Nafn: _____ Dagsetning: _____ Stig: _____

WireGuard í samanburði við OpenVPN Verkefnablað

Samanburður á WireGuard og OpenVPN, stærð kóðagrunns, hraða og dulritunarstöðlum

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

- Berðu saman flækjustig kóða og hraða úttekta á samskiptareglum.
- Greindu afkastaaukningu við keyrslu í kjarnarými.
- Berðu OpenSSL-dulrit saman við nútíma dulritun WireGuard.
- Settu upp opinber og leynileg lyklapör fyrir handabönd jafningja.
- Leiða VPN-umferð um TCP- og UDP-eldveggsgáttir.

LEIÐBEININGAR UM VERKEFNI TIL SAMANBURÐAR Á SAMSKIPTAREGLUM

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

WIREGUARD Í SAMANBURÐI VIÐ OPENVPN (INNGANGUR)

Val á VPN-samskiptareglum krefst jafnvægis milli hraða og stillingarmöguleika. OpenVPN hefur verið staðallinn í áratugi og býður sveigjanleika í TCP/UDP-stillingum. WireGuard er nútímalegur arftaki sem keyrir beint í kjarnarými með aðeins 4.000 línum af kóða. Skilningur á muninum á samskiptareglum er lykillinn að því að hámarka örugg net.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hver er áætluð stærð kóðagrunns WireGuard-samskiptareglnanna?**

- A. Um það bil 70.000 línur
- B. Yfir 100.000 línur
- C. Færri en 1.000 línur
- D. Um það bil 4.000 línur

2 **2. Í hvaða rými stýrikerfisins keyrir WireGuard?**

- A. Notendarými
- B. Kjarnarými
- C. Forritarými
- D. Sýndarrými

3 **3. Á hvaða dulritunarsafn reiðir OpenVPN sig fyrst og fremst?**

- A. ChaCha20-Poly1305
- B. OpenSSL-dulritunarsafnið
- C. Noise-samskiptarammann
- D. DES-kóðun í ódulkóðuðum texta

4 **4. Hver er helsti afkastakostur WireGuard umfram OpenVPN?**

- A. Hraðari tengingarhandtök og minni svartími
- B. Með því að komast hjá þörf fyrir opinberar IP-tölur
- C. Innbyggður innfæddur stuðningur við eldri upphringitengingar
- D. Ekkert rafhlöðuálag á farsímum

5 **5. Hvernig staðfestir WireGuard tengingar jafningja?**

- A. Með því að skiptast á venjulegum lykilorðum notenda
- B. Með því að staðfesta skráningarvottorð léna
- C. Með því að nota föst opinber og einkalyklapör
- D. Með því að athuga raðnúmer vélbúnaðar

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Fyrirferðarlítill kóðagrunnur WireGuard gerir mun auðveldara að gera úttekt á honum.

○ Satt ○ Ósatt

7 Spurning 7

7. OpenVPN er almennt hraðvirkara en WireGuard vegna þess að það keyrir í kjarnarými.

○ Satt ○ Ósatt

8 Spurning 8

8. OpenVPN er mjög stillanlegt og styður bæði UDP og TCP.

○ Satt ○ Ósatt

9 Spurning 9

9. WireGuard notar nútímadulritun eins og ChaCha20 fyrir hraða pakkadulkóðun.

○ Satt ○ Ósatt

10 Spurning 10

10. WireGuard krefst flókinnar uppsetningar vottunaraðila til auðkenningar.

○ Satt ○ Ósatt

Áfangi 3: Lykilhugtök fyllt inn

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

1. Nútímalega _____ samskiptareglan starfar beint innan stýrikerfiskjarnans.

2. Eldri _____ samskiptareglan treystir á OpenSSL-dulmálssafnið.

3. Keyrsla kóða á svæði sem kallast _____ dregur úr yfirbyggingu vegna samhengisskipta.

4. OpenVPN keyrir á svæði sem kallast _____ og beinir pökkum um sýndarviðmót.

5. WireGuard notar lykla sem koma í pörum, þ.e. _____ , til að auðkenna tengda jafningja.

6. Lítill kóðagrunnur eykur öryggi hugbúnaðarins og bætir eiginleika sem kallast _____ .

ORÐABANKI

KJARNARÝMI KÓÐASTÆRÐ LYKILPÖR NOTENDARÝMI OPENSSL OPENVPN ÚTTEKTARHÆFNI WIREGUARD

Skrifaðu svörin þín hér:

