Enw: _____ Dyddiad: _____ Sgôr: _____

Beth yw VPN Taflen Waith

Ymarferion ymarferol ar brotocolau rhwydwaith, twnelu a rheolaethau diogelwch.

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

- Esbonio'r cysyniad o dwnelu data a chrynhoi (encapsulation).
- Nodwch ffurfweddiadau protocol safonol a dulliau amgryptio.
- Dadansoddwch rolau gweinyddion a chuddio IP mewn rhwydweithiau preifat rhithwir.
- Deall sut mae ISPs yn olrhain pori a sut mae VPN yn atal hynny.
- Gwahaniaethwch ffiniau gweithredol topoleg rhwydwaith rhithwir.

CYFARWYDDIADAU CANLLAW BETH YW VPN

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 senarios go iawn yn yr adran astudiaethau achos. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

BETH YW VPN? (CYFLWYNIAD)

Mae Rhwydwaith Preifat Rhithwir yn fwy na dim ond switsh preifatrwydd. Mae'n dwnnel wedi'i amgryptio sy'n llwybro eich traffig rhyngrwyd drwy weinydd pell. Mae hyn yn cuddio eich cyfeiriad IP, yn atal eich ISP rhag casglu logiau o'ch gweithredoedd ar-lein, ac yn diogelu eich data ar rwydweithiau cyhoeddus. Mae deall y derminoleg yn hanfodol er mwyn cynnal diogelwch digidol.

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

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw prif swyddogaeth Rhwydwaith Preifat Rhithwir (VPN)?**
   - A. I gynyddu cyflymder rendro'r porwr rhyngrwyd
   - B. Amgryptio pecynnau data a chuddio eich IP cyhoeddus
   - C. Er mwyn storio cronfeydd data cwcis gwefannau yn lleol
   - D. Er mwyn disodli caledwedd ffisegol eich cyfrifiadur

2. **2. Beth yw twnelu rhwydwaith yng nghyd-destun VPN?**
   - A. Dileu ffeiliau log rhwydwaith dyblyg
   - B. Gosod ffeiliau storio cronfa ddata lleol
   - C. Rhannu ffeiliau â chyfrifiaduron lleol eraill
   - D. Amgáu un pecyn rhwydwaith y tu mewn i becyn diogel arall

3. **3. Pa safon amgryptio a ddefnyddir yn eang i ddiogelu traffig VPN?**
   - A. Amgryptio DES etifeddol
   - B. Safon AES-256 fodern
   - C. Amgodio base64 testun plaen
   - D. Seiffro rot13 safonol

4. **4. Pa elfen o draffig eich rhwydwaith sy'n cael ei hamgryptio gan VPN?**
   - A. Tasgau argraffu rhwydwaith dyfeisiau lleol yn unig
   - B. Llwybr ffisegol y cebl ether-rwyd
   - C. Holl ran llwyth data'r pecyn rhwydwaith
   - D. Dim ond hanes chwilio eich porwr gwe

5. **5. Beth yw ystyr y term 'amgryptio' mewn rhwydweithio?**
   - A. Trosi data testun plaen yn destun seiffr annarllenadwy
   - B. Dileu hen gofnodion cyfathrebu
   - C. Cynyddu terfynau cyflymder eich lled band lleol
   - D. Rhannu allweddi mynediad cronfa ddata yn gyhoeddus

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae VPN yn amgryptio eich traffig i atal clustfeinio lleol ar Wi-Fi cyhoeddus.

Gwir Gau

7 Cwestiwn 7

7. Mae VPN yn newid ffurfweddiad caledwedd eich dyfais llwybrydd yn ffisegol.

Gwir Gau

8 Cwestiwn 8

8. Mae protocolau twnelu yn lapio pecynnau data mewn haen gludo wedi'i hamgryptio.

Gwir Gau

9 Cwestiwn 9

9. Mae amgryptio cymesur yn defnyddio'r un allwedd i amgryptio a dadgryptio traffig.

Gwir Gau

10 Cwestiwn 10

10. Mae defnyddio VPN yn gwneud eich cysylltiad rhyngrwyd yn ffisegol imiwn i unrhyw doriadau pŵer all-lein.

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. Er mwyn diogelu eich traffig, mae'r VPN yn lapio eich pecynnau data y tu mewn i brotocol arall, sef proses o'r enw _____ .

