Enw: _____ Dyddiad: _____ Sgôr: _____

Diogelwch Mullvad

Dadansoddi pensaernïaeth ddiogelwch Mullvad VPN gan gynnwys gweinyddion di-ddisg RAM yn unig, polisïau dim logiau wedi'u harchwilio, cynhyrchu allweddi'n lleol, amgryptio WireGuard a ffurfweddiadau twnnel sy'n gwrthsefyll cwantwm.

TROSOLWG DYSGU DIOGELWCH MULLVAD

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 bensaernïaeth ddiogelwch Mullvad. Byddwch yn archwilio gweinyddion RAM yn unig heb ddisg, polisïau dim logiau wedi'u harchwilio, cynhyrchu allweddi'n lleol a thwneli sy'n gwrthsefyll cyfrifiadura cwantwm.

PWYNTIAU GWIRIO'R DAFLEN WAITH

- [ ] **Rhan 1-4: Meistroli ffurfweddiadau VPN a diogelwch rhwydwaith.**
- [ ] **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 VPNs Gorau VPN.com

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

Eich Map Llwybr Dysgu Diogelwch Mullvad

- Dadansoddwch bensaernïaeth dechnegol a rheolau ffurfweddu Diogelwch Mullvad.
- Ffurfweddwch osodiadau'r cleient i atal gollyngiadau traffig IP, DNS a WebRTC.
- Cymharwch brisiau personol, treialon a nodweddion perfformiad â modelau safonol.

CYFARWYDDIADAU'R CANLLAW I DDIOGELWCH MULLVAD

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 reolyddion gweinydd Mullvad sy'n rhoi preifatrwydd yn gyntaf. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

GWERTHUSO SEILWAITH SY'N RHOI ANHYSBYSRWYDD YN GYNTAF A HAENAU RAM (CYFLWYNIAD)

Nid yw Mullvad yn defnyddio cyfrifon safonol gyda chyfrineiriau, gan ddibynnu ar godau 16 digid a gynhyrchir ar hap. Mae ei seilwaith wedi'i beiriannu gyda nodau RAM yn unig heb ddisg, allweddi WireGuard a gynhyrchir yn lleol, a pholisïau dim cadw data wedi'u harchwilio.

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

Pwynt Gwirio 1: Her Amlddewis

1. **1. Pa brotocol twnelu sy'n ddiofyn yn ap Mullvad?**
   - A) OpenVPN
   - B) WireGuard
   - C) IKEv2
   - D) PPTP

2. **2. Beth mae Mullvad yn ei ofyn er mwyn creu cyfrif newydd?**
   - A) Dim byd o gwbl
   - B) Cyfeiriad e-bost
   - C) Rhif ffôn
   - D) Dogfen adnabod

3. **3. Pa dwnnel cryptograffig sy'n amddiffyn rhag cyfrifiaduron cwantwm?**
   - A) AES-256-GCM
   - B) Quantum WireGuard
   - C) RSA-4096
   - D) Dirprwy SOCKS5

4. **4. Pa fecanwaith diogelwch sy'n blocio peryglon gollyngiadau WebRTC?**
   - A) Estyniad Porwr
   - B) Kill Switch Rhwydwaith
   - C) Llwybro WebRTC drwy ryngwyneb y VPN
   - D) Twnelu Hollt

5. **5. Pa nodwedd aml-naid sy'n llwybro traffig drwy nodau lluosog?**
   - A) NAT Dwbl
   - B) WireGuard Multihop
   - C) Protocol Chameleon
   - D) Bypasser

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae Mullvad yn gofyn am gyfeiriad e-bost wrth gynhyrchu cyfrif.

