Enw: _____ Dyddiad: _____ Sgôr: _____

WireGuard yn erbyn OpenVPN Taflen Waith

Cymharu protocolau WireGuard ac OpenVPN, meintiau cronfeydd cod, cyflymder, a safonau cryptograffig

TROSOLWG DYSGU VPN

DYSGWR
STATWS MYFYRIWR
Llwybr Amddiffynnwr Rhwydwaith

DIOGEL
STATWS Y CYSYLLTIAD
Cysgodi pecynnau data

GWEITHREDOL
DIOGELU RHAG GOLLYNGIADAU
Diogelu rhag gollyngiadau DNS ac IPv6

Croeso! Mae'r pecyn gweithgareddau hwn yn eich tywys drwy egwyddorion sylfaenol Rhwydweithiau Preifat Rhithwir (VPNs). Byddwch yn archwilio sut mae twneli amgryptiedig yn diogelu'ch data, sut mae protocolau rhwydwaith yn gweithio, a sut i adnabod a lliniaru gollyngiadau preifatrwydd.

PWYNTIAU GWIRIO'R DAFLEN WAITH

- [ ] **Rhan 1-4: Meistroli cysyniadau a phrotocolau VPN.**
- [ ] **Rhan 5-7: Datrys posau croesair a chwilair.**
- [ ] **Rhan 8-9: Datrys astudiaethau achos a her y seiffr.**
- [ ] **Rhan 10: Adolygu tudalennau Cwestiynau Cyffredin sylfaenol ac uwch.**
- [ ] **Rhan 11: Archwilio 10 ffaith ddiddorol o'r byd go iawn.**
- [ ] **Bonws: her Meddwl yn Gyflym.**

Agorwch Ganllaw VPN gan VPN.com

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

Eich Map Llwybr Dysgu VPN

- Cymharwch gymhlethdod cronfeydd cod a chyflymder archwilio protocolau.
- Dadansoddwch y manteision perfformiad o redeg yng ngofod y cnewyllyn.
- Cyferbynnwch seiffrau OpenSSL â chryptograffeg fodern WireGuard.
- Sefydlu parau allweddi cyhoeddus a phreifat ar gyfer ysgwyd llaw rhwng cymheiriaid.
- Llwybrwch draffig VPN drwy byrth wal dân TCP ac UDP.

CYFARWYDDIADAU'R DAFLEN WAITH CYMHARU PROTOCOLAU

Atebwch y cwestiynau amlddewis a gwir/gau, cwblhewch y brawddegau llenwi bylchau gan ddefnyddio'r banc geiriau, parwch y diffiniadau, a datryswch y posau croesair a chwilair. Cymhwyswch eich gwybodaeth i archwilio protocolau modern. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

WIREGUARD YN ERBYN OPENVPN (CYFLWYNIAD)

Mae dewis protocol VPN yn gofyn am gydbwyso cyflymder ac opsiynau ffurfweddu. OpenVPN fu'r safon ers degawdau, gan gynnig hyblygrwydd ffurfweddu TCP/UDP. Mae WireGuard yn ddisodlydd modern sy'n rhedeg yn uniongyrchol yng ngofod y cnewyllyn gyda dim ond 4,000 o linellau cod. Mae deall y gwahaniaethau rhwng protocolau yn allweddol i optimeiddio eich rhwydweithiau diogel.

DARLLENWCH BOB PWYNT GWIRIO YN OFALUS A DEWISWCH NEU YSGRIFENNWCH YR YMATEB CYWIR.

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw maint bras sylfaen god protocol WireGuard?**
   - A. Tua 70,000 o linellau
   - B. Dros 100,000 o linellau
   - C. Llai na 1,000 o linellau
   - D. Tua 4,000 o linellau

2. **2. Ym mha ofod o'r system weithredu y mae WireGuard yn rhedeg?**
   - A. Gofod defnyddiwr
   - B. Gofod y cnewyllyn
   - C. Gofod rhaglenni
   - D. Gofod rhithwir

3. **3. Ar ba lyfrgell gryptograffig y mae OpenVPN yn dibynnu'n bennaf?**
   - A. ChaCha20-Poly1305
   - B. Llyfrgell gryptograffig OpenSSL
   - C. Fframwaith protocol Noise
   - D. Amgodio DES testun plaen

4. **4. Beth yw un o fanteision perfformiad allweddol WireGuard dros OpenVPN?**
   - A. Ysgwyd llaw cysylltu cyflymach a hwyrni is
   - B. Osgoi'r angen am gyfeiriadau IP cyhoeddus
   - C. Cefnogaeth frodorol adeiledig ar gyfer deialu hen ffasiwn
   - D. Dim gorbenion batri ar ddyfeisiau symudol

5. **5. Sut mae WireGuard yn dilysu cysylltiadau cymheiriaid?**
   - A. Drwy gyfnewid cyfrineiriau defnyddwyr safonol
   - B. Drwy wirio tystysgrifau cofrestru parthau
   - C. Drwy ddefnyddio parau allweddi cyhoeddus a phreifat statig
   - D. Drwy wirio rhifau cyfresol caledwedd

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae sylfaen god gryno WireGuard yn ei gwneud yn sylweddol haws ei archwilio.

