Enw: _____ Dyddiad: _____ Sgôr: _____

Diogelwch ProtonVPN

Dadansoddi pensaernïaeth ddiogelwch ProtonVPN gan gynnwys gweinyddion Secure Core, hidlo DNS NetShield, awdurdodaeth preifatrwydd y Swistir, apiau ffynhonnell agored wedi'u harchwilio, a'r protocol Stealth.

TROSOLWG DYSGU DIOGELWCH PROTONVPN

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 Proton VPN. Byddwch yn archwilio gweinyddion hop dwbl Secure Core, rhwystro DNS NetShield, cyfreithiau preifatrwydd y Swistir, a chuddio Stealth.

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/protonvpn/diogelwch/

Eich Map Llwybr Dysgu Diogelwch ProtonVPN

- Dadansoddwch bensaernïaeth dechnegol a rheolau ffurfweddu Diogelwch ProtonVPN.
- 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 DIOGELWCH PROTONVPN

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 lwybro dwbl-naid Secure Core a llywodraethu preifatrwydd y Swistir. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

PENSAERNÏAETH DWBL-NAID SECURE CORE AC AWDURDODAETH PREIFATRWYDD Y SWISTIR

Mae Proton VPN yn amddiffyn traffig defnyddwyr gyda gweinyddion Secure Core sy'n eiddo i Proton yn y Swistir, Gwlad yr Iâ a Sweden, rhaglenni cod agored wedi'u harchwilio, a'r protocol cuddio Stealth a gynlluniwyd i osgoi archwilio pecynnau dwfn.

(CYFLWYNIAD)

Mae Proton VPN yn amddiffyn traffig defnyddwyr gyda gweinyddion Secure Core sy'n eiddo i Proton yn y Swistir, Gwlad yr Iâ a Sweden, rhaglenni cod agored wedi'u harchwilio, a'r protocol cuddio Stealth a gynlluniwyd i osgoi archwilio pecynnau dwfn.

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

Pwynt Gwirio 1: Her Amlddewis

1. 1. Pa fath o gyfleusterau sy'n gartref i weinyddion Secure Core Proton?
   - A) Peiriannau Rhithwir Cwmwl Cyhoeddus
   - B) Safleoedd Diogelwch Uchel
   - C) Canolfannau Data Cyhoeddus
   - D) Raciau a Rennir

2. 2. Pa brotocol sy'n helpu i osgoi sensoriaeth lem gan lywodraethau?
   - A) PPTP
   - B) Protocol Stealth
   - C) OpenVPN UDP
   - D) IKEv2

3. 3. Beth yw swyddogaeth nodwedd NetShield Proton VPN?
   - A) Speed Booster
   - B) Rhwystro Hysbysebion a Maleiswedd drwy DNS
   - C) Storio yn y Cwmwl
   - D) Anfon Porthladdoedd Ymlaen

4. 4. O dan gyfreithiau preifatrwydd pa wlad y mae Proton AG yn gweithredu?
   - A) Yr Unol Daleithiau
   - B) Y Deyrnas Unedig
   - C) Y Swistir
   - D) Panama

5. 5. Sut mae arbenigwyr yn dilysu rhaglenni cleient Proton VPN?
   - A) Cod Cyfrinachol
   - B) Archwiliadau Ffynhonnell Agored
   - C) Trwydded Berchnogol
   - D) Adolygiad gan y Llywodraeth

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae Secure Core yn llwybro traffig drwy wledydd sy'n ystyriol o breifatrwydd cyn gadael.