2. Os yw cyflymder lawrlwytho'n araf wrth ffrydio, gallai hynny fod oherwydd _____ rhwydwaith cyfyngedig.

3. Mae gwasanaeth ffrydio sydd ar gael mewn gwlad benodol yn unig yn defnyddio _____ i gyfyngu ar ddefnyddwyr byd-eang.

4. Yr enw ar y rheolau cysylltu sy'n diffinio'r paramedrau amgryptio a chysylltu yw _____ y VPN.

5. Mae eich cyfrifiadur yn defnyddio _____ leol i fonitro traffig rhwydwaith a rhwystro cysylltiadau anniogel.

6. Pan fyddwch yn cysylltu â VPN, caiff eich data ei lwybro drwy gyfrwng _____ pell i guddio eich IP cyhoeddus.

BANC GEIRIAU GEIRFA

GEO-FLOCIO GWEINYDD ISP LLED BAND PREIFATRWYDD PROTOCOL TWNELU WAL DÂN

Ysgrifennwch eich atebion yma:

1. **2.**

3. **4.**

5. **6.**

Pwynt Gwirio 4: Paru Cysyniadau Rhwydwaith

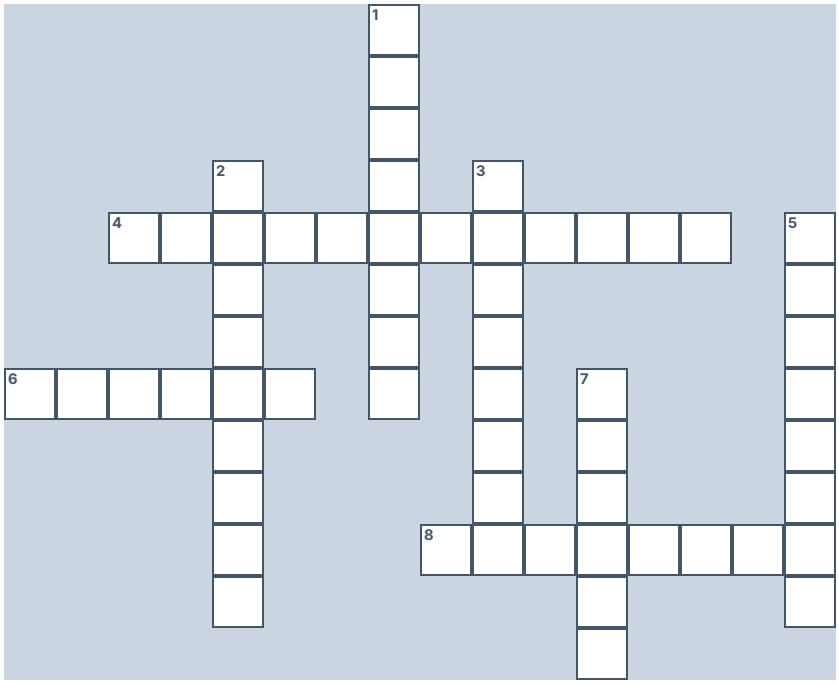
PARU DIFFINIADAU

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. Twnelu	A	Cyfrifiadur pell sy'n llwybro eich traffig ac yn cuddio eich IP.
	2. Protocol	B	Darparwr Gwasanaeth Rhyngrwyd sy'n cludo eich traffig ac sy'n gallu gweld gweithgarwch heb ei amgryptio.
	3. Lled Band	C	Cyfyngiad sy'n atal mynediad i'r we yn seiliedig ar leoliad ffisegol.
	4. Gweinydd	D	System ddiogelwch sy'n monitro ac yn blocio traffig heb awdurdod.
	5. GEO-FLOCIO	E	Set o reolau sy'n pennu sut y caiff data ei drosglwyddo dros y rhwydwaith.
	6. Wal dân	F	Y cyflwr o fod yn rhydd rhag olrhain neu wyliadwriaeth gyhoeddus.
	7. Preifatrwydd	G	Y gyfradd uchaf o drosglwyddo data ar draws cysylltiad.
	8. ISP	H	Lapio pecynnau data y tu mewn i becyn arall ar gyfer cludo diogel.