○ Gwir ○ Gau

7 Cwestiwn 7

7. Gellir ffurfweddu dirprwyon SOCKS5 y tu mewn i dwneli Mullvad.

○ Gwir ○ Gau

8 Cwestiwn 8

8. Mae Mullvad yn berchen ar ei holl galedwedd gweinyddion ac yn ei weithredu.

○ Gwir ○ Gau

9 Cwestiwn 9

9. Mae'r Network Kill Switch bob amser yn weithredol yn ddiofyn.

○ Gwir ○ Gau

10 Cwestiwn 10

10. Nid oes modd ad-dalu taliadau arian parod a anfonir drwy'r post o gwbl.

○ 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 Mullvad yn dibynnu ar _____ fel ei brif brotocol twnnel diogel cyflym.

2. Yr enw ar lwybro data drwy ddau leoliad gweinydd yw ffurfweddiad _____ .

3. Er mwyn atal logiau data ar ddisg, mae Mullvad yn defnyddio nodau penodedig _____ .

4. Caiff traffig y system ei rwystro pan fydd twnnel yn methu drwy'r mesur diogelwch _____ adeiledig.

5. Mae datganiadau archwilio yn cadarnhau bod Mullvad yn cynnal pensaernïaeth _____ lem wedi'i dilysu.

6. Gellir ynysu llwybro rhaglenni mewnol gan ddefnyddio gosodiad _____ pwrpasol.

7. Mae algorithmau amgryptio ôl-gwantwm yn diogelu data y tu mewn i dwnnel _____ .

8. Caiff gweinyddion enwau preifat eu defnyddio ledled y byd i helpu i rwystro peryglon _____ .

BANC GEIRIAU GEIRFA

AML-NAID CWANTWM DIM LOGIAU DIRPRWY SOCKS5 GOLLYNGIAD DNS KILL SWITCH RAM YN UNIG WIREGUARD

Ysgrifennwch eich atebion yma:

1. 2.

3. 4.

5. 6.

7. 8.

