

### ATHUGASEMD FYRIR KENNARA

Multi-Hop-leiðarval tengir tvo aðskilda netþjónahnúta í röð. Heimild: Most Secure VPN.

## Lausnir: Áfangi 2 – Satt eða ósatt

**6** **Netþjónn eingöngu í vinnsluminni** EINGÖNGU VINNSLUMINNI Rétt svar: Satt

### ATHUGASEMD FYRIR KENNARA

Netþjónabúnaður sem keyrir eingöngu í vinnsluminni skrifar engin gögn á disk og þurrkast út við endurræsingu. Heimild: Most Secure VPN.

**7** **Hraði WireGuard** WIREGUARD Rétt svar: Satt

### ATHUGASEMD FYRIR KENNARA

WireGuard notar nútímadulritun sem forðast flöskuhálsa í vinnslu. Heimild: Most Secure VPN.

**8** **Kill Switch** ÖRYGGISROFI Rétt svar: Satt

### ATHUGASEMD FYRIR KENNARA

Kill switch lokar á alla umferð ef VPN-tengingin rofnar. Heimild: Most Secure VPN.

**9** **Úttektir þriðju aðila** ÚTTEKTIR NAUÐSYNLEGAR Rétt svar: Ósatt

### ATHUGASEMD FYRIR KENNARA

Úttektir þriðju aðila eru nauðsynlegar til að sannreyna fullyrðingar fyrirtækja um persónuvernd. Heimild: Most Secure VPN.

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

### ATHUGASEMD FYRIR KENNARA

Zero Trust veitir ekkert óbeint traust byggt á staðsetningu í neti.

# 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. Zero Trust | E 2. Multi-Hop | F 3. Netþjónn eingöngu í vinnsluminni | G 4. DNS-vörn |
| H 5. Kill Switch | A 6. Úttektarsannað kerfi | B 7. Dulkóðun | D 8. Samskiptaregla |

## ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

| | | | |
|---|---|---|---|
| 1 ZERO TRUST | 2 MULTI-HOP | 3 DISKALAUS | 4 DNS-VÖRN |
| 5 KILL SWITCH | 6 ÚTTEKTARKERFI | | |

## ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

| | | | |
|---|---|---|---|
| 1 E – KILLSWITCH | 2 D – DNSVÖRN | 3 B – MULTIHOP | 4 H – SAMSKIPTAREGLA |
| 5 G – DULKÓÐUN | 6 C – DISKALAUS | 7 F – ÚTTEKTARKERFI | 8 A – ZEROTRUST |

## UMRÆÐUATRIÐI FYRIR KENNARA

**Lykilhugtök:**
Athugaðu hvort nemendur geti útskýrt Zero Trust, Multi-Hop og Netþjónn eingöngu í vinnsluminni með eigin orðum og gefið dæmi um hvert hugtak.

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

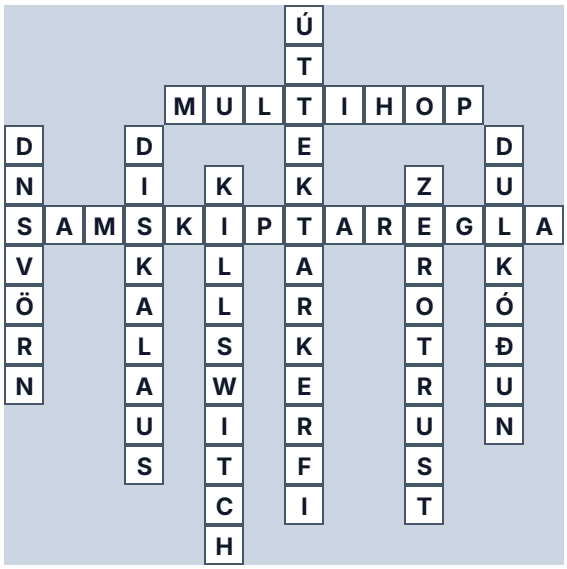
**Mat á heimildum:**
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