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

4. Y cyflwr o fod yn rhydd rhag cael eich tracio neu rhag gwyliadwriaeth gyhoeddus (12)

6. Lapio pecynnau data y tu mewn i becyn arall er mwyn eu cludo'n ddiogel (6)

8. Y gyfradd uchaf o drosglwyddo data ar draws cysylltiad (8)

CLIWIAU I LAWR

1. Y cwmni gwasanaeth rhyngrwyd (ISP), sy'n logio eich traffig oni bai ei fod wedi'i amgryptio (8)

2. Cyfyngiad sy'n atal mynediad i'r we yn seiliedig ar leoliad ffisegol (9)

3. Set o reolau sy'n pennu sut caiff data ei drosglwyddo dros y rhwydwaith (8)

5. Cyfrifiadur pell sy'n llwybro eich traffig ac yn cuddio eich IP (8)

7. System ddiogelwch sy'n monitro ac yn rhwystro traffig heb awdurdod (6)

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

4 ar draws: Y cyflwr o fod yn rhydd rhag cael eich tracio neu rhag gwyliadwriaeth gyhoeddus (12 llythyren):

6 ar draws: Lapio pecynnau data y tu mewn i becyn arall er mwyn eu cludo'n ddiogel (6 llythyren):

8 ar draws: Y gyfradd uchaf o drosglwyddo data ar draws cysylltiad (8 llythyren):

CLIWIAU I LAWR

1 i lawr: Y cwmni gwasanaeth rhyngrwyd (ISP), sy'n logio eich traffig oni bai ei fod wedi'i amgryptio (8 llythyren):

2 i lawr: Cyfyngiad sy'n atal mynediad i'r we yn seiliedig ar leoliad ffisegol (9 llythyren):

3 i lawr: Set o reolau sy'n pennu sut caiff data ei drosglwyddo dros y rhwydwaith (8 llythyren):

5 i lawr: Cyfrifiadur pell sy'n llwybro eich traffig ac yn cuddio eich IP (8 llythyren):

7 i lawr: System ddiogelwch sy'n monitro ac yn rhwystro traffig heb awdurdod (6 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.

T W N E L U S L Z V C Z W F K

H R Z D N D Q L X P G C U B A

Z W N D K A D E O D W F H I D

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

I A F A A Q O B N P I T X P Q

C P K R U S D A N Y N B F R S

O R X W J A R N Z Y Y Y L O G

L A I M R J M D L T D O H T Q

F D Q H Z A O V G U D B Y O R

O Y B H L Z G J O P N W C C M

E P R E I F A T R W Y D D O Z

G Y G Y O W U K V P B N V L T

M G W A L D A N V D Y U K R B

X Z Y M R Q X I P D A D J Q V

W W L J H T H G B E I K T S V

RHESTR GEIRIAU GEIRFA

TWNELU PROTOCOL LLEDBAND GWEINYDD GEOFLOCIO WALDAN PREIFATRWYDD DARPARWR

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. TWNELU
B. PROTOCOL
C. LLEDBAND
D. GWEINYDD
E. GEOFLOCIO
F. WALDAN
G. PREIFATRWYDD
H. DARPARWR