Pwynt Gwirio 4: Paru Cysyniadau VPN a Rhwydwaith

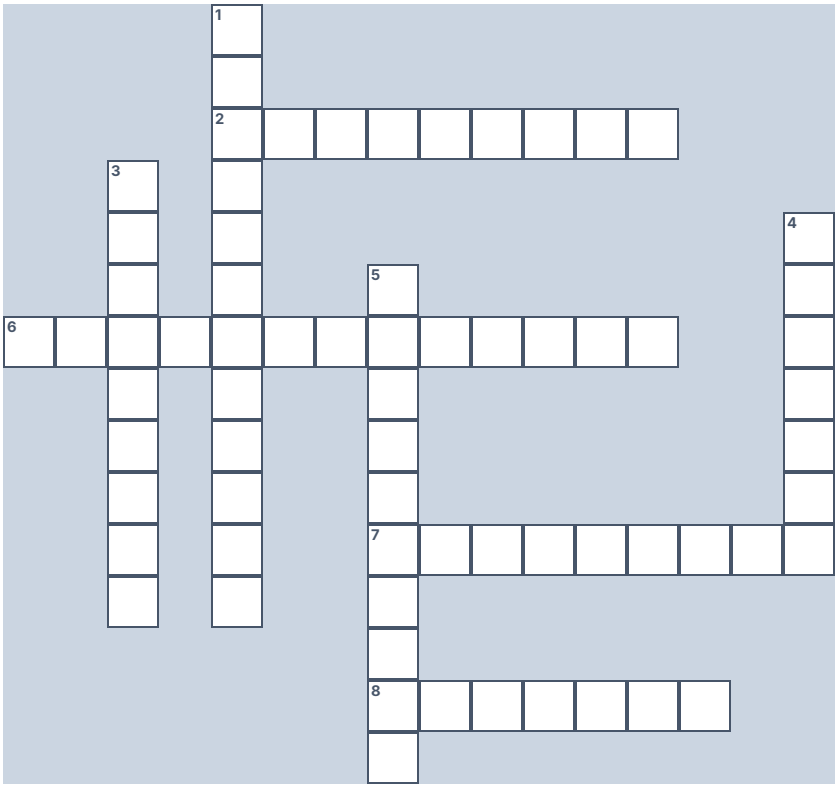
PARU DIFFINIADAU

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	Nodwedd ddiogelwch sy'n torri traffig pan fydd VPN yn gollwng.
☐	2. AML-NAID	B	Protocol twnelu diogel ysgafn, perfformiad uchel.
☐	3. RAM YN UNIG	C	Protocol dirprwy mewnol a ddefnyddir i ynysu rhaglenni cleient.
☐	4. KILL SWITCH WRT	D	Llwybro traffig drwy nod gweinydd mynediad ac allanfa.
☐	5. DIM LOGIAU	E	Mecanweithiau amgryptio a gynlluniwyd i wrthsefyll ymosodiadau cwantwm.
☐	6. DIRPRWY SOCKS5	F	Datgelu cyrchfannau ymholiadau DNS y tu allan i dwnnel y VPN.
☐	7. CWANTWM	G	Caledwedd gweinydd cof anweddol nad yw'n cadw unrhyw ddata wrth ailgychwyn.
☐	8. GOLLYNGIADAU DNS	H	Safon dim cadw data wedi'i gwirio gan archwiliadau annibynnol.

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

2. Caledwedd gweinydd cof anweddol nad yw'n cadw unrhyw ddata wrth ailgychwyn (9)

6. Datgelu cyrchfannau ymholiadau DNS y tu allan i dwnnel y VPN (13)

7. Protocol twnelu diogel ysgafn, perfformiad uchel (9)

8. Mecanweithiau amgryptio a gynlluniwyd i wrthsefyll ymosodiadau cwantwm (7)

CLIWIAU I LAWR

1. Protocol mewnol (SOCKS5) a ddefnyddir i ynysu rhaglenni cleient (12)

3. Safon cadw sero data a ddilyswyd gan archwiliadau annibynnol (9)

4. Llwybro traffig drwy nod gweinydd mynediad a nod gweinydd allanfa (7)

5. Nodwedd ddiogelwch sy'n torri traffig pan fydd VPN yn cwympo (10)

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

2 ar draws: Caledwedd gweinydd cof anweddol nad yw'n cadw unrhyw ddata wrth ailgychwyn (9 llythyren):

6 ar draws: Datgelu cyrchfannau ymholiadau DNS y tu allan i dwnnel y VPN (13 llythyren):

7 ar draws: Protocol twnelu diogel ysgafn, perfformiad uchel (9 llythyren):

8 ar draws: Mecanweithiau amgryptio a gynlluniwyd i wrthsefyll ymosodiadau cwantwm (7 llythyren):

CLIWIAU I LAWR

1 i lawr: Protocol mewnol (SOCKS5) a ddefnyddir i ynysu rhaglenni cleient (12 llythyren):

3 i lawr: Safon cadw sero data a ddilyswyd gan archwiliadau annibynnol (9 llythyren):

4 i lawr: Llwybro traffig drwy nod gweinydd mynediad a nod gweinydd allanfa (7 llythyren):

5 i lawr: Nodwedd ddiogelwch sy'n torri traffig pan fydd VPN yn cwympo (10 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.

S G I R Z S F K Q V F A A Q O

K I M N P T X I Q K W R U S D

C N W N Y B F L S X I W J A R

O U T Z A Y Y L L G R I M R J

S N N M M L T S O H E Q Q H Z

Y Y A A L O V W G U G B Y R Y

W M W B N H L I Z G U J O P N

R A C W A C M T Z Y A G Y O W

P R U K I V P C B N R V T M G

R V D Y D U K H R B D X Z Y M

I G O L L Y N G I A D D N S R

D Q X I P D A D J Q V W W L J

H T D I M L O G I A U H G B E

I K T S V R Z E H E S C A L Q

C Z M K V R U A S W J M M H H

RHESTR GEIRIAU GEIRFA

WIREGUARD AMLNAID RAMYNUNIG KILLSWITCH DIMLOGIAU
DIRPRWYSOCKS CWANTWM GOLLYNGIADDNS

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. AMLNAID
C. RAMYNUNIG
D. KILLSWITCH
E. DIMLOGIAU
F. DIRPRWYSOCKS
G. CWANTWM
H. GOLLYNGIADDNS