○ Gwir ○ Gau

7 Cwestiwn 7

7. Mae'r Swistir yn aelod o gynghrair gwyliadwriaeth cudd-wybodaeth y 14 Llygad.

○ Gwir ○ Gau

8 Cwestiwn 8

8. Mae NetShield yn rhwystro hysbysebion a pharthau maleisus yn uniongyrchol ar lefel DNS.

○ Gwir ○ Gau

9 Cwestiwn 9

9. Mae rhaglenni Proton VPN yn 100% cod agored ac wedi'u harchwilio'n gyhoeddus.

○ Gwir ○ Gau

10 Cwestiwn 10

10. Mae protocol Stealth yn defnyddio penynnau WireGuard safonol heb eu cuddio.

○ 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. Yr enw ar lwybro aml-naid drwy weinyddion sy'n eiddo i Proton mewn gwledydd sy'n gyfeillgar i breifatrwydd yw pensaernïaeth _____ .

2. Er mwyn trechu archwilio pecynnau dwfn a waliau tân rhwydwaith, mae defnyddwyr yn actifadu'r modd _____ .

3. Caiff parthau maleiswedd, tracwyr a sgriptiau hysbysebu eu hidlo gan DNS _____ .

4. Yn ôl Proton, nid oes rhaid iddo gadw logiau o weithgarwch defnyddwyr oherwydd y gyfraith berthnasol, sef _____ .

5. Os bydd twnnel y VPN yn datgysylltu'n annisgwyl, caiff traffig rhyngrwyd ei rwystro gan fesur diogelu'r _____ .

6. Mae ymchwilwyr diogelwch annibynnol yn dilysu cywirdeb y cleient am fod yr apiau wedi'u rhyddhau fel _____ .

BANC GEIRIAU GEIRFA

AES-GCM COD AGORED DEDDF SWISAIDD KILL SWITCH NETSHIELD SECURE CORE STEALTH WIREGUARD

Ysgrifennwch eich atebion yma:

1. **2.**

3. **4.**

5. **6.**

Pwynt Gwirio 4: Paru Cysyniadau VPN a Rhwydwaith

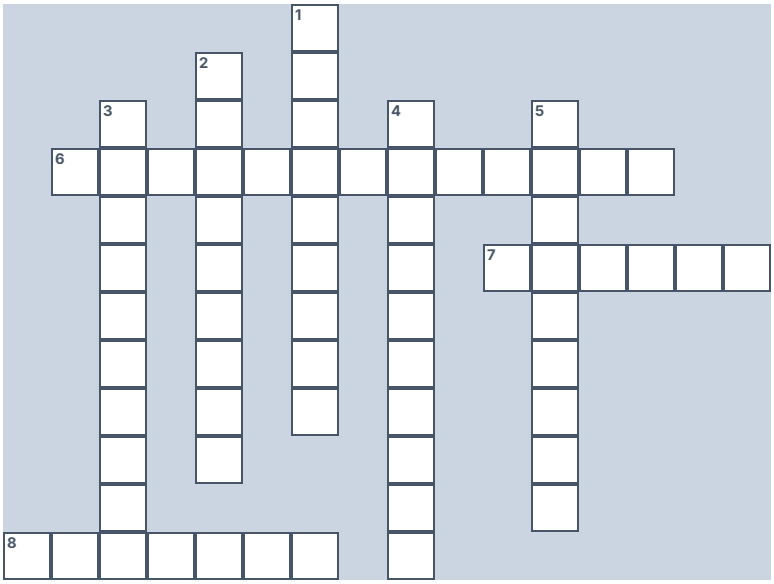
PARU DIFFINIADAU

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. SECURE CORE	A	Meddalwedd rhaglenni cleient sydd ar gael i'r cyhoedd ac wedi'i harchwilio'n annibynnol.
☐	2. PROTOCOL STEALTH	B	Safon seiffr cymesur sy'n amgryptio pecynnau data'r VPN.
☐	3. NETSHIELD	C	Statudau preifatrwydd cyfreithiol llym yn y Swistir y tu allan i awdurdodaeth y 14 Llygad.
☐	4. CYFREITHIAU'R SWISTIR	D	Protocol twnelu wedi'i guddio fel traffig gwe HTTPS safonol.
☐	5. KILL SWITCH	E	Protocol ysgafn modern sy'n darparu cryptograffeg gadarn a chyflymderau uchel.
☐	6. COD AGORED	F	Hidlydd seiliedig ar DNS sy'n blocio hysbysebion, tracwyr telemetreg a maleiswedd.
☐	7. WIREGUARD	G	Cynllun aml-naid sy'n llwybro traffig drwy weinyddion naid gyntaf sy'n eiddo i Proton.
☐	8. AES-GCM	H	Mesur diogelu sy'n atal trosglwyddo dros y rhwydwaith pan fydd y cysylltiad yn gollwng.

