Enw: _____ Dyddiad: _____ Sgôr: _____

# Diogelwch ExpressVPN

Gwerthuso seilwaith diogelwch ExpressVPN, y protocol ffynhonnell agored pwrpasol Lightway, technoleg TrustedServer RAM yn unig, archwiliadau diogelwch annibynnol, a kill switch Network Lock.

## TROSOLWG DYSGU DIOGELWCH EXPRESSVPN

**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 nodweddion diogelwch ExpressVPN. Byddwch yn archwilio protocolau ffynhonnell agored, nodau gweinydd RAM yn unig, seiffrau, a'r Internet Kill Switch.

### 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/expressvpn/diogelwch/

# Eich Map Llwybr Dysgu Diogelwch ExpressVPN

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

### CYFARWYDDIADAU CANLLAW DIOGELWCH EXPRESSVPN

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 brotocolau ffynhonnell agored a nodau gweinydd RAM-yn-unig. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

### ARAEAU GWEINYDDION RAM-YN-UNIG A PHROTOCOLAU CYSYLLTU COD AGORED

Mae ExpressVPN yn defnyddio technoleg TrustedServer RAM yn unig i atal logiau lleol, ynghyd â'i brotocol ffynhonnell agored pwrpasol Lightway ac Internet Kill Switch i ddarparu diogelwch data defnyddwyr o un pen i'r llall.

### (CYFLWYNIAD)

Mae ExpressVPN yn defnyddio technoleg TrustedServer RAM yn unig i atal logiau lleol, ynghyd â'i brotocol ffynhonnell agored pwrpasol Lightway ac Internet Kill Switch i ddarparu diogelwch data defnyddwyr o un pen i'r llall.

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

## Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw protocol ffynhonnell agored pwrpasol ExpressVPN?**
   - A) Lightway
   - B) WireGuard
   - C) OpenVPN
   - D) Chameleon

2. **2. Pa dechnoleg gweinydd sy'n rhedeg mewn RAM anweddol yn unig?**
   - A) TrustedServer
   - B) RAM-Core
   - C) SecureRAM
   - D) Gweinydd NoSpy

3. **3. Beth sy'n digwydd os bydd cysylltiad VPN yn gollwng yn annisgwyl?**
   - A) Mae'r kill switch yn rhwystro traffig
   - B) Traffig yn gollwng i'r ISP
   - C) Ailgychwyn y system
   - D) Mae'r data'n cael ei ddadamgryptio

4. **4. Ble mae ExpressVPN wedi'i gorffori i ddiogelu preifatrwydd?**
   - A) Ynysoedd Virgin Prydeinig
   - B) Y Swistir
   - C) Panama
   - D) Rwmania

5. **5. Pa seiffr amgryptio cymesur a ddefnyddir yn ddiofyn?**
   - A) AES-256-GCM
   - B) Blowfish
   - C) DES-64
   - D) RC4

## Pwynt Gwirio 2: Her Gwir neu Gau

### 6 Cwestiwn 6

6. Mae technoleg TrustedServer yn storio logiau'r gweinydd ar yriannau caled.

Gwir Gau

### 7 Cwestiwn 7

7. Mae ExpressVPN wedi bod drwy archwiliadau diogelwch trydydd parti.

Gwir Gau

### 8 Cwestiwn 8

8. Mae protocol Lightway wedi'i adeiladu ar ben sylfaen cod OpenVPN.

Gwir Gau

### 9 Cwestiwn 9

9. Mae'r kill switch ymlaen yn ddiofyn ar apiau bwrdd gwaith.

Gwir Gau

### 10 Cwestiwn 10

10. Mae ExpressVPN yn gweithredu DNS preifat ar bob un o'i weinyddion.

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. Y protocol cyflym a ddyluniwyd yn fewnol gan ExpressVPN yw _____ .

2. Er mwyn atal cadw data, mae'r rhwydwaith gweinyddion yn dibynnu ar nodau RAM yn unig o'r enw _____ .

3. Hen enw kill switch ExpressVPN oedd Network _____ .

4. Mae ExpressVPN wedi'i gofrestru o dan gyfreithiau _____ Virgin Prydeinig.

5. Mae llwythi data wedi'u diogelu gan y seiffr cymesur cadarn _____ .

6. Mae'r polisi dim logiau wedi'i ddilysu, ac mae'n _____ yn annibynnol gan gwmnïau blaenllaw.

**BANC GEIRIAU GEIRFA**

AES-256 ARCHWILIEDIG DNS PREIFAT GOLLYNGIAD LIGHTWAY LOCK TRUSTED SERVER YNYSOEDD

**Ysgrifennwch eich atebion yma:**

1. 2.