Gwir Gau

7 Cwestiwn 7

7. Yn gyffredinol mae OpenVPN yn gyflymach na WireGuard oherwydd ei fod yn rhedeg yng ngofod y cnewyllyn.

Gwir Gau

8 Cwestiwn 8

8. Mae modd ffurfweddu OpenVPN yn helaeth ac mae'n cefnogi protocolau UDP a TCP.

Gwir Gau

9 Cwestiwn 9

9. Mae WireGuard yn defnyddio cryptograffeg fodern fel ChaCha20 ar gyfer amgryptio pecynnau'n gyflym.

Gwir Gau

10 Cwestiwn 10

10. Mae WireGuard angen gosodiadau awdurdod tystysgrifau cymhleth i ddilysu.

Gwir Gau

Pwynt Gwirio 3: Mewnosod Termau Allweddol

Darllenwch bob brawddeg isod a llenwch y bwlch gyda'r term cywir o'r Banc Geiriau.

1. Mae'r protocol _____ modern yn gweithredu'n uniongyrchol y tu mewn i gnewyllyn y system weithredu.

2. Mae'r protocol _____ etifeddol yn dibynnu ar y llyfrgell gryptograffig OpenSSL.

3. Mae gweithredu cod yn y _____ yn lleihau gorbenion newid cyd-destun.

4. Mae OpenVPN yn rhedeg yn y _____ , gan lwybro pecynnau drwy ryngwynebau rhithwir.

5. Mae WireGuard yn defnyddio _____ cyhoeddus a phreifat i adnabod cymheiriaid cysylltiad.

6. Mae sylfaen god fach yn gwella _____ diogelwch y feddalwedd.

BANC GEIRIAU GEIRFA

ARCHWILIADWYEDD GOFOD CNEWYLLYN GOFOD DEFNYDDIWR OPENSSL
OPENVPN PARAU ALLWEDDI TCP/UDP WIREGUARD

Ysgrifennwch eich atebion yma:

1. **2.**

3. **4.**

5. **6.**

Pwynt Gwirio 4: Paru Cysyniadau Rhwydwaith

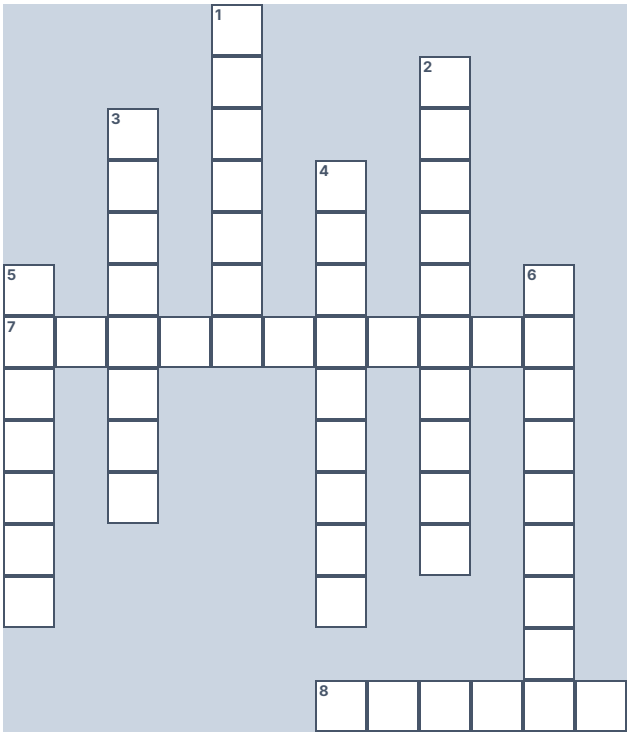
PARU DIFFINIADAU

Parwch bob term geirfa ar y chwith â'i ddiffiniad cywir ar y dde drwy ysgrifennu'r llythyren gyfatebol (A-H) yn y blwch mewnbwn y gellir ei lenwi.

☐	1. WireGuard	A	Ardal weithredu lle mae OpenVPN yn rhedeg, gan greu gorbenion newid cyd-destun.
☐	2. OpenVPN	B	Maint cryno sylfaen god WireGuard, sy'n ei gwneud yn llawer haws ei harchwilio.
☐	3. Gofod y Cnewyllyn	C	Llyfrgell gryptograffig y mae OpenVPN yn dibynnu arni ar gyfer algorithmau seiffr.
☐	4. Gofod y Defnyddiwr	D	Protocolau trosglwyddo y mae OpenVPN yn eu cefnogi; mae WireGuard ei hun yn rhedeg dros UDP yn unig.
☐	5. 4,000 o Linellau	E	Ardal weithredu'r system weithredu lle mae WireGuard yn rhedeg er mwyn cyflymder.
☐	6. OpenSSL	F	Tocynnau anghymesur a ddefnyddir gan WireGuard i wirio cysylltiadau cymheiriaid.
☐	7. Pâr o Allweddi	G	Protocol VPN modern a gynlluniwyd ar gyfer cyflymder uchel ac archwilio cod syml.
☐	8. TCP/UDP	H	Protocol hŷn cadarn sy'n defnyddio sylfaen cod ffurfweddu fawr a chymhleth.

Pwynt Gwirio 5: Pos Croesair

Datryswch y croesair drwy deipio llythrennau yn y blychau gwyn gweithredol. Mae'r rhifau'n cyfateb i'r cliwiau isod.