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

6. Statudau preifatrwydd cyfreithiol llym yn y Swistir, y tu allan i awdurdodaeth 14-Eyes (13)

7. Seiffr cymesur gradd filwrol sy'n diogelu pob pecyn data VPN wedi'i amgáu (6)

8. Protocol twnelu aneglur wedi'i guddio fel traffig gwe HTTPS safonol (7)

CLIWIAU I LAWR

1. Hidlydd ar sail DNS sy'n rhwystro hysbysebion, tracwyr telemetreg a maleiswedd (9)

2. Meddalwedd cleient sydd ar gael i'r cyhoedd ac wedi'i harchwilio'n annibynnol (9)

3. Cynllun aml-naid sy'n llwybro traffig drwy weinyddion naid gyntaf sy'n eiddo i Proton (10)

4. Mesur diogelwch sy'n atal trosglwyddo ar y rhwydwaith pan fydd y cysylltiad yn cwympo (10)

5. Protocol ysgafn modern sy'n darparu cryptograffeg gadarn a chyflymder uchel (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

6 ar draws: Statudau preifatrwydd cyfreithiol llym yn y Swistir, y tu allan i awdurdodaeth 14-Eyes (13 llythyren):

7 ar draws: Seiffr cymesur gradd filwrol sy'n diogelu pob pecyn data VPN wedi'i amgáu (6 llythyren):

8 ar draws: Protocol twnelu aneglur wedi'i guddio fel traffig gwe HTTPS safonol (7 llythyren):

CLIWIAU I LAWR

1 i lawr: Hidlydd ar sail DNS sy'n rhwystro hysbysebion, tracwyr telemetreg a maleiswedd (9 llythyren):

2 i lawr: Meddalwedd cleient sydd ar gael i'r cyhoedd ac wedi'i harchwilio'n annibynnol (9 llythyren):

3 i lawr: Cynllun aml-naid sy'n llwybro traffig drwy weinyddion naid gyntaf sy'n eiddo i Proton (10 llythyren):

4 i lawr: Mesur diogelwch sy'n atal trosglwyddo ar y rhwydwaith pan fydd y cysylltiad yn cwympo (10 llythyren):

5 i lawr: Protocol ysgafn modern sy'n darparu cryptograffeg gadarn a chyflymder uchel (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.

I D D R Q M E K I R Z S F Q V

F E A A Q O N I P T N X Q K R

E R U S D N Y L S T E A L T H

R O B F A S X L W J T A R Z Y

O G Y L E G I S M R S J M L T

C A O H S Q Q W H Z H A O V G

E D U B G Y R I Y B I H L Z G

R O J O C P N T W C E M Z Y G

U C Y O M W U C K V L P B N V

C T M G V D Y H U K D R B X Z

E D E D D F S W I S A I D D Y

S M R Q X I P D A D J Q V W W

L J W I R E G U A R D H T 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

RHESTR GEIRIAU GEIRFA

SECURECORE STEALTH NETSHIELD DEDDFSWISAIDD KILLSWITCH

CODAGORED WIREGUARD AESGCM

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. SECURECORE
B. STEALTH
C. NETSHIELD
D. DEDDFSWISAIDD
E. KILLSWITCH
F. CODAGORED
G. WIREGUARD
H. AESGCM