3. 4.

5. 6.

# Pwynt Gwirio 4: Paru Cysyniadau VPN a Rhwydwaith

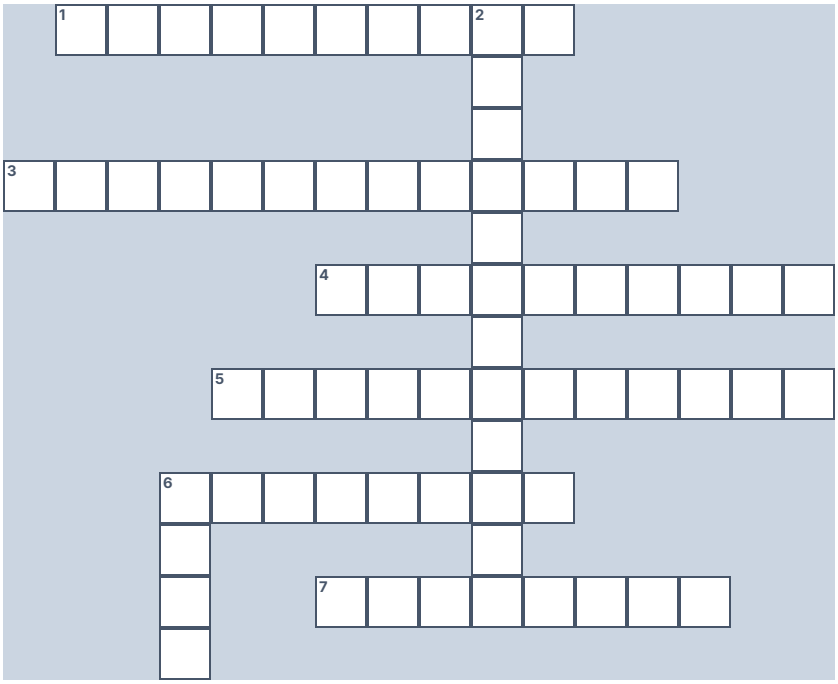
**PARU DIFFINIADAU**

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. LIGHTWAY | A | Awdurdodaeth Ynysoedd Virgin Prydain sy'n cynnig preifatrwydd cryf |
| ☐ | 2. TRUSTED SERVER | B | Datgelu data IP, DNS neu WebRTC preifat yn anfwriadol |
| ☐ | 3. CLOI | C | Mae datryswyr y System Enwau Parth yn rhedeg yn breifat ar bob nod gweinydd |
| ☐ | 4. YNYSOEDD | D | Wedi'i ddilysu'n annibynnol gan gwmnïau diogelwch trydydd parti |
| ☐ | 5. AES-256 | E | Pensaernïaeth gweinyddion RAM-yn-unig sy'n atal storio data ar ddisg |
| ☐ | 6. WEDI'I ARCHWILIO | F | Gair olaf Network Lock, hen enw'r kill switch |
| ☐ | 7. GOLLYNGIAD | G | Protocol cysylltu ysgafn a ffynhonnell agored ExpressVPN |
| ☐ | 8. DNS | H | Safon amgryptio cymesur sy'n diogelu trosglwyddo data |