1. **2.**

3. **4.**

5. **6.**

Áfangi 4: Pörun hugtaka um net

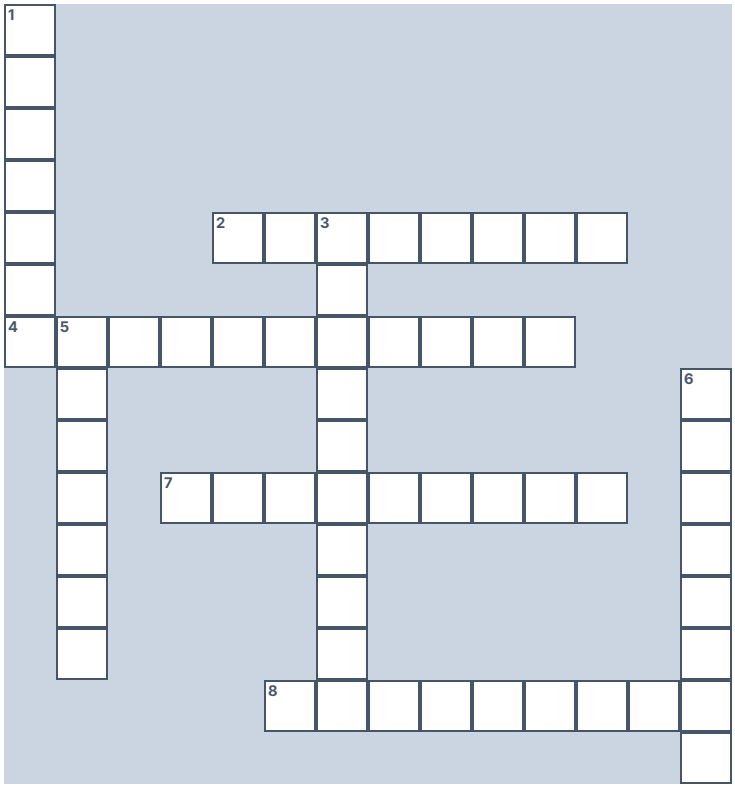
PÖRUN SKILGREININGA

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

☐	1. WireGuard	A	Keyrslusvæði þar sem OpenVPN keyrir, sem skapar samhengisskiptaálag.
☐	2. OpenVPN	B	Þéttur kóðagrunnur WireGuard, sem gerir mun auðveldara að gera á honum úttekt.
☐	3. Kjarnarými	C	Dulritunarsafn sem OpenVPN reiðir sig á fyrir dulritunarreiknirit.
☐	4. Notendarými	D	Flutningsreglur sem OpenVPN styður; WireGuard sjálft keyrir aðeins yfir UDP.
☐	5. 4.000 línur	E	Keyrslusvæði stýrikerfis þar sem WireGuard keyrir til að ná hraða.
☐	6. OpenSSL	F	Ósamhverf tákn sem WireGuard notar til að sannreyna tengingar jafningja.
☐	7. Lyklapar	G	Nútíma VPN-samskiptareglur hannaðar fyrir mikinn hraða og einfalda kóðaúttekt.
☐	8. TCP/UDP	H	Öflug eldri samskiptaregla sem notar stóran og flókinn stillingarkóða.

Áfangi 5: Krossgáta

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



LÁRÉTT

2. Ósamhverfir lyklar sem WireGuard notar til að sannreyna tengda jafningja (8)

4. Framkvæmdarsvæði þar sem OpenVPN keyrir og skapar yfirbyggingu vegna samhengisskipta (11)

7. Smæð kóðagrunns WireGuard sem gerir úttekt mun auðveldari (9)

8. Nútímaleg VPN-samskiptaregla hönnuð fyrir mikinn hraða og einfalda kóðarýni (9)

LÓÐRÉTT

1. Öflug eldri samskiptaregla með stóran og flókinn stillingakóðagrunn (7)