DIFFINIADAU A MEYSYDD PARU	
	1. Protocol mewnol (SOCKS5) a ddefnyddir i ynysu rhaglenni cleient.
	2. Mecanweithiau amgryptio a gynlluniwyd i wrthsefyll ymosodiadau cwantwm.
	3. Protocol twnelu diogel ysgafn, perfformiad uchel.
	4. Caledwedd gweinydd cof anweddol nad yw'n cadw unrhyw ddata wrth ailgychwyn.
	5. Nodwedd ddiogelwch sy'n torri traffig pan fydd VPN yn cwympo.
	6. Llwybro traffig drwy nod gweinydd mynediad a nod gweinydd allanfa.
	7. Datgelu cyrchfannau ymholiadau DNS y tu allan i dwnnel y VPN.
	8. Safon cadw sero data a ddilyswyd gan archwiliadau annibynnol.

Pwynt Gwirio 7: Her Geiriau Cymysg

Dad-sgramblwch y llythrennau isod i ddatgelu cysyniadau a thermau allweddol Rhwydwaith Preifat Rhithwir (VPN). Ysgrifennwch eich atebion yn y blychau mewnbwn a ddarperir.

1. **UGEIWARDR** _____

2. **GRIYAUNNM** _____

3. **DGOIIULAM** _____

4. **MWTNWCA** _____

5. **ADNLAIM** _____

6. **CSLITKIWHL** _____

7. **SORDIYSCKRWP** _____

8. **ALYNDISGGONDL** _____

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Nodweddion diogelwch yn Mullvad			
2	Cwestiynau i dîm cymorth cwsmeriaid Mullvad			
3	Ffyrdd o greu cyfrinair cryf			
4	Pobl y byddech chi'n argymell Mullvad iddynt			
5	Pethau y gall archwiliad eu gwirio			
6	Gwledydd sy'n adnabyddus am gyfreithiau preifatrwydd cryf			
7	Pethau rydych chi'n eu gwneud ar-lein bob dydd			
8	Gwledydd lle byddech chi eisiau gweinyddion Mullvad			
9	Gosodiadau rydych chi'n eu troi ymlaen er mwyn diogelwch ychwanegol			
10	Pethau y mae amgryptio yn eu diogelu			
11	Mathau o ollyngiadau VPN			
12	Geiriau diogelwch a ddysgoch yn y daflen waith hon			
13	Bygythiadau ar Wi-Fi cyhoeddus			
14	Apiau y byddech chi'n eu defnyddio ynghyd â Mullvad			
15	Dyfeisiau y byddech chi'n gosod Mullvad arnynt			

Pwynt Gwirio 8: Astudiaethau Achos VPN a Rhwydwaith

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

ASTUDIAETH ACHOS 1: INTEGREIDDIO GWRTHIANT CWANTWM

👷

Senario: Mae angen i gwmni ariannol ddiogelu trosglwyddiadau ffeiliau rhag dadgryptio cwantwm yn y dyfodol.

Cwestiwn Trafod: Pa ffurfweddiad twnnel y dylent ei ddefnyddio yn ap Mullvad?

ASTUDIAETH ACHOS 2: LLWYBRO YMCHWILIADOL LLECHWRAIDD

👷

Senario: Mae ymchwilydd am lwybro ei rwydwaith ddwywaith i guddio ei bwynt mynediad.

Cwestiwn Trafod: Pa nodwedd Mullvad y dylid ei galluogi i gyflawni llwybro drwy sawl gweinydd?

Pwynt Gwirio 9: Dadgryptio'r Seiffr

Mae peiriannydd rhwydwaith yn diogelu sianeli llwybro a thwneli cleientiaid. Defnyddiwch yr allwedd Llythyren-i-Rif isod i ddadgryptio'r neges drwy ysgrifennu'r llythrennau cyfatebol yn y bylchau gwag.