# 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

**1. Datgelu cyfeiriad IP, DNS neu ddata WebRTC preifat yn anfwriadol (10)**

**3. Pensaernïaeth gweinyddion RAM yn unig sy'n atal storio data ar ddisg (13)**

**4. Datryswyr System Enwau Parth a redir yn breifat ar bob nod gweinydd (10)**

**5. Wedi'i ddilysu'n annibynnol gan gwmnïau diogelwch trydydd parti (12)**

**6. Protocol cysylltu ysgafn, cod agored ExpressVPN (8)**

**7. Awdurdodaeth y BVI (Virgin Prydeinig) sy'n cynnig preifatrwydd cryf (8)**

## CLIWIAU I LAWR

**2. Safon gymesur sy'n diogelu data wrth ei drosglwyddo (12)**

**6. Gair olaf Network Lock, hen enw'r kill switch (4)**

# 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

**1 ar draws: Datgelu cyfeiriad IP, DNS neu ddata WebRTC preifat yn anfwriadol (10 llythyren):**

**3 ar draws: Pensaernïaeth gweinyddion RAM yn unig sy'n atal storio data ar ddisg (13 llythyren):**

**4 ar draws: Datryswyr System Enwau Parth a redir yn breifat ar bob nod gweinydd (10 llythyren):**

**5 ar draws: Wedi'i ddilysu'n annibynnol gan gwmnïau diogelwch trydydd parti (12 llythyren):**

**6 ar draws: Protocol cysylltu ysgafn, cod agored ExpressVPN (8 llythyren):**

**7 ar draws: Awdurdodaeth y BVI (Virgin Prydeinig) sy'n cynnig preifatrwydd cryf (8 llythyren):**

## CLIWIAU I LAWR

**2 i lawr: Safon gymesur sy'n diogelu data wrth ei drosglwyddo (12 llythyren):**

**6 i lawr: Gair olaf Network Lock, hen enw'r kill switch (4 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 T H G B E I K T S V R Z E H
E E D A I G N Y L L O G S Y L
A C A L Q C Z K M K V R N I U
O A S W J M C M H H N Y G H R
I F K T L O R W H B S H U F Y
T O Y W L S H T X O T A P U N
P N Z O I Q T I E W P V U O U
Y U K A E P M D A K A N V G G
R P Q X Y J D Y K V J Y W Y P
G J T A F I E R P S N D I Z I
M T R U S T E D S E R V E R J
A N A E I A S A J F W E K Z K
E K A R C H W I L I E D I G Q
N J A F O K N D N C D H I B A
P R L P W T I Y F Y S G X W H

**RHESTR GEIRIAU GEIRFA**

LIGHTWAY TRUSTEDSERVER LOCK YNYSOEDD AMGRYPTIOAES
ARCHWILIEDIG GOLLYNGIAD DNSPREIFAT

## 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. LIGHTWAY |
| B. TRUSTEDSERVER |
| C. LOCK |
| D. YNYSOEDD |
| E. AMGRYPTIOAES |
| F. ARCHWILIEDIG |
| G. GOLLYNGIAD |
| H. DNSPREIFAT |

| DIFFINIADAU A MEYSYDD PARU | |
| --- | --- |
| | 1. Datgelu cyfeiriad IP, DNS neu ddata WebRTC preifat yn anfwriadol. |
| | 2. Awdurdodaeth y BVI (Virgin Prydeinig) sy'n cynnig preifatrwydd cryf. |
| | 3. Datryswyr System Enwau Parth a redir yn breifat ar bob nod gweinydd. |
| | 4. Protocol cysylltu ysgafn, cod agored ExpressVPN. |
| | 5. Gair olaf Network Lock, hen enw'r kill switch. |
| | 6. Safon gymesur sy'n diogelu data wrth ei drosglwyddo. |
| | 7. Pensaernïaeth gweinyddion RAM yn unig sy'n atal storio data ar ddisg. |
| | 8. Wedi'i ddilysu'n annibynnol gan gwmnïau diogelwch trydydd parti. |

## 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. AHTLWIYG
2. LCKO
3. AMITEOGPSYAR
4. NAYDLIGGOL
5. EVRUSTRERDTES
6. DDSEYONY
7. IEWARLGDICIH
8. APETDRNIFS