	DIFFINIADAU A MEYSYDD PARU
____	1. Protocol twnelu aneglur wedi'i guddio fel traffig gwe HTTPS safonol.
____	2. Protocol ysgafn modern sy'n darparu cryptograffeg gadarn a chyflymder uchel.
____	3. Statudau preifatrwydd cyfreithiol llym yn y Swistir, y tu allan i awdurdodaeth 14-Eyes.
____	4. Cynllun aml-naid sy'n llwybro traffig drwy weinyddion naid gyntaf sy'n eiddo i Proton.
____	5. Seiffr cymesur gradd filwrol sy'n diogelu pob pecyn data VPN wedi'i amgáu.
____	6. Mesur diogelwch sy'n atal trosglwyddo ar y rhwydwaith pan fydd y cysylltiad yn cwympo.
____	7. Hidlydd ar sail DNS sy'n rhwystro hysbysebion, tracwyr telemetreg a maleiswedd.
____	8. Meddalwedd cleient sydd ar gael i'r cyhoedd ac wedi'i harchwilio'n 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. **RCERESOEUC** _____
2. **DNLSEIEHT** _____
3. **KWCIISHLTL** _____
4. **GDREAUWIR** _____
5. **LHAESTT** _____
6. **FAWSIDDSDEIDD** _____
7. **OCEDRAOGD** _____
8. **SMACGE** _____

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Pethau rydych chi'n eu gwneud ar-lein bob dydd			
2	Gwledydd sy'n adnabyddus am gyfreithiau preifatrwydd cryf			
3	Nodweddion diogelwch yn Proton VPN			
4	Mathau o ollyngiadau VPN			
5	Sefyllfaoedd lle mae kill switch yn helpu			
6	Pethau y gall archwiliad eu gwirio			
7	Gosodiadau rydych chi'n eu troi ymlaen er mwyn diogelwch ychwanegol			
8	Pethau y mae amgryptio yn eu diogelu			
9	Geiriau sy'n disgrifio ap VPN da			
10	Rhesymau dros ddewis Proton VPN			
11	Botymau neu ddewislenni mewn ap VPN			
12	Gwasanaethau ffrydio rydych chi'n eu gwylio			
13	Bygythiadau ar Wi-Fi cyhoeddus			
14	Ffyrdd o greu cyfrinair cryf			
15	Gwledydd lle byddech chi eisiau gweinyddion Proton VPN			

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: OSGOI WALIAU TÂN CYFYNGOL

👷

Senario: Mae defnyddiwr yn teithio i wlad lle mae traffig VPN safonol fel OpenVPN a WireGuard yn cael ei rwystro gan DPI.

Cwestiwn Trafod: Pa ffurfweddiad protocol Proton VPN sy'n caniatáu i'r defnyddiwr osgoi archwiliad ar lefel y wladwriaeth?

ASTUDIAETH ACHOS 2: DIOGELU RHAG GWRTHWYNEBWYR SOFFISTIGEDIG

👷

Senario: Mae archwilydd ariannol yn amau y gallai nod allanfa ei ISP lleol gael ei beryglu gan fygythiadau parhaus datblygedig.

Cwestiwn Trafod: Sut mae Secure Core yn diogelu hunaniaeth yr archwilydd os caiff nod allanfa ei beryglu?

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

19 5 3 21 18 5 3 15 18 5 25 14

4 9 15 7 5 12 21 4 1 20 1

4 5 6 14 25 4 4 23 25 18

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: Beth yw Proton VPN Secure Core?

Mae Secure Core yn llwybro traffig drwy weinyddion lluosog mewn gwledydd sy'n ystyriol o breifatrwydd cyn gadael.

Q2: Beth yw'r protocol Stealth?

Protocol wedi'i guddio yw Stealth sy'n cuddio cysylltiadau VPN fel traffig TLS/HTTPS rheolaidd.

Q3: Sut mae NetShield yn diogelu defnyddwyr?