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

3	25	6	18	9	6	15	14		13	21	12	12	22	1	4		8	5	2

7	25	6	18	9	14	1	9	18		14	1	3		5	2	15	19	20

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 am Rwydweithiau Preifat Rhithwir (VPNs) a thwnelu.

Q1: Sut mae Mullvad yn diogelu cyfrifon?

Mae Mullvad yn defnyddio rhif cyfrif 16 digid a gynhyrchir heb fod angen cyfrinair nac e-bost. [1]

Q2: Pa brotocol mae Mullvad yn ei flaenoriaethu?

Mae Mullvad yn blaenoriaethu WireGuard oherwydd ei gyflymder, ei symlrwydd a'i gryptograffeg fodern. [9]

Q3: A yw gweinyddion Mullvad yn cael eu harchwilio?

Ie, mae cwmnïau diogelwch trydydd parti yn cynnal archwiliadau rheolaidd o'r seilwaith a'r cod.

Q4: A yw Mullvad yn cefnogi OpenVPN?

Na, tynnodd Mullvad OpenVPN ar 15 Ionawr 2026; WireGuard yn unig ydyw. [7]

Q5: Beth yw kill switch Mullvad?

Mae'n rheol wal dân integredig sy'n atal traffig rhyngrwyd os bydd y VPN yn methu.

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

Adolygwch y cwestiynau a'r atebion mwyaf cyffredin am Rwydweithiau Preifat Rhithwir (VPNs) a thwnelu.

Q6: A yw IPv6 yn cael ei gefnogi gan Mullvad?

Ydy, mae Mullvad yn cefnogi llwybro IPv6 brodorol a diogelwch rhag gollyngiadau.

Q7: A yw Mullvad yn cynnig multihop?

Ydy, mae multihop WireGuard yn caniatáu cadwyno sawl lleoliad gweinydd.

Q8: A allaf ddefnyddio datryswyr DNS personol?

Gellir, gellir ffurfweddu cyfeiriadau DNS wedi'u teilwra yng ngosodiadau cleient Mullvad.

Q9: Sut mae logiau'n cael eu hatal?

Mae ffurfweddiadau system yn analluogi logio ac yn glanhau celciau ar bob ellyll gweinydd.

Q10: Ble mae Mullvad wedi'i gorffori?

Mae Mullvad wedi'i gorffori yn Gothenburg, Sweden, o dan awdurdodaeth Sweden.

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

Archwilio agweddau technegol uwch ar brotocolau twnelu VPN, integreiddio cleientiaid symudol, a defnyddio mewn mentrau.

Q1: Sut mae cylchdroi allweddi'n gweithio?

Mae'r ap yn cylchdroi allweddi WireGuard yn awtomatig; yr egwyl ddiofyn yn y CLI yw 30 diwrnod. [3]

Q2: Beth yw twneli sy'n gwrthsefyll cwantwm?

Maent yn ychwanegu cyfnewid allweddi ML-KEM a Classic McEliece at WireGuard i wrthsefyll ymosodiadau cwantwm yn y dyfodol. [2]

Q3: Sut mae nodau RAM-yn-unig yn ddiogel?

Nid yw'r nodau hyn yn ysgrifennu unrhyw ddata i yriannau caled, gan wneud dwyn gweinyddion ffisegol yn ddiwerth.

Q4: Beth yw swyddogaeth y dirprwy SOCKS5?

Mae'n helpu i lwybro traffig apiau penodol o fewn y twnnel, gan atal gollyngiadau i rwydweithiau allanol.

Q5: A yw Mullvad yn diogelu rhag gollyngiadau WebRTC?

Ie, mae'r ap yn gorfodi ymholiadau WebRTC drwy ryngwyneb y VPN i gysgodi cyfeiriadau IP lleol.

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

Archwilio agweddau technegol uwch ar brotocolau twnelu VPN, integreiddio cleientiaid symudol, a defnyddio mewn mentrau.

Q6: Sut mae Mullvad yn ymdrin â chyrchoedd yr heddlu?