CLIWIAU AR DRAWS

7. Tocynnau anghymesur a ddefnyddir gan WireGuard i ddilysu cysylltiadau cymheiriaid (11)

8. Protocolau cludo y mae OpenVPN yn eu cefnogi; dros UDP yn unig y mae WireGuard ei hun yn rhedeg (6)

CLIWIAU I LAWR

1. Llyfrgell gryptograffig y mae OpenVPN yn dibynnu arni ar gyfer algorithmau seiffr (7)

2. Gofod y ...: ardal weithredu lle mae OpenVPN yn rhedeg, gan greu gorbenion newid cyd-destun (10)

3. Maint bach sylfaen god WireGuard, sy'n ei gwneud yn llawer haws ei harchwilio (8)

4. Gofod y ...: ardal weithredu'r system weithredu lle mae WireGuard yn rhedeg er mwyn cyflymder (9)

5. Protocol etifeddol cadarn sy'n defnyddio sylfaen god ffurfweddu fawr a chymhleth (7)

6. Protocol VPN modern a gynlluniwyd ar gyfer cyflymder uchel ac archwilio cod syml (9)

Pwynt Gwirio 5, dewis arall: Cliwiau Croesair Hygyrch

Gall defnyddwyr darllenwyr sgrin a bysellfwrdd deipio atebion y croesair yn uniongyrchol yn y meysydd testun isod.

CLIWIAU AR DRAWS

7 ar draws: Tocynnau anghymesur a ddefnyddir gan WireGuard i ddilysu cysylltiadau cymheiriaid (11 llythyren):

8 ar draws: Protocolau cludo y mae OpenVPN yn eu cefnogi; dros UDP yn unig y mae WireGuard ei hun yn rhedeg (6 llythyren):

CLIWIAU I LAWR

1 i lawr: Llyfrgell gryptograffig y mae OpenVPN yn dibynnu arni ar gyfer algorithmau seiffr (7 llythyren):

2 i lawr: Gofod y ...: ardal weithredu lle mae OpenVPN yn rhedeg, gan greu gorbenion newid cyd-destun (10 llythyren):

3 i lawr: Maint bach sylfaen god WireGuard, sy'n ei gwneud yn llawer haws ei harchwilio (8 llythyren):

4 i lawr: Gofod y ...: ardal weithredu'r system weithredu lle mae WireGuard yn rhedeg er mwyn cyflymder (9 llythyren):

5 i lawr: Protocol etifeddol cadarn sy'n defnyddio sylfaen god ffurfweddu fawr a chymhleth (7 llythyren):

6 i lawr: Protocol VPN modern a gynlluniwyd ar gyfer cyflymder uchel ac archwilio cod syml (9 llythyren):

Pwynt Gwirio 6: Chwilair Geiriau Cudd

Dewch o hyd i'r 8 term geirfa allweddol sydd wedi'u cuddio yn y grid isod. Gall geiriau fod yn llorweddol, yn fertigol neu'n groeslinol.

U S T E L J B C A B C P X L K
Y K X T K D Q O M J O D I N N
R K Q P G M M D Q R P S T T G
W P C S Q O H C S B E W D S Z
I D V C Z P W R F K N H Z W D
D U N D Q A X Y P C V U B I A
D P Z N D R K N C A P D O R D
Y C F H I A D O N O N R Q E M
N T E I R L Z S E P F Q V G F
F A A Q O L N P W E T X Q U K
E R U S D W N Y Y N B F S A X
D W J A R E Z Y L S Y L G R I
M R J M L D T O L S H Q Q D H
Z A O V G D U B Y L Y R Y B H
L Z G J O I P N N W C M Z Y G

RHESTR GEIRIAU GEIRFA

WIREGUARD
OPENVPN
CNEWYLLYN
DEFNYDDIWR
CODCRYNO
OPENSSL
PARALLWEDDI
TCPUDP

Pwynt Gwirio 6, dewis arall: Paru Geirfa Hygyrch

Parwch bob un o'r 8 term geirfa o'r Chwilair â'i ddiffiniad cywir drwy ysgrifennu'r llythyren (A-H) yn y bwlch.

TERMAU GEIRFA
A. WIREGUARD
B. OPENVPN
C. CNEWYLLYN
D. DEFNYDDIWR
E. CODCRYNO
F. OPENSSL
G. PARALLWEDDI
H. TCPUDP

DIFFINIADAU A MEYSYDD PARU	
	1. Llyfrgell gryptograffig y mae OpenVPN yn dibynnu arni ar gyfer algorithmau seiffr.
	2. Gofod y ...: ardal weithredu'r system weithredu lle mae WireGuard yn rhedeg er mwyn cyflymder.
	3. Protocol etifeddol cadarn sy'n defnyddio sylfaen god ffurfweddu fawr a chymhleth.
	4. Tocynnau anghymesur a ddefnyddir gan WireGuard i ddilysu cysylltiadau cymheiriaid.
	5. Protocolau cludo y mae OpenVPN yn eu cefnogi; dros UDP yn unig y mae WireGuard ei hun yn rhedeg.
	6. Maint bach sylfaen god WireGuard, sy'n ei gwneud yn llawer haws ei harchwilio.
	7. Protocol VPN modern a gynlluniwyd ar gyfer cyflymder uchel ac archwilio cod syml.
	8. Gofod y ...: ardal weithredu lle mae OpenVPN yn rhedeg, gan greu gorbenion newid cyd-destun.

Pwynt Gwirio 7: Her Geiriau Cymysg

Dad-sgramblwch y llythrennau isod i ddatgelu cysyniadau a thermau allweddol VPN. Ysgrifennwch eich atebion yn y blychau mewnbwn y gellir eu llenwi.