Mae NetShield yn offeryn seiliedig ar DNS sy'n rhwystro hysbysebion, tracwyr a pharthau maleiswedd yn awtomatig.

Q4: A yw Proton VPN wedi'i ddiogelu'n gyfreithiol yn y Swistir?

Ydy, mae gan y Swistir gyfreithiau preifatrwydd llym ac mae y tu allan i awdurdodaeth yr UD a'r UE/14-Eyes. [4]

Q5: A yw apiau Proton VPN yn god agored?

Ie. Mae apiau Proton VPN yn ffynhonnell agored ac wedi bod drwy archwiliadau diogelwch cyhoeddedig.

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: Pa seiffrau amgryptio sy'n cael eu defnyddio?

Mae Proton VPN yn defnyddio AES-256-GCM neu ChaCha20-Poly1305 gydag ysgwyd llaw HMAC-SHA384 ac RSA-4096.

Q7: A oes gan Proton VPN Kill Switch?

Ydy, mae Proton VPN yn cynnwys Kill Switch safonol a Kill Switch Parhaol i atal gollyngiadau heb eu hamgryptio.

Q8: A all Proton VPN ollwng ymholiadau DNS?

Na, mae pob ymholiad DNS yn cael ei lwybro drwy weinyddion DNS preifat wedi'u hamgryptio sy'n eiddo i Proton.

Q9: A yw Proton VPN yn cadw logiau cysylltu?

Na, mae Proton VPN yn cadw polisi dim logiau llym, wedi'i gadarnhau gan archwiliadau blynyddol Securitum. [3]

Q10: A yw Proton VPN yn agored i ollyngiadau WebRTC?

Na, mae cleientiaid Proton yn cynnwys rheolau wal dân a pholisïau llwybro adeiledig sy'n rhwystro gollyngiadau WebRTC.

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: Ble mae canolfannau data Secure Core wedi'u lleoli'n ffisegol?

Maent yn y Swistir, mewn hen ganolfan filwrol yng Ngwlad yr Iâ, ac mewn safle tanddaearol yn Sweden. [1]

Q2: Sut mae Perfect Forward Secrecy yn gweithredu yn Proton VPN?

Cynhyrchir allwedd amgryptio dros dro unigryw ar gyfer pob sesiwn, gan atal dadgryptio ôl-weithredol.

Q3: Beth yw Permanent Kill Switch ar Windows/Linux?

Mae Kill Switch Parhaol yn rhwystro pob traffig rhwydwaith hyd yn oed os yw'r ap VPN wedi'i gau'n llwyr neu'n chwalu.

Q4: A yw Proton VPN yn cefnogi llwybro IPv6 ac amddiffyn rhag gollyngiadau?

Mae Proton VPN yn llwybro traffig IPv6 yn llawn drwy dwneli neu'n ei analluogi'n ddiogel i atal gollyngiadau.

Q5: Sut mae hidlo DNS NetShield yn ymdrin ag archwilio HTTPS?

Mae NetShield yn gweithredu ar yr haen datrys DNS yn unig heb fod angen dadgryptio TLS ymwthiol.

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: Pwy gynhaliodd archwiliadau cod trydydd parti Proton VPN?

Archwiliodd SEC Consult yr apiau, ac mae Securitum yn archwilio'r apiau a'r polisi dim logiau.

Q7: Sut mae'r protocol Stealth yn cymharu ag OpenVPN XOR neu Shadowsocks?

Mae Stealth yn twnelu WireGuard dros TLS wedi'i guddio ac yn perfformio'n well na chuddio hŷn sy'n seiliedig ar OpenVPN. [5]

Q8: A all awdurdodau'r Swistir orfodi Proton VPN i gofnodi traffig?

Mae Proton yn datgan nad yw o dan rwymedigaeth o dan gyfraith y Swistir i gadw logiau o weithgarwch na data defnyddwyr.