3. Framkvæmdarsvæði stýrikerfis þar sem WireGuard keyrir fyrir hraða (10)

5. Dulmálssafn sem OpenVPN reiðir sig á fyrir dulmálsalgrím (7)

6. Flutningsreglur sem OpenVPN styður; WireGuard sjálft keyrir eingöngu yfir UDP (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: Ósamhverfir lyklar sem WireGuard notar til að sannreyna tengda jafningja (8 stafir):

4 lárétt: Framkvæmdarsvæði þar sem OpenVPN keyrir og skapar yfirbyggingu vegna samhengisskipta (11 stafir):

7 lárétt: Smæð kóðagrunns WireGuard sem gerir úttekt mun auðveldari (9 stafir):

8 lárétt: Nútímaleg VPN-samskiptaregla hönnuð fyrir mikinn hraða og einfalda kóðarýni (9 stafir):

LÓÐRÉTT

1 lóðrétt: Öflug eldri samskiptaregla með stóran og flókinn stillingakóðagrunn (7 stafir):

3 lóðrétt: Framkvæmdarsvæði stýrikerfis þar sem WireGuard keyrir fyrir hraða (10 stafir):

5 lóðrétt: Dulmálssafn sem OpenVPN reiðir sig á fyrir dulmálsalgrím (7 stafir):

6 lóðrétt: Flutningsreglur sem OpenVPN styður; WireGuard sjálft keyrir eingöngu yfir UDP (8 stafir):

Áfangi 6: Falið orð í orðaleit

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

Ú T U E K Í B L A Á B Ó Þ K J

Þ K Ý Ú J Ð R Y M Í T Ð I N N

I L K R P G M K M R C S T Ú Ú

M S G B T P O I H T P B Y Ð U

Ý S Æ V D N Ö L Y F O J G W Ö

R N Ð N Ð O R P Ý P G B V I Á

A E A Ö O T Ð Ö K K U A Ð R O

N P Ð É G E I R Ó O D Ð S E R

R O M E I N T Ö Ð P P U É G R

A X É A A D R Ó A E N P Ú U Þ

J R J S Ú A T D S N N Æ B A F

K T Ý Y Í R A S T V Ö Æ Æ R K

F I M S J Ý L L Æ P U Ó G D P

R G Ö A O M X F R N V B Æ T Æ

Á G L Ö G I J O Ð P N Ý B L Ö

ORÐALISTI

WIREGUARD, OPENVPN, KJARNARÝMI, NOTENDARÝMI, KÓÐASTÆRÐ, OPENSSL, LYKILPÖR, TCPOGUDP

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. WIREGUARD**
- **B. OPENVPN**
- **C. KJARNARÝMI**
- **D. NOTENDARÝMI**
- **E. KÓÐASTÆRÐ**
- **F. OPENSSL**
- **G. LYKILPÖR**
- **H. TCPOGUDP**