1. UGEIWARDR
2. NCYWNLLYE
3. COCRYOND
4. WDILRLDEPAA
5. VNNEOPP
6. WYNDIDEDRF
7. OSSLPNE
8. PPTDUC

Gweithgaredd Bonws: Meddwl yn Gyflym

3 ATEB YM MHOB CATEGORI. Y PERSON CYNTAF I GWBLHAU'R RHESTR SY'N ENNILL.

1	Rhesymau dros ddewis WireGuard			
2	Addewidion y mae darparwr VPN da yn eu gwneud			
3	Rhesymau dros ddewis OpenVPN			
4	Rhesymau dros ddefnyddio VPN wrth deithio			
5	Pethau y gall eich darparwr rhyngrwyd eu gweld			
6	Ffyrdd o adnabod rhwydwaith Wi-Fi ffug			
7	Mythau am VPNs			
8	Mannau lle byddech chi'n defnyddio VPN			
9	Pethau cyflym ym mywyd bob dydd			
10	Pethau na all VPN eich diogelu rhagddynt			
11	Pethau sy'n gwneud cod yn haws ei wirio			
12	Pethau y gall VPN eu cuddio			
13	Gwahaniaethau rhwng WireGuard ac OpenVPN			
14	Geiriau sy'n ymwneud â phreifatrwydd			
15	Enwau amgryptio rydych chi'n eu hadnabod			

Pwynt Gwirio 8: Astudiaethau Achos VPN

Cymhwyswch y cysyniadau rydych wedi'u dysgu i ddatrys y senarios go iawn isod.

SARAH (MYFYRIWR YN Y SIOP GOFFI)

👩‍💻 "Helô! Rwy ar Wi-Fi y caffi ac mae fy ap VPN yn gadael i mi ddewis WireGuard neu OpenVPN. Mae fy ngalwadau fideo yn torri o hyd pan fyddaf yn cerdded rhwng rhwydwaith y caffi a man problemus fy ffôn. Pa brotocol ddylwn i ei ddewis, a pham y byddai'n ymdopi'n well â'r newid?"

ALEX (MYFYRIWR SY'N TEITHIO)

👩‍💻 "Rwy dramor ar rwydwaith gwesty sy'n ymddangos fel pe bai'n rhwystro'r rhan fwyaf o draffig VPN. Nid yw WireGuard yn cysylltu o gwbl, ond mae angen i mi gyrraedd adnoddau fy ysgol gartref. Beth sy'n debygol o gael ei rwystro, a sut gallai OpenVPN fy helpu i fynd drwodd?"

Pwynt Gwirio 9: Dadgryptio'r Seiffr

I gwblhau eich hyfforddiant ar archwilio protocolau, dadgryptiwch y neges gudd hon am weithredu yng ngofod y cnewyllyn.

ALLWEDD AMGRYPTIO LLYTHRENNAU-I-RIFAU

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

21 23 3 8 18 1 4 4 9 23 3 8 5 9 3 8

15 16 5 14 22 16 14 7 25 4 1 20 8 23 14 14 5 12

3 25 6 12 25 13 1 3 8

Neges wedi'i datgodio:

AWGRYM: MAE POB RHIF YN CYNRYCHIOLI SAFLE'R LLYTHYREN HONNO YN YR WYDDOR (E.E. 1 = A, 2 = B, 26 = Z).

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am VPN (Rhan A)

Adolygwch y cwestiynau a'r atebion mwyaf cyffredin sydd gan ddarpar gwsmeriaid am ddefnyddio rhwydweithiau preifat rhithwir.

Q1: Beth yw VPN a sut mae'n gweithio?

Mae Rhwydwaith Preifat Rhithwir (VPN) yn amgryptio eich cysylltiad â'r rhyngrwyd ac yn llwybro eich traffig drwy weinydd pell diogel. Mae hyn yn cuddio eich cyfeiriad IP cyhoeddus ac yn cyfyngu ar yr hyn y gall arsylwyr y rhwydwaith lleol a'ch ISP ei weld am draffig a lwybrir drwy dwnnel y VPN.

Q2: Pam mae protocolau'n bwysig?

Mae'r protocol yn penderfynu sut mae eich VPN yn adeiladu ei dwnnel, pa gryptograffeg sy'n diogelu eich data, a pha mor gyflym y mae'n cysylltu ac yn ailgysylltu. WireGuard ac OpenVPN yw'r ddau brotocol cod agored y mae'r rhan fwyaf o apiau VPN yn eu cynnig, ac maent yn gwneud cyfaddawdau gwahanol rhwng symlrwydd, cyflymder a'r gallu i'w ffurfweddu.

Q3: A yw un ohonynt yn fwy preifat na'r llall?

Nid yw'r naill brotocol na'r llall yn eich gwneud yn ddienw. Mae'r ddau'n amgryptio traffig y twnnel gyda seiffrau cryf; mae eich preifatrwydd yn dibynnu'n bennaf ar yr hyn y mae'r darparwr VPN yn ei logio a sut mae'n rheoli allweddi, cyfrifon a gweinyddion.

Q4: A fydd VPN yn arafu cyflymder fy rhyngrwyd?

Ie, ychydig. Mae'r broses amgryptio a'r pellter ffisegol i weinydd y VPN yn ychwanegu oedi a gorbenion. Mae'r effaith yn amrywio yn ôl y darparwr, y protocol, pellter y gweinydd, y ddyfais ac amodau'r rhwydwaith.

Q5: A yw'r ddau'n god agored?

Ie. Mae WireGuard a rhifyn cymunedol OpenVPN ill dau yn cyhoeddi eu cod ffynhonnell, felly gall ymchwilwyr annibynnol eu hadolygu. Mae cronfa god fach WireGuard yn gwneud adolygiad llawn yn llawer cyflymach.

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am VPN (Rhan B)

Adolygwch y cwestiynau a'r atebion mwyaf cyffredin sydd gan ddarpar gwsmeriaid am ddefnyddio rhwydweithiau preifat rhithwir.