Q9: Sut mae gweinyddion Proton VPN yn cael eu diogelu rhag eu hatafaelu?

Mae holl weinyddion Proton VPN yn beiriannau metel noeth wedi'u diogelu ag amgryptio disg llawn. [2]

Q10: A yw Proton VPN yn cefnogi ffurfweddiadau gweinydd DNS personol?

Ie, gall tanysgrifwyr taledig ffurfweddu gweinyddion DNS i fyny'r llif personol yn uniongyrchol yn newisiadau'r ap.

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

1. Mae Proton yn berchen ar ei weinyddion Secure Core ac yn eu gosod ei hun, mewn safleoedd diogelwch uchel yn y Swistir, Gwlad yr Iâ a Sweden. [1]

2. CIPOLWG AR VPN

2. Mae apiau cleient Proton VPN yn ffynhonnell agored ac yn cael archwiliadau cod cylchol gan drydydd parti.

3. CIPOLWG AR VPN

3. Mae protocol cuddio Stealth yn osgoi Archwilio Pecynnau Dwfn drwy efelychu traffig TLS safonol.

4. CIPOLWG AR VPN

4. Mae'r Swistir y tu allan i gynghreiriau rhannu cudd-wybodaeth rhyngwladol 5-Eyes, 9- Eyes a 14-Eyes. [4]

5. CIPOLWG AR VPN

5. Mae NetShield yn gweithredu ar lefel y datryswr DNS, gan atal hysbysebion a maleiswedd cyn lawrlwytho'r llwyth.

6. CIPOLWG AR VPN

6. Mae Perfect Forward Secrecy yn sicrhau na all allweddi sydd wedi'u peryglu ddadgryptio sesiynau traffig a ddaliwyd yn flaenorol. [7]

7. MEWNWELEDIAD VPN

7. Mae Proton VPN yn defnyddio amgryptio disg llawn ar weinyddion metel noeth i ddiogelu ffurfweddiadau gweinyddion. [2]

8. MEWNWELEDIAD VPN

8. Mae'r Kill Switch Parhaol yn atal gollyngiadau data heb ei amgryptio hyd yn oed wrth ailgychwyn y system weithredu.

9. MEWNWELEDIAD VPN

9. Mae Securitum wedi archwilio a chadarnhau polisi dim logiau Proton VPN mewn pum archwiliad blynyddol olynol. [3]

10. CIPOLWG AR VPN

10. Datblygwyd Proton VPN gan wyddonwyr a gyfarfu yn CERN (Sefydliad Ewropeaidd ar gyfer Ymchwil Niwclear). [4]

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] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Cwestiwn 1** **Ateb Cywir: B**

NODYN ADDYSGU

Mae gweinyddion Secure Core mewn safleoedd diogelwch uchel, gan gynnwys hen ganolfan filwrol yng Ngwlad yr Iâ a chanolfan ddata danddaearol yn Sweden.

2 **Protocol Cuddio Llechwraidd** AMDDIFFYN RHAG SENSORIAETH **Ateb Cywir: B**

NODYN ADDYSGU

Mae protocol Stealth Proton yn cuddio cysylltiadau WireGuard fel traffig TLS/HTTPS safonol i osgoi waliau tân Archwilio Pecynnau Dwfn (DPI). Ffynhonnell: Proton Stealth Protocol Whitepaper.

3 **Atalydd Hysbysebion DNS NetShield** HIDLO DNS **Ateb Cywir: B**

NODYN ADDYSGU

Mae NetShield yn defnyddio hidlo ar lefel DNS i rwystro parthau maleiswedd, ysbïwedd, hysbysebu ymwthiol a thracwyr telemetreg cyn i dudalennau gwe lwytho. Ffynhonnell: NetShield Security Specs.