# Lausnir við þrautum og athugasemdir fyrir kennara

## LAUSN ORÐALEITAR

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

## LAUSN KROSSGÁTUNNAR




## LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

### LÁRÉTT

**2 lárétt: MULTIHOP** Raðtengt VPN-leiðarval sem tengir saman tvo netþjónshnúta (8 stafir)

**8 lárétt: SAMSKIPTAREGLA** Safn tæknilegra reglna sem ákvarða hvernig gögn eru pökkuð og send (14 stafir)

### LÓÐRÉTT

**1 lóðrétt: ÚTTEKTARKERFI** Óháð rýnd uppsetning sem staðfestir að engar skrár séu geymdar (13 stafir)

**3 lóðrétt: DNSVÖRN** Að framfylgja einkafyrirspurnum DNS til að vernda nafnaleit (7 stafir)

**4 lóðrétt: DISKALAUS** Netþjónaarkitektúr sem notar rokgjarnt minni til að geyma gagnahleðslu (9 stafir)

**5 lóðrétt: DULKÓÐUN** Dulmálsfelun gagnahleðslu til að tryggja gagnaflutning (8 stafir)

**6 lóðrétt: KILLSWITCH** Öryggisbúnaður sem lokar á umferð ef VPN bilar (10 stafir)

**7 lóðrétt: ZEROTRUST** Öryggisrammi sem krefst stöðugrar auðkenningar allra notenda (9 stafir)

# Lausnir: Stafaruglingur og dulmál

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

## LYKILL ORÐARAÐAR

1. RTOEZUSTR — ZEROTRUST
2. SDUKILAAS — DISKALAUS
3. KWCIISHLTL — KILLSWITCH
4. KUNÐÓDUL — DULKÓÐUN
5. IHUPTMOL — MULTIHOP
6. RSÖDVNN — DNSVÖRN
7. ERRTÚTKKIFTAE — ÚTTEKTARKERFI
8. STGIARAASPMLEK — SAMSKIPTAREGLA

## LYKILL AÐ LEYNIDULMÁLSÞRAUT

**"ÖRUG VPN VERNDA VERÐMÆTAR STAFRÆNAR EIGNIR"**

# Lausnir dæmisagna

## A DÆMISAGA 1: STYRKING INNVIÐA FYRIRTÆKJA

Lausn fyrir kennara

### VIÐMIÐ VIÐ EINKUNNAGJÖF

**Svör nemenda ættu að ná yfir eftirfarandi atriði:**

- Greining aðstæðna: Viðskiptabanki endurhannar fjaraðgangsuppbyggingu sína. Hann krefst núlltraustsarkitektúrs sem tengir öll biðlaratæki við örugga netþjóna.
- Ráðlögð aðferð og lausn: Matsleiðbeiningar: Útskýrðu að örskipting netsins takmarkar aðgang við tiltekin föng og kemur í veg fyrir hliðarhreyfingu ógna ef tæki er í hættu.

## B DÆMISAGA 2: VÖRN NETÞJÓNA MEÐ AÐEINS VINNSLUMINNI

Lausn fyrir kennara

### VIÐMIÐ VIÐ EINKUNNAGJÖF

**Svör nemenda ættu að ná yfir eftirfarandi atriði:**

- Greining aðstæðna: VPN-þjónustuveita með áherslu á öryggi uppfærir netþjóna sína til að koma í veg fyrir að líkamleg haldlagning á netþjónum afhjúpi notendaskrársögu.
- Ráðlögð aðferð og lausn: Matsleiðbeiningar: Útskýrðu að netþjónar sem keyra eingöngu í vinnsluminni hafa ekkert diskapláss. Rafmagnsleysi eyðir sjálfkrafa öllum tímabundnum gögnum í rokgjörnu minni.