Q6: Pa un sy'n gyflymach?

Mae WireGuard fel arfer yn gyflymach: mae'n rhedeg yn y cnewyllyn, yn defnyddio amgryptio ChaCha20-Poly1305 darbodus ac yn cwblhau ysgwyd llaw yn gyflym. Mae gan OpenVPN fwy o orbenion, ond mae cyflymderau go iawn hefyd yn dibynnu ar lwyth y gweinydd a'r pellter.

Q7: A all y ddau redeg dros TCP ac UDP?

Na. Gall OpenVPN redeg dros UDP neu TCP, ac mae modd TCP yn helpu ar rwydweithiau sy'n rhwystro UDP. Mae WireGuard yn anfon ei becynnau dros UDP yn unig, felly gall fethu ar rwydweithiau sy'n caniatáu TCP yn unig. [4]

Q8: Sut mae dewis y VPN gorau?

Chwiliwch am bolisïau dim logiau wedi'u harchwilio, protocolau cryf (WireGuard, OpenVPN), lleoliadau gweinyddion diogel, cyflymderau uchel, gweinyddion RAM yn unig, nodwedd kill switch, ac awdurdodaeth y tu allan i gynghreiriau rhannu cudd-wybodaeth (fel y 5/9/14 Eyes).

Q9: A allaf ddefnyddio WireGuard ac OpenVPN ar fy ffôn?

Ie. Mae WireGuard yn draws-lwyfan, gydag apiau ar gyfer Windows, macOS, Linux, iOS ac Android, ac mae cleientiaid OpenVPN yn bodoli ar gyfer yr un systemau. Mae'r rhan fwyaf o apiau VPN yn gadael i chi ddewis y naill neu'r llall. [1]

Q10: Pam mae WireGuard mor fach?

Mae WireGuard yn cefnogi un set sefydlog o seiffrau modern yn hytrach na llawer o opsiynau. Mae ei weithrediad Linux angen llai na 4,000 o linellau cod, sy'n ei gwneud yn haws ei archwilio na sylfeini cod VPN mwy. [3]

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am VPN (Rhan C)

Archwilio agweddau technegol a strwythurol ar rwydweithiau preifat rhithwir a phrotocolau twnelu diogel.

Q1: Beth yw'r gwahaniaeth rhwng WireGuard, OpenVPN ac IKEv2?

Protocol modern ac ysgafn yw WireGuard (dim ond ~4,000 o linellau cod) sy'n cynnig cyflymderau cyflym ac amseroedd cysylltu cyflym. Protocol ffynhonnell agored hynod ddiogel sydd wedi'i brofi'n drylwyr yw OpenVPN. Mae IKEv2 yn ardderchog ar gyfer dyfeisiau symudol oherwydd ei allu i ailgysylltu'n gyflym wrth newid rhwydweithiau.

Q2: Pa seiffrau mae WireGuard yn eu defnyddio?

Mae WireGuard yn defnyddio ChaCha20 gyda Poly1305 ar gyfer amgryptio, Curve25519 ar gyfer cyfnewid allweddi, BLAKE2s ar gyfer stwnsio a fframwaith Noise ar gyfer ei ysgwyd llaw. Nid oes negodi seiffr, felly ni all defnyddwyr ddewis opsiwn gwan. [2]

Q3: Pa seiffrau a llyfrgelloedd y gall OpenVPN eu defnyddio?

Mae OpenVPN wedi'i integreiddio'n dynn â llyfrgell OpenSSL ac mae'n defnyddio TLS i gyfnewid allweddi. Gall gweinyddwyr ddewis seiffrau sianel ddata fel AES-256-GCM, sy'n ychwanegu hyblygrwydd ond hefyd le i osodiadau gwan. [4]

Q4: Sut mae pob protocol yn dilysu cymheiriaid?

Mae cymheiriaid WireGuard yn adnabod ei gilydd drwy allweddi cyhoeddus statig, yn debyg iawn i gyfnewid allweddi SSH, ac mae pob allwedd yn mapio i IPs twnnel a ganiateir. Mae OpenVPN fel arfer yn dibynnu ar awdurdod tystysgrifau gyda thystysgrifau X.509, yn aml ynghyd ag enw defnyddiwr a chyfrinair.

Q5: Sut mae cuddio (Obfuscation) yn osgoi rhwystrau VPN?

Mae cuddio (neu "VPN Llechwraidd") yn cuddio traffig VPN fel ei fod yn edrych fel traffig HTTPS cyffredin (porth 443). Gall hyn ei helpu i fynd heibio i Archwilio Pecynnau Dwfn (DPI) a ddefnyddir gan lywodraethau neu rwydweithiau ysgolion/swyddfeydd i rwystro VPNs.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am VPN (Rhan D)

Archwilio agweddau technegol a strwythurol ar rwydweithiau preifat rhithwir a phrotocolau twnelu diogel.

Q6: Beth sy'n digwydd pan fyddaf yn newid o Wi-Fi i ddata symudol?

Mae WireGuard yn ddigyswllt: mae'n anfon pecynnau o'r cyfeiriad newydd ac mae'r twnnel yn parhau ar ôl ysgwyd llaw cyflym. Mae OpenVPN yn cadw cyflwr y sesiwn, felly gall newid rhwydwaith olygu bod angen ailgysylltu, sy'n cymryd ychydig yn hirach.

Q7: Sut mae Cyfrinachedd Ymlaen (Cyfrinachedd Ymlaen Perffaith) yn gweithio?