4 **Awdurdodaeth Gyfreithiol y Swistir** AWDURDODAETH **Ateb Cywir: C**

NODYN ADDYSGU

Mae pencadlys Proton AG yn Genefa, y Swistir, gan elwa ar gyfreithiau preifatrwydd cryf y Swistir y tu allan i gynghreiriau gwyliadwriaeth 14-Eyes yr Unol Daleithiau a'r UE. Ffynhonnell: Swiss Federal Data Protection Act. [4]

5 **Cwestiwn 5** **Ateb Cywir: B**

NODYN ADDYSGU

Mae holl apiau Proton VPN yn god agored; mae SEC Consult ac yn ddiweddarach Securitum wedi'u harchwilio.

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Secure Core Aml-Awdurdodaeth** PENSAERNÏAETH LLWYBRO **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae Secure Core yn llwybro traffig drwy awdurdodaethau â phreifatrwydd cadarn cyn gadael i'r wlad gyrchfan, gan helpu i amddiffyn rhag gweinydd allanfa sydd wedi'i beryglu. Ffynhonnell: Secure Core Architecture.

7 **Cynghrair Gwyliadwriaeth y Swistir** CYNGHREIRIAU GWYLIADWRIAETH **Ateb Cywir: Gau**

NODYN ADDYSGU

Nid yw'r Swistir yn aelod o gytundebau rhannu cudd-wybodaeth y 5 Llygad, y 9 Llygad na'r 14 Llygad, gan gadw sofraniaeth gyfreithiol annibynnol. Ffynhonnell: International Surveillance Treaties.

8 **Cwestiwn 8** **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae NetShield yn defnyddio gweinyddion DNS Proton i wirio parthau yn erbyn rhestrau o barthau hysbysebion, tracwyr a maleiswedd hysbys.

9 **Archwilio Cleientiaid Cod Agored** TRYLOYWDER DIOGELWCH **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae Proton wedi gwneud ei apiau bwrdd gwaith a symudol yn god agored ac mae'n cyhoeddi adroddiadau archwilio trydydd parti. Ffynhonnell: SEC Consult Security Report.

10 **Cwestiwn 10** **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae Stealth yn twnelu WireGuard y tu mewn i TLS aneglur dros TCP fel bod y traffig yn edrych fel HTTPS cyffredin.

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. SECURE CORE	D 2. PROTOCOL STEALTH	F 3. NETSHIELD	C 4. CYFREITHIAU'R SWISTIR
H 5. KILL SWITCH	A 6. COD AGORED	E 7. WIREGUARD	B 8. AES-GCM

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 DEDDF SWISAIDD
5 KILL SWITCH	6 COD AGORED		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 B – STEALTH	2 G – WIREGUARD	3 D – DEDDFSWISAIDD	4 A – SECURECORE
5 H – AESGCM	6 E – KILLSWITCH	7 C – NETSHIELD	8 F – CODAGORED

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio SECURE CORE, PROTOCOL STEALTH a NETSHIELD 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.

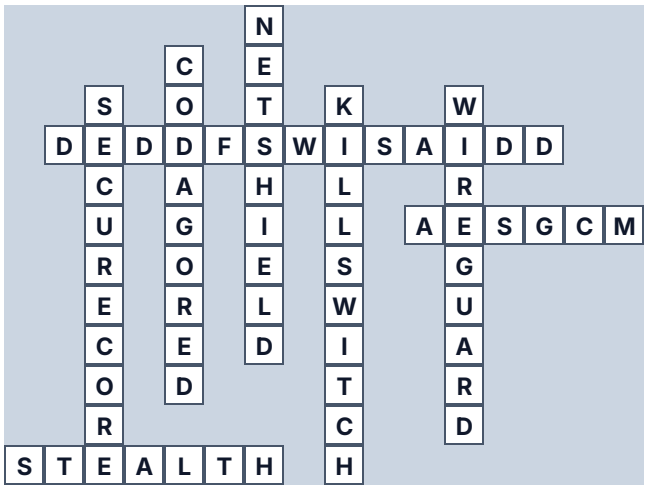
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