SKILGREININGAR OG PÖRUNARREITIR

_____ 1. Dulmálssafn sem OpenVPN reiðir sig á fyrir dulmálsalgrím.

_____ 2. Framkvæmdarsvæði stýrikerfis þar sem WireGuard keyrir fyrir hraða.

_____ 3. Öflug eldri samskiptaregla með stóran og flókinn stillingakóðagrunn.

_____ 4. Ósamhverfir lyklar sem WireGuard notar til að sannreyna tengda jafningja.

_____ 5. Flutningsreglur sem OpenVPN styður; WireGuard sjálft keyrir eingöngu yfir UDP.

_____ 6. Smæð kóðagrunns WireGuard sem gerir úttekt mun auðveldari.

_____ 7. Nútímaleg VPN-samskiptaregla hönnuð fyrir mikinn hraða og einfalda kóðarýni.

_____ 8. Framkvæmdarsvæði þar sem OpenVPN keyrir og skapar yfirbyggingu vegna samhengisskipta.

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. **UGEIWARDR** _____

2. **MRKJNIRÝAA** _____

3. **KTSÓÆÐARÐ** _____

4. **IÖRPLLYK** _____

5. **VNNEOPP** _____

6. **NIDRMÝNOATE** _____

7. **OSSLPNE** _____

8. **OCGPTDUP** _____

Aukaverkefni: Hugsaðu hratt

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

1	Ástæður fyrir því að velja WireGuard			
2	Loforð sem góð VPN-þjónusta gefur			
3	Ástæður fyrir því að velja OpenVPN			
4	Ástæður fyrir því að nota VPN á ferðalögum			
5	Hlutir sem netþjónustuaðilinn þinn getur séð			
6	Leiðir til að þekkja falskt Wi-Fi net			
7	Mýtur um VPN			
8	Staðir þar sem þú myndir nota VPN			
9	Fljótir hlutir í daglegu lífi			
10	Hlutir sem VPN getur ekki verndað þig fyrir			
11	Hlutir sem gera kóða auðveldari að yfirfara			
12	Hlutir sem VPN getur falið			
13	Munur á WireGuard og OpenVPN			
14	Orð tengd friðhelgi			
15	Heiti á dulkóðun sem þú þekkir			

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 er á Wi-Fi á kaffihúsi og VPN-forritið mitt leyfir mér að velja WireGuard eða OpenVPN. Myndsímtölin mín rofna stöðugt þegar ég geng á milli kaffihúsanetsins og heita reitsins í símanum. Hvaða samskiptareglu ætti ég að velja og hvers vegna myndi hún höndla skiptin betur?“

ALEX (FERÐALANGUR OG NEMANDI)

👩‍💻 „Ég er erlendis á hótelneti sem virðist loka á flesta VPN-umferð. WireGuard tengist alls ekki, en ég þarf að komast í úrræði skólans míns heima. Hvað er líklega verið að loka á og hvernig gæti OpenVPN hjálpað mér að komast í gegn?“

Áfangi 9: Leystu dulmálið

Til að ljúka þjálfun þinni í úttekt á samskiptareglum skaltu afkóða þessi földu skilaboð um keyrslu í kjarnarými.

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

26	21	21	9	35	23	6	26		19	21	7	18	28	21	18		13
11	23	1	6	1	23	12		10	36	18	10						

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 skipta samskiptareglur máli?

Samskiptareglan ræður því hvernig VPN-ið byggir upp göngin, hvaða dulritun ver gögnin þín og hversu hratt það tengist og endurtengist. WireGuard og OpenVPN eru tvær opnu samskiptareglurnar sem flest VPN-forrit bjóða upp á og þær gera ólíkar málamiðlanir milli einfaldleika, hraða og stillanleika.

Q3: Er annað þeirra persónuverndarvænna en hitt?

Hvorugar samskiptareglurnar gera þig nafnlausan. Báðar dulkóða göngaumferð með sterkum dulmálum; friðhelgi þín fer aðallega eftir því hvað VPN-þjónustuveitan skráir og hvernig hún stýrir lyklum, reikningum og netþjónum.

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: Eru bæði opinn hugbúnaður?

Já. WireGuard og OpenVPN community edition birta bæði frumkóða sinn, svo óháðir rannsakendur geta yfirfarið þau. Lítill kóðagrunnur WireGuard gerir fulla yfirferð mun fljótlegri.

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

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

Q6: Hvort þeirra er hraðvirkara?

WireGuard er yfirleitt hraðvirkara: það keyrir í kjarnanum, notar létta ChaCha20-Poly1305-dulkóðun og lýkur handtökum fljótt. OpenVPN hefur meira aukaálag, en raunverulegur hraði fer einnig eftir álagi á netþjóni og fjarlægð.

Q7: Geta bæði keyrt yfir TCP og UDP?

Nei. OpenVPN getur keyrt yfir UDP eða TCP og TCP-hamur hjálpar á netum sem loka á UDP. WireGuard sendir pakka sína aðeins yfir UDP, svo það getur brugðist á netum sem leyfa aðeins TCP. [4]

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 WireGuard og OpenVPN í símanum mínum?

Já. WireGuard er fjölvettvangs, með forritum fyrir Windows, macOS, Linux, iOS og Android, og OpenVPN-biðlarar eru til fyrir sömu kerfi. Flest VPN-forrit leyfa þér að velja hvora sem er. [1]

Q10: Hvers vegna er WireGuard svona lítið?

WireGuard styður eitt fast sett nútímadulmála í stað margra valkosta. Linux-útfærsla þess þarf innan við 4.000 kóðalínur, sem gerir auðveldara að gera úttekt á því en á stærri VPN-kóðagrunnum. [3]

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.