# Gweithgaredd Bonws: Meddwl yn Gyflym

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

| | | | | |
|---|---|---|---|---|
| 1 | Nodweddion rydych chi'n chwilio amdanynt yn ExpressVPN | | | |
| 2 | Bygythiadau ar Wi-Fi cyhoeddus | | | |
| 3 | Mathau o ollyngiadau VPN | | | |
| 4 | Ffyrdd o greu cyfrinair cryf | | | |
| 5 | Botymau neu ddewislenni mewn ap VPN | | | |
| 6 | Pethau rydych chi'n eu gwneud ar-lein bob dydd | | | |
| 7 | Pobl y byddech chi'n argymell ExpressVPN iddynt | | | |
| 8 | Gwledydd sy'n adnabyddus am gyfreithiau preifatrwydd cryf | | | |
| 9 | Protocolau VPN rydych chi'n eu hadnabod | | | |
| 10 | Pethau y gall archwiliad eu gwirio | | | |
| 11 | Nodweddion diogelwch yn ExpressVPN | | | |
| 12 | Pethau i'w gwirio cyn prynu VPN | | | |
| 13 | Gosodiadau rydych chi'n eu troi ymlaen er mwyn diogelwch ychwanegol | | | |
| 14 | Pethau y mae amgryptio yn eu diogelu | | | |
| 15 | Pethau y gall ExpressVPN eu cuddio rhag eich rhwydwaith | | | |

# 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: GORFODI MESURAU DIOGELU RAM YN UNIG



**Senario:** Mae asiantaeth y llywodraeth yn cipio gweinydd ExpressVPN i dynnu logiau defnyddwyr a hanes cysylltu.

**Cwestiwn Trafod: Pa wybodaeth y byddant yn ei chanfod ar y gweinydd, a pham?**

## ASTUDIAETH ACHOS 2: TWNELI CYSYLLTIAD WI-FI ANSEFYDLOG



**Senario:** Mae gweithiwr o bell yn defnyddio Wi-Fi cyhoeddus gwesty sy'n torri bob ychydig funudau wrth olygu dogfennau.

**Cwestiwn Trafod:** Sut mae ExpressVPN yn diogelu eu data rhag gollwng pan fydd y cysylltiad yn torri?

## 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**

| 13 | 1 | 5 | | 20 | 18 | 21 | 19 | 20 | 5 | 4 | 19 | 5 | 18 | 22 | 5 | 18 | | 25 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | |

| 4 | 9 | 12 | 5 | 21 | | 16 | 15 | 2 | | 12 | 15 | 7 | | 2 | 15 | 2 | | 4 | 25 | 4 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | | |

**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: Pa amgryptio mae ExpressVPN yn ei ddefnyddio?

Mae ExpressVPN yn defnyddio amgryptio cymesur AES-256-GCM yn ddiofyn.

### Q2: Beth yw'r protocol Lightway?

Lightway yw protocol pwrpasol ExpressVPN a adeiladwyd ar gyfer cyflymder, diogelwch a sefydlogrwydd.

### Q3: A yw ExpressVPN yn cofnodi fy hanes chwilio?

Na, mae ExpressVPN yn gorfodi polisi dim logiau llym sydd wedi'i archwilio'n annibynnol.

### Q4: Beth yw Internet Kill Switch?

Dyma kill switch brodorol ExpressVPN sy'n rhwystro traffig rhyngrwyd os bydd y cysylltiad yn torri.

### Q5: A yw'r protocol Lightway yn god agored?

Ie, mae cod craidd y protocol Lightway yn ffynhonnell agored ac ar GitHub. [9]

# 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 ExpressVPN yn rhedeg DNS preifat?

Ydy, mae ExpressVPN yn gweithredu ei DNS preifat ei hun, wedi'i amgryptio, ar bob gweinydd. [7]

### Q7: Beth yw technoleg TrustedServer?

Mae'n drefniant gweinydd lle mae'r system weithredu a'r apiau'n rhedeg yn gyfan gwbl yng nghof RAM anweddol.

### Q8: A yw ExpressVPN wedi cael ei archwilio?

Ydy, mae ExpressVPN wedi cael ei archwilio gan gwmnïau fel PwC, Cure53 ac F-Secure. [1]

### Q9: A yw ExpressVPN yn diogelu rhag gollyngiadau DNS ac IPv6?

Ydy, mae Internet Kill Switch yn blocio traffig IPv4, IPv6 a DNS y tu allan i'r twnnel.

### Q10: Ble mae ExpressVPN wedi'i leoli?

Mae ExpressVPN wedi'i gorffori yn Ynysoedd Virgin Prydain (BVI).

# 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 pensaernïaeth RAM yn unig yn gwella diogelwch?

Nid yw data'n cael ei ysgrifennu i yriannau caled, ac mae data sy'n cael ei gadw yn y cof yn cael ei ddileu bob tro y caiff y gweinydd ei ddiffodd.