6 ar draws: DEDDFSWISAIDD Statudau preifatrwydd cyfreithiol llym yn y Swistir, y tu allan i awdurdodaeth 14-Eyes (13 llythyren)

7 ar draws: AESGCM Seiffr cymesur gradd filwrol sy'n diogelu pob pecyn data VPN wedi'i amgáu (6 llythyren)

8 ar draws: STEALTH Protocol twnelu aneglur wedi'i guddio fel traffig gwe HTTPS safonol (7 llythyren)

CLIWIAU I LAWR

1 i lawr: NETSHIELD Hidlydd ar sail DNS sy'n rhwystro hysbysebion, tracwyr telemetreg a maleiswedd (9 llythyren)

2 i lawr: CODAGORED Meddalwedd cleient sydd ar gael i'r cyhoedd ac wedi'i harchwilio'n annibynnol (9 llythyren)

3 i lawr: SECURECORE Cynllun aml-naid sy'n llwybro traffig drwy weinyddion naid gyntaf sy'n eiddo i Proton (10 llythyren)

4 i lawr: KILLSWITCH Mesur diogelwch sy'n atal trosglwyddo ar y rhwydwaith pan fydd y cysylltiad yn cwympo (10 llythyren)

5 i lawr: WIREGUARD Protocol ysgafn modern sy'n darparu cryptograffeg gadarn a chyflymder uchel (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.	RCERESOEUC	SECURECORE	5.	LHAESTT	STEALTH
2.	DNLSEIEHT	NETSHIELD	6.	FAWSIDDSDEIDD	DEDDFSWISAIDD
3.	KWCIISHLTL	KILLSWITCH	7.	OCEDRAOGD	CODAGORED
4.	GDREAUWIR	WIREGUARD	8.	SMACGE	AESGCM

ALLWEDD HER Y SEIFFR CYFRINACHOL

"SECURE CORE YN DIOGELU DATA DEFNYDDWYR"

Allwedd Atebion yr Astudiaethau Achos

A ASTUDIAETH ACHOS 1: OSGOI WALIAU TÂN CYFYNGOL

Datrysiad i Athrawon

CYNLLUN MARCIO A CHANLLAWIAU DATRYSIADAU

- Dadansoddi Senario: Mae defnyddiwr yn teithio i wlad lle mae traffig VPN safonol fel OpenVPN a WireGuard yn cael ei rwystro gan DPI.
- Cwestiwn Ffocws: Pa ffurfweddiad protocol Proton VPN sy'n galluogi'r defnyddiwr i osgoi archwilio ar lefel y wladwriaeth?
- Strategaeth ac Ateb a Argymhellir: Dylai'r defnyddiwr actifadu'r protocol Stealth, sy'n cuddio penawdau pecynnau VPN fel traffig gwe TLS/HTTPS arferol, gan lithro heibio i hidlwyr DPI.

B ASTUDIAETH ACHOS 2: DIOGELU RHAG GWRTHWYNEBWYR SOFFISTIGEDIG

Datrysiad i Athrawon

CYNLLUN MARCIO A CHANLLAWIAU DATRYSIADAU

- Dadansoddi Senario: Mae archwilydd ariannol yn amau y gallai nod allanfa ei ddarparwr gwasanaeth rhyngrwyd lleol fod wedi'i gyfaddawdu gan fygythiadau parhaus datblygedig.
- Cwestiwn Ffocws: Sut mae Secure Core yn diogelu hunaniaeth yr archwilydd rhag i nod gadael gael ei gyfaddawdu?
- Strategaeth ac Ateb a Argymhellir: Mae Secure Core yn llwybro traffig yn gyntaf drwy weinyddion sy'n eiddo i Proton yn y Swistir, Gwlad yr Iâ neu Sweden, felly ni all gweinydd allanfa sydd wedi'i gyfaddawdu olrhain IP y defnyddiwr.