Nid yw Mullvad yn cadw unrhyw logiau cronfa ddata defnyddwyr, sy'n golygu na ellir echdynnu unrhyw wybodaeth am ddefnyddwyr.

Q7: Beth yw risg awdurdodaeth Sweden?

Mae Sweden yn aelod o'r 14 Llygad, ond mae pensaernïaeth dim logiau Mullvad yn dileu'r risg i ddata.

Q8: A yw archwiliadau apiau cleient yn god agored?

Ie, mae'r apiau'n ffynhonnell agored (GPL-3) ac wedi'u harchwilio gan gwmnïau fel X41 D-Sec. [6]

Q9: Sut mae twnelu hollt yn gweithredu?

Mae'n defnyddio tablau llwybro'r system weithredu i eithrio apiau penodol o orbenion y VPN.

Q10: Sut mae Mullvad yn ymdrin â thaliadau arian parod?

Caiff arian parod ei bostio gyda chod tocyn, ei gredydu â llaw, a chaiff yr amlenni eu rhwygo.

Rhan 11: 10 Ffaith a Mewnwelediad VPN o'r Byd Go Iawn

Adolygwch ffeithiau o'r byd go iawn am gyflymderau amgryptio VPN, archwiliadau protocol, cysylltedd symudol, a gweithio o bell mewn mentrau.

1. CIPOLWG AR VPN

Sefydlwyd Mullvad yn 2009 gan Amagicom AB yn Gothenburg, Sweden.

2. CIPOLWG AR VPN

Rhifau cyfrif yw'r unig ddynodwr a ddefnyddir i gredydu a chyrchu cyfrifon.

3. CIPOLWG AR VPN

Ni chaiff unrhyw enwau, e-byst, cyfrineiriau na rhifau ffôn eu storio yng nghronfa ddata'r defnyddwyr.

4. CIPOLWG AR VPN

Caiff allweddi WireGuard eu cynhyrchu'n lleol ar ddyfeisiau cleient i atal cyfaddawdu ar ochr y gweinydd.

5. CIPOLWG AR VPN

Ni chanfu archwiliad seilwaith Cure53 yn 2024 unrhyw ddiffyg sy'n torri anhysbysrwydd traffig VPN. [5]

6. CIPOLWG AR VPN

Mae pob gweinydd WireGuard Mullvad yn rhedeg dirprwy SOCKS5, y gellir ei gyrraedd o fewn y twnnel yn unig. [8]

7. MEWNWELEDIAD VPN

Gellir cuddio traffig WireGuard gyda Shadowsocks, QUIC neu LWO i basio drwy waliau tân. [10]

8. MEWNWELEDIAD VPN

Cwblhaodd Mullvad ei symudiad i weinyddion VPN RAM yn unig ym mis Medi 2023. [4]

9. MEWNWELEDIAD VPN

Mae ML-KEM a Classic McEliece yn negodi allwedd a rennir ymlaen llaw ôl-gwantwm ar gyfer WireGuard. [2]

10. CIPOLWG AR VPN

Caiff amlenni arian parod a'u cynnwys nad yw'n arian eu rhwygo ar ôl i'r amser gael ei gredydu.

Cyfeiriadau a Ffynonellau Technegol

Mae'r canllaw astudio a'r posau rhyngweithiol wedi'u llunio o safonau technegol, manylebau a fframweithiau rheoleiddio byd-eang.

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[1] Mullvad VPN. (n.d.). Why Mullvad VPN?
https://mullvad.net/en/why-mullvad-vpn

[2] Mullvad VPN. (n.d.). Quantum-resistant tunnels with WireGuard.
https://mullvad.net/en/help/quantum-resistant-tunnels-with-wireguard

[3] Mullvad VPN. (n.d.). CLI commands for using WireGuard.
https://mullvad.net/en/help/cli-command-wg

[4] Mullvad VPN. (2023). We have successfully completed our migration to RAM-only VPN infrastructure.
https://mullvad.net/en/blog/we-have-successfully-completed-our-migration-to-ram-only-vpn-infrastructure