### Q2: Pam mae awdurdodaeth BVI yn bwysig i breifatrwydd?

Mae ExpressVPN wedi'i leoli yn BVI, felly mae ceisiadau cyfreithiol am ddata yn ddarostyngedig i gyfreithiau BVI.

### Q3: A yw ExpressVPN yn cefnogi cyfrinachedd ymlaen perffaith?

Ydy, mae Lightway yn defnyddio allweddi deinamig sy'n cael eu dileu a'u hailgynhyrchu'n rheolaidd.

### Q4: Sut mae Network Lock yn atal gollyngiadau IP?

Mae'n rhwystro pob traffig ar lefel y system pryd bynnag y bydd y cysylltiad VPN yn torri.

### Q5: A yw Lightway yn diogelu rhag ymosodiadau cwantwm?

Ydy, mae gan Lightway amddiffyniad ôl-gwantwm sy'n defnyddio safon ML-KEM NIST.

# 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: A all asiantaethau'r llywodraeth ryng-gipio traffig Lightway?

Gallant ei ryng-gipio, ond ni allant ei ddadgryptio oherwydd amgryptio AES-256/ChaCha20.

### Q7: Sut mae DNS preifat yn diogelu logiau chwilio defnyddwyr?

Mae'n prosesu pob ymholiad DNS o fewn y twnnel wedi'i amgryptio, gan atal monitro gan yr ISP.

### Q8: Ar gyfer beth mae Lightway Turbo yn cael ei ddefnyddio?

Mae'n defnyddio twnelu aml-lôn i anfon mwy o ddata ar yr un pryd ar gyfer cyflymderau cyflymach.

### Q9: Beth yw mantais Lightway dros WireGuard?

Mae Lightway wedi'i adeiladu'n bwrpasol i ymdopi'n gyflym â newidiadau rhwydwaith (fel Wi-Fi i ddata symudol) heb ollwng y cysylltiad.

### Q10: Pa mor aml mae meddalwedd y gweinydd yn cael ei hailosod?

Gyda TrustedServer, caiff y pentwr meddalwedd cyfan ei ail-lwytho o ddelwedd ddiogel darllen-yn-unig ar bob ailgychwyn.

## 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**

Mae Lightway yn defnyddio AES-256-GCM, neu ChaCha20/Poly1305 ar ddyfeisiau pŵer isel. [6]

**2. CIPOLWG AR VPN**

Mae technoleg TrustedServer wedi'i chynllunio i redeg holl weithrediadau'r gweinydd mewn RAM. [4]

**3. CIPOLWG AR VPN**

Ynysoedd Virgin Prydain (BVI) yw'r awdurdodaeth gorfforaethol. [8]

**4. CIPOLWG AR VPN**

Ailysgrifennwyd Lightway o C i Rust a chafodd ei archwilio gan Cure53 a Praetorian. [3]

**5. CIPOLWG AR VPN**

Mae Internet Kill Switch yn rhwystro traffig ar lefel y system os bydd y VPN yn torri. [5]

**6. CIPOLWG AR VPN**

Caiff pob ymholiad DNS ei ddatrys drwy weinyddion DNS preifat wedi'u hamgryptio. [7]

**7. MEWNWELEDIAD VPN**

Mae ExpressVPN wedi cyhoeddi mwy nag 20 o archwiliadau trydydd parti annibynnol. [1]

**8. MEWNWELEDIAD VPN**

Nid yw'r gwasanaeth yn cofnodi cyfeiriadau IP, hanes pori na metadata traffig.

**9. MEWNWELEDIAD VPN**

Cynhelir Perfect Forward Secrecy drwy gylchdroi allweddi sesiwn yn ddeinamig. [1]

**10. CIPOLWG AR VPN**

Mae protocol Lightway yn cefnogi haenau cludo UDP a TCP.