Q2: Hvaða dulmál notar WireGuard?

WireGuard notar ChaCha20 með Poly1305 til dulkóðunar, Curve25519 til lyklaskipta, BLAKE2s til tætingar og Noise-rammann fyrir handtakið. Engin dulmálssamningaviðræða fer fram, svo notendur geta ekki valið veikan valkost. [2]

Q3: Hvaða dulmál og söfn getur OpenVPN notað?

OpenVPN er þétt samþætt OpenSSL-safninu og notar TLS til að skiptast á lyklum. Stjórnendur geta valið dulmál fyrir gagnarásina, svo sem AES-256-GCM, sem eykur sveigjanleika en einnig hættu á veikum stillingum. [4]

Q4: Hvernig sannvotta samskiptareglurnar hver um sig jafningja?

WireGuard-jafningjar auðkenna hver annan með föstum opinberum lyklum, líkt og með SSH-lyklum, og hver lykill tengist leyfðum IP-tölum ganganna. OpenVPN reiðir sig yfirleitt á vottunaraðila með X.509-vottorðum, oft ásamt notandanafni og lykilorði.

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 gerist þegar ég skipti úr Wi-Fi yfir í farsímanet?

WireGuard er tengingarlaust: það sendir pakka frá nýja vistfanginu og göngin halda áfram eftir fljótt handtak. OpenVPN heldur lotustöðu, svo netbreyting getur krafist endurtengingar sem tekur örlítið lengri tíma.

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: Er OpenVPN enn góður kostur ef WireGuard er hraðara?

Já. OpenVPN er þroskað og víða í notkun, keyrir yfir TCP þegar UDP er lokað og styður fyrirtækjauppsetningar með vottorðum. Margar þjónustuveitur bjóða báðar samskiptareglurnar svo notendur geti skipt ef önnur er lokuð eða hæg.

Q9: Hvaða gáttir nota þau?

Staðalgátt OpenVPN er 1194, en hana má færa á hvaða UDP- eða TCP-gátt sem er, þar á meðal 443. WireGuard hlustar á UDP-gátt sem er stillt í uppsetningu þess; 51820 er gáttin sem notuð er í opinberum dæmum þess.

Q10: Hvaða samskiptareglur eru auðveldari í handvirkri uppsetningu?

WireGuard er yfirleitt einfaldara: þú býrð til lyklapar, skiptist á opinberum lyklum og skráir leyfðar IP-tölur. OpenVPN krefst vottorða, vottunaraðila og fleiri valkosta, þótt .ovpn-prófílar safni þeim saman í eina skrá.

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. TVEIR FLUTNINGAR

OpenVPN getur flutt göngin sín yfir UDP eða TCP, og í TLS-ham deila stjórn- og gagnarásir þess einni gátt. [4]

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. [3]

4. NÚTÍMADULMÁL

WireGuard sameinar ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 og HKDF innan Noise-samskiptarammans, án þess að notendur hafi dulmálsval sem hægt er að velja rangt. [2]

5. OPENSSL INNAN OPENVPN

OpenVPN er þétt samþætt OpenSSL-safninu og sækir mikið af dulritunargetu sinni þangað, þar á meðal TLS sem er notað til að skiptast á lyklum. [4]

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. LYKLAR AÐ HÆTTI SSH

WireGuard-tengingar eru settar upp með því að skiptast á einföldum opinberum lyklum, líkt og með SSH-lyklum, án þess að þörf sé á vottunaraðila. [1]

8. FYRIR ÖLL KERFI

WireGuard kom fyrst út fyrir Linux-kjarnann og er nú í boði fyrir Windows, macOS, BSD, iOS og Android, svo sömu samskiptareglur virka á flestum tækjum. [1]

9. FRAMVIRKT LEYNDARMÁL (FORWARD SECRECY)

WireGuard endurtekur Noise_IK-handtakið á nokkurra mínútna fresti til að skipta um samhverfa lotulykla, sem veitir fullkomið framvirkt leynd (perfect forward secrecy) jafnvel þótt langtímalykill leki síðar. [2]

10. TUN/TAP VIÐMÓT

OpenVPN er hannað til að vinna með sýndarnetviðmótinu TUN/TAP, sem er í boði á flestum kerfum og flytur pakka ganganna. [4]

Tæknilegar heimildir og tilvísanir

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

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] 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/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Lausnir: Samanburður á WireGuard og OpenVPN, samskiptareglum, kóðastærð, hraða og dulkóðunarstöðlum

1 Stærð kóða WireGuard

SAMSKIPTAREGLUR

Rétt svar: D

ATHUGASEMD FYRIR KENNARA

WireGuard er afar fyrirferðarlítið og keyrir á um 4.000 kóðalínum. Það heldur árásarfletinum litlum og gerir úttektir auðveldari. Heimild: WireGuard Project.