DIFFINIADAU A MEYSYDD PARU

_____ 1. Set o reolau sy'n pennu sut caiff data ei drosglwyddo dros y rhwydwaith.

_____ 2. Cyfyngiad sy'n atal mynediad i'r we yn seiliedig ar leoliad ffisegol.

_____ 3. System ddiogelwch sy'n monitro ac yn rhwystro traffig heb awdurdod.

_____ 4. Y cyflwr o fod yn rhydd rhag cael eich tracio neu rhag gwyliadwriaeth gyhoeddus.

_____ 5. Y cwmni gwasanaeth rhyngrwyd (ISP), sy'n logio eich traffig oni bai ei fod wedi'i amgryptio.

_____ 6. Lapio pecynnau data y tu mewn i becyn arall er mwyn eu cludo'n ddiogel.

_____ 7. Cyfrifiadur pell sy'n llwybro eich traffig ac yn cuddio eich IP.

_____ 8. Y gyfradd uchaf o drosglwyddo data ar draws cysylltiad.

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. **NTELUW** _____

2. **DLDLNABE** _____

3. **GOLECOFIO** _____

4. **DRFETDAYWPRI** _____

5. **OCRLTPOO** _____

6. **DDIYGNWE** _____

7. **AWDNLA** _____

8. **PAARDWRR** _____

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Pethau y gall cyfeiriad IP eu datgelu			
2	Mythau am VPNs			
3	Pethau sy'n teithio ar draws y rhyngrwyd			
4	Addewidion y mae darparwr VPN da yn eu gwneud			
5	Cyfrinachau y byddech chi'n eu hamgryptio			
6	Pethau na all VPN eich diogelu rhagddynt			
7	Ffyrdd o adnabod rhwydwaith Wi-Fi ffug			
8	Geiriau sy'n ymwneud â phreifatrwydd			
9	Dyfeisiau sy'n gallu defnyddio VPN			
10	Pethau sy'n digwydd pan fyddwch chi'n pwyso 'Cysylltu'			
11	Mannau lle byddech chi'n defnyddio VPN			
12	Rhesymau dros ddefnyddio VPN wrth deithio			
13	Pethau go iawn sy'n edrych fel twnnel			
14	Geiriau o'r daflen waith hon rydych chi am eu cofio			
15	Geiriau i esbonio VPN i blentyn			

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'n eistedd yn Coffee & Bytes. Mae rhwydwaith cyhoeddus heb ei ddiogelu o'r enw 'Free_Wi-Fi_No_Password'. Rwyf eisiau mewngofnodi i'm e-bost ysgol a lanlwytho fy aseiniad, ond rwy'n poeni am hacwyr. Beth yw'r risgiau o ddefnyddio'r rhwydwaith hwn heb VPN, a sut mae VPN yn diogelu fy nata?"

ALEX (MYFYRIWR SY'N TEITHIO)

👩‍💻 "O na! Rwy'n teithio dramor ar gyfer prosiect ac yn ceisio gwylio rhaglen ddogfen bioleg sy'n cael ei chynnal ar weinydd yn fy ngwlad gartref. Ond mae'r wefan yn dweud 'Nid yw'r fideo hwn ar gael yn eich lleoliad presennol.' Pam rwy wedi fy rhwystro, a sut gall VPN fy helpu i'w gwylio?"

Pwynt Gwirio 9: Dadgryptio'r Seiffr

Mae VPN yn amgryptio eich traffig i'w ddiogelu. Defnyddiwch yr allwedd Llythyren-i-Rif isod i ddadgryptio'r neges seiberddiogelwch 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

4 9 15 7 5 12 23 3 8 5 9 3 8

16 18 5 9 6 1 20 18 23 25 4 4 7 25 4 1

20 8 23 14 14 5 12 4 9 15 7 5 12

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 dylwn i ddefnyddio VPN?

Mae VPN yn diogelu eich preifatrwydd digidol, yn sicrhau eich cysylltiad ar rwydweithiau Wi-Fi cyhoeddus (fel siopau coffi neu feysydd awyr), gall leihau arafu bwriadol ar sail gweithgarwch pan na all yr ISP adnabod y math o draffig wedi'i amgryptio, yn osgoi cyfyngiadau daearyddol i gyrchu cynnwys byd-eang, ac yn helpu i ddiogelu adnoddau gweithio o bell.

Q3: A yw VPN yn fy ngwneud yn gwbl ddienw ar-lein?

Na. Er bod VPN yn cuddio eich cyfeiriad IP ac yn amgryptio traffig, gallwch gael eich olrhain o hyd drwy gwcis porwr, cyfrifon gweithredol (fel Google neu Facebook), olion bysedd porwr, neu os yw eich darparwr VPN yn logio eich data.

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 defnyddio VPN yn gyfreithlon?

Mae defnyddio VPN yn gyfreithlon mewn llawer o wledydd, ond mae rhai awdurdodaethau'n cyfyngu ar wasanaethau VPN, yn eu rheoleiddio neu'n eu rhwystro. Dylai defnyddwyr wirio'r cyfreithiau lleol cyfredol cyn eu defnyddio. Am ragor o fanylion, edrychwch ar y canllawiau cyfreithlondeb ar VPN.com.

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: A allaf ddefnyddio VPN am ddim?

Gall VPNs am ddim ddibynnu ar hysbysebu, nodweddion cyfyngedig, dadansoddeg defnydd, capiau data, neu fodelau gwneud arian eraill. Dylai defnyddwyr adolygu polisi preifatrwydd, perchnogaeth, archwiliadau a model busnes y darparwr cyn eu defnyddio.

Q7: Beth yw polisi "dim logiau"?