# 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] ExpressVPN. (n.d.). ExpressVPN Trust Center.
https://www.expressvpn.com/trust

[2] ExpressVPN. (n.d.). Lightway: A VPN Protocol by ExpressVPN.
https://www.expressvpn.com/lightway

[3] ExpressVPN. (2025). Lightway's Rust rewrite undergoes two security audits, by Cure53 and Praetorian.
https://www.expressvpn.com/blog/lightway-audits-cure53-praetorian/

[4] ExpressVPN. (n.d.). ExpressVPN TrustedServer Technology.
https://www.expressvpn.com/features/trustedserver

[5] ExpressVPN. (n.d.). VPN Kill Switch: What It Is & How ExpressVPN Keeps You Safe.
https://www.expressvpn.com/features/network-lock

[6] ExpressVPN. (n.d.). How Secure Is VPN Encryption?
https://www.expressvpn.com/what-is-vpn/vpn-encryption

[7] ExpressVPN. (n.d.). Get a VPN With Private DNS.
https://www.expressvpn.com/features/dns

[8] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[9] ExpressVPN. (n.d.). Lightway Rust Open Source Workspace [GitHub repository].
https://github.com/expressvpn/lightway

[10] Cure53. (2024). Audit-Report ExpressVPN Lightway Protocol 10.-11.2024.
https://cure53.de/pentest-report_expressvpn-lightway_2024.pdf

[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] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

## Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

**1 Cwestiwn 1** — **Ateb Cywir: A**

**NODYN ADDYSGU**

Beth yw protocol ffynhonnell agored pwrpasol ExpressVPN? → Lightway

**2 Cwestiwn 2** — **Ateb Cywir: A**

**NODYN ADDYSGU**

Pa dechnoleg gweinydd sy'n rhedeg mewn RAM anweddol yn unig? → TrustedServer

**3 Cwestiwn 3** — **Ateb Cywir: A**

**NODYN ADDYSGU**

Beth sy'n digwydd os bydd cysylltiad VPN yn gollwng yn annisgwyl? → A) Mae'r kill switch yn rhwystro traffig

**4 Cwestiwn 4** — **Ateb Cywir: A**

**NODYN ADDYSGU**

Ble mae ExpressVPN wedi'i gorffori i ddiogelu preifatrwydd? → Ynysoedd Virgin Prydeinig

**5 Cwestiwn 5** — **Ateb Cywir: A**

**NODYN ADDYSGU**

Pa seiffr amgryptio cymesur a ddefnyddir yn ddiofyn? → AES-256-GCM

## Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

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

**NODYN ADDYSGU**

Mae technoleg TrustedServer yn storio logiau'r gweinydd ar yriannau caled.

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

**NODYN ADDYSGU**

Mae ExpressVPN wedi bod drwy archwiliadau diogelwch trydydd parti. [1]

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

**NODYN ADDYSGU**

Mae protocol Lightway wedi'i adeiladu ar ben sylfaen cod OpenVPN.

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

**NODYN ADDYSGU**

Mae'r kill switch ymlaen yn ddiofyn ar apiau bwrdd gwaith.

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

**NODYN ADDYSGU**

Mae ExpressVPN yn gweithredu DNS preifat ar bob un o'i weinyddion.

# 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. LIGHTWAY | E 2. TRUSTED SERVER | F 3. CLOI | A 4. YNYSOEDD |
| H 5. AES-256 | D 6. WEDI'I ARCHWILIO | B 7. GOLLYNGIAD | C 8. DNS |

## PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

| | | | |
|---|---|---|---|
| 1 LIGHTWAY | 2 TRUSTED SERVER | 3 LOCK | 4 YNYSOEDD |
| 5 AES-256 | 6 ARCHWILIEDIG | | |

## PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

| | | | |
|---|---|---|---|
| 1 G – GOLLYNGIAD | 2 D – YNYSOEDD | 3 H – DNSPREIFAT | 4 A – LIGHTWAY |
| 5 C – LOCK | 6 E – AMGRYPTIOAES | 7 B – TRUSTEDSERVER | 8 F – ARCHWILIEDIG |

## NODIADAU TRAFOD I ATHRAWON

**Termau Allweddol:**
Gwiriwch fod myfyrwyr yn gallu esbonio LIGHTWAY, TRUSTED SERVER a CLOI 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.