2 Hraði í kjarnarýmі

SEINKUN

Rétt svar: B

ATHUGASEMD FYRIR KENNARA

Með því að keyra beint í kjarnarými forðast WireGuard álag vegna samhengisskipta, sem gerir mikið gegnumstreymi mögulegt. Heimild: WireGuard Project.

3 Spurning 3

Rétt svar: B

ATHUGASEMD FYRIR KENNARA

OpenVPN er náið samþætt OpenSSL, sem veitir dulmál á borð við AES-GCM og gerir það mjög stillanlegt en flóknara.

4 Afköst samskiptareglu

STÝRINGAR LEIÐARVALS

Rétt svar: A

ATHUGASEMD FYRIR KENNARA

WireGuard kemur á handtökum á millisekúndum og bregst samstundis við flakki milli neta (t.d. þegar skipt er úr Wi-Fi í farsímanet). Heimild: Microsoft Native Gateway, Apple Support.

5 Ósamhverf dulritun

FRIÐHELGI

Rétt svar: C

ATHUGASEMD FYRIR KENNARA

WireGuard notar Cryptokey Routing, sem tengir opinbera lykla við leyfðar IP-tölur ganganna, líkt og í SSH-uppsetningum. Heimild: WireGuard Project.

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Linux-útfærsla WireGuard er innan við 4.000 línur og því geta öryggisteymi yfirfarið hana mun hraðar en mun stærri VPN-kóðagrunna á borð við OpenVPN.

7 **Seinkun í notendarými** HRAÐI — **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

OpenVPN keyrir í notendarými og sendir pakka fram og til baka frá síndarviðmóti kjarnans, sem bætir við álagi vegna samhengisskipta (nema kjarnaafhleðsla á borð við OpenVPN DCO sé notuð). Heimild: DD-WRT custom firmware.

8 **OpenVPN-stillingar** HLERUNARHÆTTA — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

OpenVPN getur keyrt yfir TCP (fyrir áreiðanleika/til að komast framhjá eldveggjum) eða UDP (fyrir hraða), sem gerir það samhæft flóknum fyrirtækiseldveggjum. Heimild: IETF Cryptographic Protocols.

9 **Nútímadulritun** ELDVEGGIR — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

WireGuard sleppir eldri dulmálum í þágu nútímalegra, öruggra frumeininga eins og ChaCha20 og Poly1305, sem keyra hratt á farsímaörgjörvum. Heimild: WireGuard Project.

10 **Einföldun lyklapars** ENGIN SKRÁNING — **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

WireGuard notar hvorki vottorð né flókið stigveldi vottunaraðila; það byggir á einföldum opinberum/einkalyklapörum sem jafningjar skiptast á. Heimild: WireGuard Project.

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. WireGuard	H 2. OpenVPN	E 3. Kjarnarými	A 4. Notendarými
B 5. 4.000 línur	C 6. OpenSSL	F 7. Lyklapar	D 8. TCP/UDP

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 WIREGUARD	2 OPENVPN	3 KJARNARÝMI	4 NOTENDARÝMI
5 LYKILPÖR	6 ÚTTEKTARHÆFNI		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 F – OPENSSL	2 C – KJARNARÝMI	3 B – OPENVPN	4 G – LYKILPÖR
5 H – TCPOGUDP	6 E – KÓÐASTÆRÐ	7 A – WIREGUARD	8 D – NOTENDARÝMI

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt WireGuard, OpenVPN og Kjarnarými með eigin orðum og gefið dæmi um hvert hugtak.