Mae PFS yn sicrhau bod allwedd amgryptio unigryw, dros dro yn cael ei chynhyrchu ar gyfer pob sesiwn unigol. Hyd yn oed os caiff allwedd breifat ei pheryglu yn y dyfodol, ni ellir ei defnyddio i ddadgryptio sesiynau'r gorffennol na'r dyfodol oherwydd eu bod wedi defnyddio allweddi annibynnol.

Q8: A yw OpenVPN yn dal i fod yn ddewis da os yw WireGuard yn gyflymach?

Ie. Mae OpenVPN yn aeddfed ac wedi'i ddefnyddio'n eang, mae'n rhedeg dros TCP pan fydd UDP wedi'i rwystro, ac mae'n cefnogi gosodiadau menter sy'n seiliedig ar dystysgrifau. Mae llawer o ddarparwyr yn cynnig y ddau brotocol fel y gall defnyddwyr newid os yw un wedi'i rwystro neu'n araf.

Q9: Pa borthladdoedd maen nhw'n eu defnyddio?

Porth safonol OpenVPN yw 1194, ond gellir ei symud i unrhyw borth UDP neu TCP, gan gynnwys 443. Mae WireGuard yn gwrando ar borth UDP a osodir yn ei ffurfweddiad; 51820 yw'r porth a ddefnyddir yn ei enghreifftiau swyddogol.

Q10: Pa brotocol sy'n haws i'w osod â llaw?

Mae WireGuard fel arfer yn symlach: cynhyrchu pâr o allweddi, cyfnewid allweddi cyhoeddus a rhestru'r IPs a ganiateir. Mae OpenVPN angen tystysgrifau, CA a mwy o opsiynau, er bod proffiliau .ovpn yn eu cyfuno mewn un ffeil.

Rhan 11: 10 Ffaith Ddiddorol am VPN a Mewnwelediadau o'r Byd Go Iawn

Adolygwch y ffeithiau a'r mewnwelediadau gwerthfawr iawn hyn o'r byd go iawn am hanes, marchnad a thechnoleg VPNs.

1. Y PROTOCOL VPN CYNTAF

Datblygwyd PPTP (Point-to-Point Tunneling Protocol) gan grŵp o werthwyr gan gynnwys Microsoft a'i gyhoeddi fel RFC 2637 ym mis Gorffennaf 1999 i gefnogi VPNs mynediad o bell. [6]

2. DAU DDULL CLUDO

Gall OpenVPN gludo ei dwnnel dros UDP neu TCP, ac yn y modd TLS mae ei sianeli rheoli a data yn rhannu un porth. [4]

3. CHWYLDRO WIREGUARD

Mae gan WireGuard sylfaen god hynod symlach a gynlluniwyd ar gyfer effeithlonrwydd, gan ei gwneud yn haws ei harchwilio am wendidau diogelwch na phrotocolau traddodiadol. [3]

4. CRYPTOGRAFFEG FODERN

Mae WireGuard yn cyfuno ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 a HKDF o fewn fframwaith protocol Noise, heb ddewisiadau seiffr y gallai defnyddwyr eu gosod yn anghywir. [2]

5. OPENSSL Y TU MEWN I OPENVPN

Mae OpenVPN wedi'i integreiddio'n dynn â llyfrgell OpenSSL ac mae'n cael llawer o'i alluoedd cryptograffig ohoni, gan gynnwys y TLS a ddefnyddir i gyfnewid allweddi. [4]

6. ARCHWILIO PECYNNAU DWFN

Mae Archwilio Pecynnau Dwfn (DPI) yn archwilio cynnwys pecynnau a phatrymau traffig, nid penawdau yn unig, ac mae rhai waliau tân yn ei ddefnyddio i ganfod a rhwystro protocolau VPN cyffredin.

7. ALLWEDDI ARDDULL SSH

Caiff cysylltiadau WireGuard eu sefydlu drwy gyfnewid allweddi cyhoeddus syml, yn debyg iawn i gyfnewid allweddi SSH, heb fod angen awdurdod tystysgrifau. [1]

8. TRAWS-BLATFFORM

Rhyddhawyd WireGuard yn gyntaf ar gyfer cnewyllyn Linux ac mae bellach ar gael ar gyfer Windows, macOS, BSD, iOS ac Android, felly mae'r un protocol yn gweithio ar y rhan fwyaf o ddyfeisiau. [1]

9. CYFRINACHEDD YMLAEN

Mae WireGuard yn ailadrodd ei ysgwyd llaw Noise_IK bob ychydig funudau i gylchdroi'r allweddi sesiwn cymesur, gan roi cyfrinachedd ymlaen perffaith hyd yn oed os bydd allwedd hirdymor yn gollwng yn ddiweddarach. [2]

10. RHYNGWYNEBAU TUN/TAP

Mae OpenVPN wedi'i gynllunio i weithio gyda'r rhyngwyneb rhwydwaith rhithwir TUN/TAP, sydd ar gael ar y rhan fwyaf o lwyfannau ac sy'n cludo pecynnau'r twnnel. [4]

Cyfeiriadau a Ffynonellau Technegol

Cyhoeddiadau a ddyfynnwyd, manylebau cryptograffig, a safonau dogfennau swyddogol a ddefnyddiwyd ar draws y daflen waith hon.