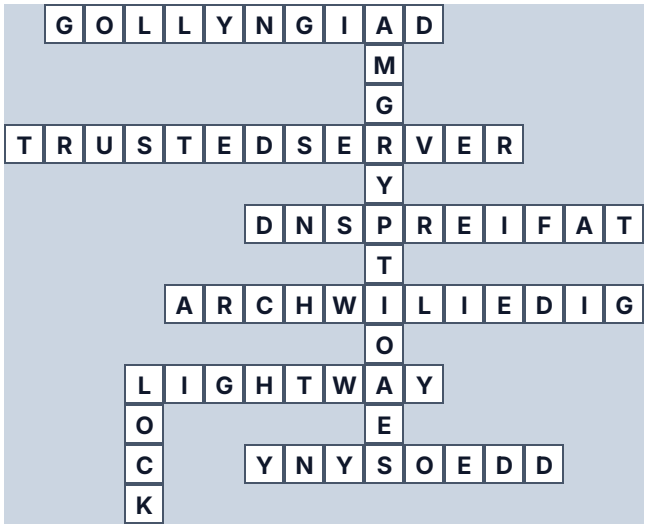
**Gwerthuso Ffynonellau:**
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

# Allweddi Posau a Nodiadau i Athrawon

## DATRYSIAD Y CHWILAIR

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

## DATRYSIAD Y CROESAIR




## CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

### CLIWIAU AR DRAWS

**1 ar draws: GOLLYNGIAD** Datgelu cyfeiriad IP, DNS neu ddata WebRTC preifat yn anfwriadol (10 llythyren)

**3 ar draws: TRUSTEDSERVER** Pensaernïaeth gweinyddion RAM yn unig sy'n atal storio data ar ddisg (13 llythyren)

**4 ar draws: DNSPREIFAT** Datryswyr System Enwau Parth a redir yn breifat ar bob nod gweinydd (10 llythyren)

**5 ar draws: ARCHWILIEDIG** Wedi'i ddilysu'n annibynnol gan gwmnïau diogelwch trydydd parti (12 llythyren)

**6 ar draws: LIGHTWAY** Protocol cysylltu ysgafn, cod agored ExpressVPN (8 llythyren)

**7 ar draws: YNYSOEDD** Awdurdodaeth y BVI (Virgin Prydeinig) sy'n cynnig preifatrwydd cryf (8 llythyren)

### CLIWIAU I LAWR

**2 i lawr: AMGRYPTIOAES** Safon gymesur sy'n diogelu data wrth ei drosglwyddo (12 llythyren)

**6 i lawr: LOCK** Gair olaf Network Lock, hen enw'r kill switch (4 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. AHTLWIYG — LIGHTWAY
2. LCKO — LOCK
3. AMITEOGPSYAR — AMGRYPTIOAES
4. NAYDLIGGOL — GOLLYNGIAD
5. EVRUSTRERDTES — TRUSTEDSERVER
6. DDSEYONY — YNYSOEDD
7. IEWARLGDICIH — ARCHWILIEDIG
8. APETDRNIFS — DNSPREIFAT

### ALLWEDD HER Y SEIFFR CYFRINACHOL

**"MAE TRUSTEDSERVER YN DILEU POB LOG BOB DYDD"**

# Allwedd Atebion yr Astudiaethau Achos

## A ASTUDIAETH ACHOS 1: GORFODI MESURAU DIOGELU RAM YN UNIG

Datrysiad i Athrawon

### CANLLAW MARCIO

**Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:**

- Dadansoddi Senario: Mae asiantaeth y llywodraeth yn atafaelu gweinydd ExpressVPN i dynnu logiau defnyddwyr a hanes cysylltu.
- Strategaeth ac Ateb a Argymhellir: Dim byd. Mae technoleg TrustedServer ExpressVPN yn rhedeg yn gyfan gwbl yn RAM, felly caiff yr holl ddata ei ddileu ar unwaith wrth golli pŵer.

## B ASTUDIAETH ACHOS 2: TWNELI CYSYLLTIAD WI-FI ANSEFYDLOG

Datrysiad i Athrawon

### CANLLAW MARCIO

**Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:**

- Dadansoddi Senario: Mae gweithiwr o bell yn defnyddio Wi-Fi cyhoeddus gwesty sy'n torri bob ychydig funudau wrth iddo olygu dogfennau.
- Strategaeth ac Ateb a Argymhellir: Mae Internet Kill Switch yn rhwystro'r holl draffig rhyngrwyd yn awtomatig nes bod y twnnel VPN wedi'i ailsefydlu.