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

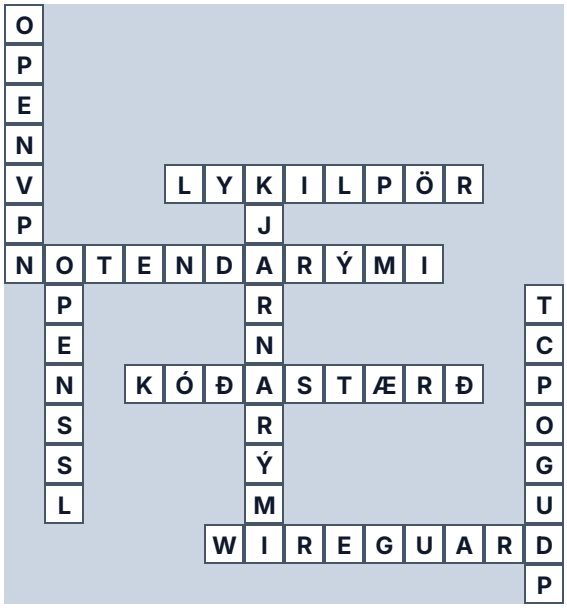
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

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

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

2 lárétt: LYKILPÖR Ósamhverfir lyklar sem WireGuard notar til að sannreyna tengda jafningja (8 stafir)

4 lárétt: NOTENDARÝMI Framkvæmdarsvæði þar sem OpenVPN keyrir og skapar yfirbyggingu vegna samhengisskipta (11 stafir)

7 lárétt: KÓÐASTÆRÐ Smæð kóðagrunns WireGuard sem gerir úttekt mun auðveldari (9 stafir)

8 lárétt: WIREGUARD Nútímaleg VPN-samskiptaregla hönnuð fyrir mikinn hraða og einfalda kóðarýni (9 stafir)

LÓÐRÉTT

1 lóðrétt: OPENVPN Öflug eldri samskiptaregla með stóran og flókinn stillingakóðagrunn (7 stafir)

3 lóðrétt: KJARNARÝMI Framkvæmdarsvæði stýrikerfis þar sem WireGuard keyrir fyrir hraða (10 stafir)

5 lóðrétt: OPENSSL Dulmálssafn sem OpenVPN reiðir sig á fyrir dulmálsalgrím (7 stafir)

6 lóðrétt: TCPOGUDP Flutningsreglur sem OpenVPN styður; WireGuard sjálft keyrir eingöngu yfir UDP (8 stafir)

Lausnir: Stafaruglingur og dulmál

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

LYKILL ORÐARAÐAR

1. UGEIWARDR — WIREGUARD
2. MRKJNIRÝAA — KJARNARÝMI
3. KTSÓÆÐARÐ — KÓÐASTÆRÐ
4. IÖRPLLYK — LYKILPÖR
5. VNNEOPP — OPENVPN
6. NIDRMÝNOATE — NOTENDARÝMI
7. OSSLPNE — OPENSSL
8. OCGPTDUP — TCPOGUDP

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"UPPFÆRÐU OPENVPN Í HRAÐARI GÖNG"

Lausnir dæmisagna

A Aðstæður A: Val á samskiptareglu

HLERUN OG DULKÓÐUN

Vandi Sarah

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Ráðlegging: WireGuard. Létt og tengingarlaus hönnun þess gerir göngunum kleift að ná sér fljótt þegar netið hennar breytist, og ChaCha20-Poly1305 heldur dulkóðuninni hraðri.
- Öryggi: Báðar samskiptareglurnar dulkóða umferð hennar á Wi-Fi kaffihússins, svo hvor um sig ver innskráningar hennar ef rétt er stillt; valið hefur aðallega áhrif á hraða og stöðugleika.

B Aðstæður B: Komist framhjá VPN-lokunum

LANDFRÆÐILEGAR LOKANIR OG IP-TÖLUR

Vandi Alex

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Hvers vegna lokað: WireGuard notar eingöngu UDP og eldveggur hótelsins lokar líklega á UDP eða þekkir WireGuard-pakka með síun eða djúpri pakkaskoðun.
- Hvernig OpenVPN hjálpar: Það getur keyrt yfir TCP, þar á meðal gátt 443 sem HTTPS notar, og hótel-eldveggir loka sjaldan alfarið á hana þar sem vefskoðun byggir á henni.