[5] Mullvad VPN. (2024). Fourth Infrastructure audit completed by Cure53.
https://mullvad.net/en/blog/fourth-infrastructure-audit-completed-by-cure53

[6] Mullvad VPN. (2024). The report for the 2024 security audit of the app is now available.
https://mullvad.net/en/blog/the-report-for-the-2024-security-audit-of-the-app-is-now-available

[7] Mullvad VPN. (2024). Removing OpenVPN 15th January 2026.
https://mullvad.net/en/blog/removing-openvpn-15th-january-2026

[8] Mullvad VPN. (n.d.). SOCKS5 proxy.
https://mullvad.net/en/help/socks5-proxy

[9] Mullvad VPN. (n.d.). Why WireGuard?
https://mullvad.net/en/help/why-wireguard

[10] Mullvad VPN. (n.d.). Using Mullvad VPN in restrictive locations.
https://mullvad.net/en/help/connecting-to-mullvad-vpn-from-restrictive-locations

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

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

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Cwestiwn 1** — **Ateb Cywir: B**

NODYN ADDYSGU

Pa brotocol twnelu sy'n ddiofyn yn ap Mullvad? → WireGuard

2 **Cwestiwn 2** — **Ateb Cywir: A**

NODYN ADDYSGU

Mae clicio "generate account" yn rhoi rhif cyfrif i chi; ni ofynnir am e-bost na gwybodaeth bersonol arall.

3 **Cwestiwn 3** — **Ateb Cywir: B**

NODYN ADDYSGU

Mae twnelau WireGuard Mullvad sy'n gwrthsefyll cyfrifiaduron cwantwm yn defnyddio ML-KEM a Classic McEliece i gytuno ar allwedd a rennir ymlaen llaw. [2]

4 **Cwestiwn 4** — **Ateb Cywir: C**

NODYN ADDYSGU

Pa fecanwaith diogelwch sy'n blocio peryglon gollyngiadau WebRTC? → Llwybro WebRTC drwy ryngwyneb y VPN

5 **Cwestiwn 5** — **Ateb Cywir: B**

NODYN ADDYSGU

Pa nodwedd aml-naid sy'n llwybro traffig drwy nodau lluosog? → WireGuard Multihop

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Cwestiwn 6** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: nid yw Mullvad byth yn gofyn am e-bost; dim ond rhif a gynhyrchwyd sy'n adnabod cyfrifon.

7 **Cwestiwn 7** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gellir ffurfweddu dirprwyon SOCKS5 y tu mewn i dwneli Mullvad.

8 **Cwestiwn 8** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae Mullvad yn berchen ar rai gweinyddion ond mae hefyd yn rhentu gweinyddion penodedig gan ddarparwyr.

9 **Cwestiwn 9** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae'r Network Kill Switch bob amser yn weithredol yn ddiofyn.

10 **Cwestiwn 10** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Nid oes modd ad-dalu taliadau arian parod a anfonir drwy'r post o gwbl.

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

B 1. WIREGUARD	D 2. AML-NAID	G 3. RAM YN UNIG	A 4. KILL SWITCH WRT
H 5. DIM LOGIAU	C 6. DIRPRWY SOCKS5	E 7. CWANTWM	F 8. GOLLYNGIADAU DNS

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 WIREGUARD	2 AML-NAID	3 RAM YN UNIG	4 KILL SWITCH
5 DIM LOGIAU	6 DIRPRWY SOCKS5	7 CWANTWM	8 GOLLYNGIAD DNS

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 F – DIRPRWYSOCKS	2 G – CWANTWM	3 A – WIREGUARD	4 C – RAMYNUNIG
5 D – KILLSWITCH	6 B – AMLNAID	7 H – GOLLYNGIADDNS	8 E – DIMLOGIAU

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio WIREGUARD, AML-NAID a RAM YN UNIG 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.