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[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

Allwedd Atebion: Cymharu protocolau WireGuard ac OpenVPN, meintiau cronfeydd cod, cyflymder, a safonau cryptograffig

1 **Maint Cod WireGuard** PROTOCOLAU — **Ateb Cywir: D**

NODYN ADDYSGU

Mae WireGuard yn hynod gryno, ac yn rhedeg ar tua 4,000 o linellau cod. Mae hyn yn cadw'r arwyneb ymosod yn fach ac yn gwneud archwilio'n haws. Ffynhonnell: WireGuard Project.

2 **Cyflymder Gofod y Cnewyllyn** CUDDNI — **Ateb Cywir: B**

NODYN ADDYSGU

Drwy weithredu'n uniongyrchol yng ngofod y cnewyllyn, mae WireGuard yn osgoi gorbenion newid cyd-destun, gan alluogi trwybwn uchel. Ffynhonnell: WireGuard Project.

3 **Cwestiwn 3** — **Ateb Cywir: B**

NODYN ADDYSGU

Mae OpenVPN wedi'i integreiddio'n dynn ag OpenSSL, sy'n darparu seiffrau fel AES-GCM ac yn ei wneud yn ffurfweddadwy iawn ond yn fwy cymhleth.

4 **Perfformiad Protocol** RHEOLAETHAU LLWYBRO — **Ateb Cywir: A**

NODYN ADDYSGU

Mae WireGuard yn sefydlu ysgwyd llaw mewn milieiliadau ac yn ymateb ar unwaith i grwydro rhwng rhwydweithiau (e.e. newid o Wi-Fi i rwydwaith cellog). Ffynhonnell: Microsoft Native Gateway, Apple Support.

5 **Cryptograffeg Anghymesur** PREIFATRWYDD — **Ateb Cywir: C**

NODYN ADDYSGU

Mae WireGuard yn defnyddio Cryptokey Routing, gan gysylltu allweddi cyhoeddus â chyfeiriadau IP twnnel a ganiateir, yn debyg i ffurfweddiadau gosod SSH. Ffynhonnell: WireGuard Project.

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Cwestiwn 6** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae gweithrediad Linux WireGuard yn llai na 4,000 o linellau, felly gall timau diogelwch ei adolygu'n llawer cyflymach na sylfeini cod VPN llawer mwy fel OpenVPN.

7 **Hwyrni Gofod Defnyddwyr** CYFLYMDERAU — **Ateb Cywir: Gau**

NODYN ADDYSGU

Mae OpenVPN yn rhedeg yng ngofod y defnyddiwr, gan basio pecynnau yn ôl ac ymlaen o ryngwyneb rhithwir y cnewyllyn, sy'n ychwanegu gorbenion newid cyd-destun (oni bai bod dadlwytho i'r cnewyllyn fel OpenVPN DCO yn cael ei ddefnyddio). Ffynhonnell: DD-WRT custom firmware.

8 **Ffurfweddu OpenVPN** RISG CLUSTFEINIO — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae OpenVPN yn cefnogi rhedeg dros TCP (er mwyn dibynadwyedd/osgoi waliau tân) neu UDP (er mwyn cyflymder), sy'n ei wneud yn gydnaws â waliau tân menter cymhleth. Ffynhonnell: IETF Cryptographic Protocols.

9 **Cryptograffeg Fodern** WALIAU TÂN — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae WireGuard yn cefnu ar seiffrau etifeddol o blaid cyntefigion modern a diogel fel ChaCha20 a Poly1305, sy'n rhedeg yn gyflym ar CPUau symudol. Ffynhonnell: WireGuard Project.

10 **Symleiddio Parau Allweddi** DIM LOGIAU — **Ateb Cywir: Gau**

NODYN ADDYSGU

Nid yw WireGuard yn defnyddio tystysgrifau na hierarchaethau CA cymhleth; mae'n dibynnu ar barau allweddi cyhoeddus/preifat syml a gyfnewidir rhwng cymheiriaid. Ffynhonnell: WireGuard Project.

Allweddi Geirfa a Chyfarwyddyd Marcio

Cyfarwyddyd Marcio i Athrawon: Rhowch 1 pwynt am bob paru cywir (8 pwynt i gyd) a phob term cyd-destun (6 phwynt i gyd).

PWYNT GWIRIO 4: ALLWEDD PARU CYSYNIADAU

G 1. WireGuard	H 2. OpenVPN	E 3. Gofod y Cnewyllyn	A 4. Gofod y Defnyddiwr
B 5. 4,000 o Linellau	C 6. OpenSSL	F 7. Pâr o Allweddi	D 8. TCP/UDP

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 WIREGUARD	2 OPENVPN	3 GOFOD CNEWYLLYN	4 GOFOD DEFNYDDIWR
5 PARAU ALLWEDDI	6 ARCHWILIADWYEDD		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 F – OPENSSL	2 C – CNEWYLLYN	3 B – OPENVPN	4 G – PARALLWEDDI
5 H – TCPUDP	6 E – CODCRYNO	7 A – WIREGUARD	8 D – DEFNYDDIWR

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio WireGuard, OpenVPN a Gofod y Cnewyllyn yn eu geiriau eu hunain a rhoi enghraifft o bob un.

Astudiaethau Achos:
Gofynnwch i fyfyrwyr gefnogi eu hargymhellion â ffeithiau o'r daflen waith yn hytrach na thybiaethau.

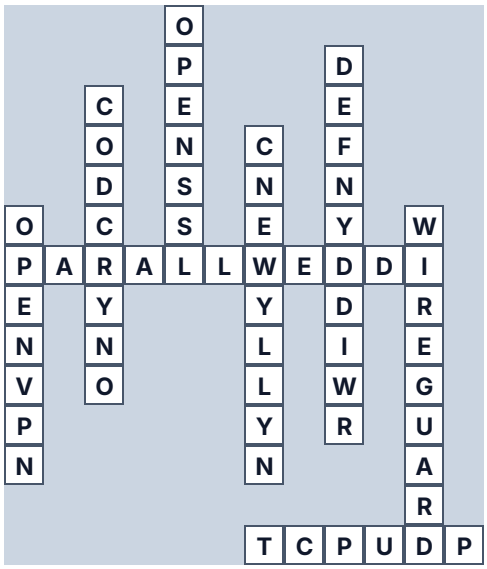
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

U	S	T	E	L	J	B	C	A	B	C	P	X	L	K
Y	K	X	T	K	D	Q	O	M	J	O	D	I	N	N
R	K	Q	P	G	M	M	D	Q	R	P	S	T	T	G
W	P	C	S	Q	O	H	C	S	B	E	W	D	S	Z
I	D	V	C	Z	P	W	R	F	K	N	H	Z	W	D
D	U	N	D	Q	A	X	Y	P	C	V	U	B	I	A
D	P	Z	N	D	R	K	N	C	A	P	D	O	R	D
Y	C	F	H	I	A	D	O	N	O	N	R	Q	E	M
N	T	E	I	R	L	Z	S	E	P	F	Q	V	G	F
F	A	A	Q	O	L	N	P	W	E	T	X	Q	U	K
E	R	U	S	D	W	N	Y	Y	N	B	F	S	A	X
D	W	J	A	R	E	Z	Y	L	S	Y	L	G	R	I
M	R	J	M	L	D	T	O	L	S	H	Q	Q	D	H
Z	A	O	V	G	D	U	B	Y	L	Y	R	Y	B	H
L	Z	G	J	O	I	P	N	N	W	C	M	Z	Y	G

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

7 ar draws: PARALLWEDDI Tocynnau anghymesur a ddefnyddir gan WireGuard i ddilysu cysylltiadau cymheiriaid (11 llythyren)

8 ar draws: TCPUDP Protocolau cludo y mae OpenVPN yn eu cefnogi; dros UDP yn unig y mae WireGuard ei hun yn rhedeg (6 llythyren)

CLIWIAU I LAWR

1 i lawr: OPENSSL Llyfrgell gryptograffig y mae OpenVPN yn dibynnu arni ar gyfer algorithmau seiffr (7 llythyren)

2 i lawr: DEFNYDDIWR Gofod y ...: ardal weithredu lle mae OpenVPN yn rhedeg, gan greu gorbenion newid cyd-destun (10 llythyren)

3 i lawr: CODCRYNO Maint bach sylfaen god WireGuard, sy'n ei gwneud yn llawer haws ei harchwilio (8 llythyren)

4 i lawr: CNEWYLLYN Gofod y ...: ardal weithredu'r system weithredu lle mae WireGuard yn rhedeg er mwyn cyflymder (9 llythyren)

5 i lawr: OPENVPN Protocol etifeddol cadarn sy'n defnyddio sylfaen god ffurfweddu fawr a chymhleth (7 llythyren)

6 i lawr: WIREGUARD Protocol VPN modern a gynlluniwyd ar gyfer cyflymder uchel ac archwilio cod syml (9 llythyren)

Allwedd Datrys Geiriau Cymysg a Seiffr

Allwedd marcio ar gyfer y gweithgaredd dad-sgramblo geirfa a'r Her Seiffr Gyfrinachol.

ALLWEDD DATRYS GEIRIAU CYMYSG

1. UGEIWARDR	WIREGUARD	5. VNNEOPP	OPENVPN
2. NCYWNLLYE	CNEWYLLYN	6. WYNDIDEDRF	DEFNYDDIWR
3. COCRYOND	CODCRYNO	7. OSSLPNE	OPENSSL
4. WDILRLDEPAA	PARALLWEDDI	8. PPTDUC	TCPUDP

ALLWEDD HER Y SEIFFR CYFRINACHOL

"UWCHRADDIWCH EICH OPENVPN GYDA THWNNEL CYFLYMACH"

Allwedd Atebion yr Astudiaethau Achos

A Senario A: Dewis Protocol

CLUSTFEINIO AC AMGRYPTIO | Cyfyng-gyngor Sarah

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Argymhelliad: WireGuard. Mae ei ddyluniad ysgafn, digyswllt yn gadael i'r twnnel adfer yn gyflym pan fydd ei rhwydwaith yn newid, ac mae ChaCha20-Poly1305 yn cadw'r amgryptio'n gyflym.
- Diogelwch: Mae'r ddau brotocol yn amgryptio ei thraffig ar Wi-Fi'r caffi, felly mae'r naill neu'r llall yn diogelu ei manylion mewngofnodi pan fyddant wedi'u ffurfweddu'n gywir; mae'r dewis yn effeithio'n bennaf ar gyflymder a sefydlogrwydd.

B Senario B: Mynd Heibio i Flociau VPN

GEO-RWYSTRO A CHYFEIRIADAU IP | Dilema Alex

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Pam Mae Wedi'i Flocio: Mae WireGuard yn defnyddio UDP yn unig, ac mae wal dân y gwesty yn debygol o flocio UDP neu adnabod pecynnau WireGuard drwy hidlo neu Archwilio Pecynnau Dwfn.
- Sut mae OpenVPN yn Helpu: Gall redeg dros TCP, gan gynnwys porth 443 a ddefnyddir gan HTTPS; anaml y bydd waliau tân gwestai'n rhwystro hwnnw'n llwyr oherwydd bod pori'r we yn dibynnu arno.