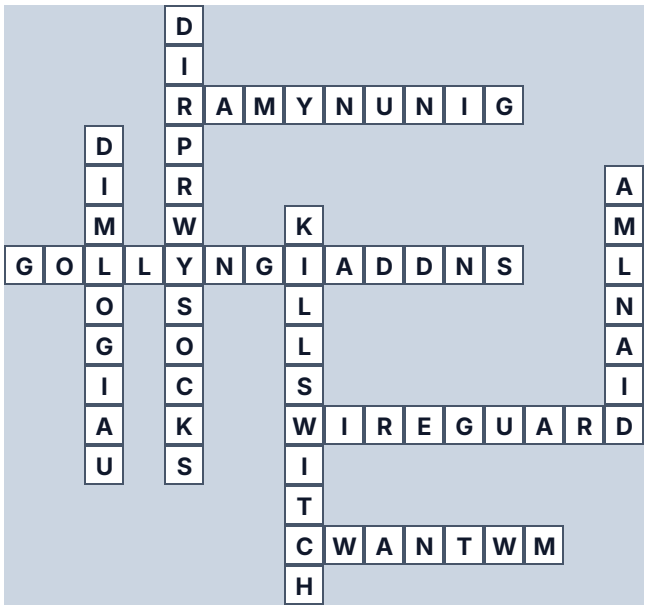
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

2 ar draws: RAMYNUNIG Caledwedd gweinydd cof anweddol nad yw'n cadw unrhyw ddata wrth ailgychwyn (9 llythyren)

6 ar draws: GOLLYNGIADDNS Datgelu cyrchfannau ymholiadau DNS y tu allan i dwnnel y VPN (13 llythyren)

7 ar draws: WIREGUARD Protocol twnelu diogel ysgafn, perfformiad uchel (9 llythyren)

8 ar draws: CWANTWM Mecanweithiau amgryptio a gynlluniwyd i wrthsefyll ymosodiadau cwantwm (7 llythyren)

CLIWIAU I LAWR

1 i lawr: DIRPRWYSOCKS Protocol mewnol (SOCKS5) a ddefnyddir i ynysu rhaglenni cleient (12 llythyren)

3 i lawr: DIMLOGIAU Safon cadw sero data a ddilyswyd gan archwiliadau annibynnol (9 llythyren)

4 i lawr: AMLNAID Llwybro traffig drwy nod gweinydd mynediad a nod gweinydd allanfa (7 llythyren)

5 i lawr: KILLSWITCH Nodwedd ddiogelwch sy'n torri traffig pan fydd VPN yn cwympo (10 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.	ADNLAIM	AMLNAID
2.	GRIYAUNNM	RAMYNUNIG	6.	CSLITKIWHL	KILLSWITCH
3.	DGOIIULAM	DIMLOGIAU	7.	SORDIYSCKRWP	DIRPRWYSOCKS
4.	MWTNWCA	CWANTWM	8.	ALYNDISGGONDL	GOLLYNGIADDNS

ALLWEDD HER Y SEIFFR CYFRINACHOL

"CYFRIFON MULLVAD HEB GYFRINAIR NAC EBOST"

Allwedd Atebion yr Astudiaethau Achos

A ASTUDIAETH ACHOS 1: INTEGREIDDIO GWRTHIANT CWANTWM

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae angen i gwmni ariannol ddiogelu trosglwyddiadau ffeiliau rhag dadgryptio cwantwm yn y dyfodol.
- Strategaeth a Datrysiad a Argymhellir: Defnyddiwch dwneli WireGuard gwrthsefyll cwantwm gan ddefnyddio allweddi a rennir ymlaen llaw ôl-gwantwm.

B ASTUDIAETH ACHOS 2: LLWYBRO YMCHWILIADOL LLECHWRAIDD

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae ymchwilydd am lwybro ei rwydwaith ddwywaith i guddio ei bwynt mynediad.
- Strategaeth a Datrysiad a Argymhellir: Galluogwch nodwedd WireGuard Multihop Mullvad i raeadru nodau mynediad ac ymadael.