Mae polisi dim logiau yn disgrifio pa ddata gweithgarwch a chysylltu y mae darparwr yn dweud nad yw'n ei gadw. Mae'r union gwmpas yn amrywio, felly dylai darllenwyr adolygu'r polisi a chanfyddiadau archwiliadau annibynnol.

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 VPN ar fy ffôn a fy nheledu clyfar?

Ie. Mae darparwyr VPN modern yn cynnig apiau pwrpasol ar gyfer iOS, Android, macOS, Windows, Linux a setiau teledu clyfar, yn ogystal â gosodiadau llwybrydd i ddiogelu pob dyfais ar eich rhwydwaith cartref.

Q10: Beth yw Kill Switch?

Nodwedd ddiogelwch yw Kill Switch sy'n datgysylltu eich dyfais o'r rhyngrwyd yn awtomatig os bydd cysylltiad y VPN yn gollwng. Mae hyn yn atal eich data heb ei amgryptio neu eich cyfeiriad IP go iawn rhag gollwng.

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. [4]

Q2: Beth yw VPN dwbl neu lwybro Aml-Hop?

Mae Aml-hop yn llwybro eich traffig drwy ddau neu fwy o weinyddion VPN yn eu trefn. Mae hyn yn ychwanegu ail haen o amgryptio ac yn helpu i gadw eich cyfeiriad IP go iawn yn gudd rhag yr ail hop os caiff un gweinydd ei gyfaddawdu.

Q3: Beth yw gollwng WebRTC a sut mae VPN yn ei atal?

Protocol porwr yw WebRTC a all ddatgelu eich cyfeiriadau IP lleol a chyhoeddus go iawn hyd yn oed pan fydd VPN yn weithredol. Mae VPNs premiwm yn blocio neu'n ffugio ceisiadau WebRTC yn eu rhaglenni bwrdd gwaith/symudol a'u hestyniadau porwr.

Q4: Beth yw gweinyddion RAM-yn-unig a pham maen nhw'n bwysig?

Mae gweinyddion traddodiadol yn ysgrifennu data i yriannau caled, y gellir eu cipio neu eu cyfaddawdu. Mae gweinyddion RAM yn unig (heb ddisg) yn rhedeg yn gyfan gwbl mewn cof anweddol (RAM). Pan gaiff y gweinydd ei ailgychwyn neu ei ddiffodd, caiff data yn y cof ei ddileu.

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 yw Twnelu Hollt a phryd y dylwn ei ddefnyddio?

Mae Twnelu Hollt yn gadael i chi ddewis pa apiau sy'n llwybro drwy dwnnel VPN wedi'i amgryptio a pha rai sy'n cysylltu'n uniongyrchol â'r rhyngrwyd. Defnyddiwch ef i lwybro apiau bancio sensitif drwy'r VPN tra bo gemau lleol yn cysylltu'n uniongyrchol, gan osgoi cuddni ychwanegol y VPN.

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: Beth yw cynghreiriau 5/9/14 Eyes a pham y dylai fod o bwys i mi?

Gall awdurdodaeth effeithio ar y broses gyfreithiol y gall darparwr ei hwynebu, ond mae'r risg ymarferol i breifatrwydd hefyd yn dibynnu ar ba ddata y mae'r darparwr yn ei gadw, ei bensaernïaeth dechnegol, ei berchnogaeth, ei adroddiadau tryloywder a'i hanes archwilio.

Q9: Beth yw diogelwch rhag Gollyngiadau DNS?

Mae diogelu rhag gollyngiadau DNS yn gorfodi eich dyfais i anfon ymholiadau chwilio gwefannau (ymholiadau DNS) drwy weinyddion DNS preifat, wedi'u hamgryptio, y VPN yn hytrach na gweinyddion eich ISP. Mae hyn yn atal eich ISP rhag olrhain pa wefannau rydych yn ymweld â nhw.

Q10: A all VPN osgoi sbarduno rhyngrwyd gan ISP?

Weithiau. Gall VPN helpu pan fydd ISP yn arafu gweithgareddau adnabyddadwy yn ddetholus, ond ni fydd yn goresgyn tagfeydd, capiau data, terfynau cyflymder ar lefel cyfrif, nac ansawdd rhwydwaith gwael.

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. PRISIAD MARCHNAD

Mae'r farchnad VPN fyd-eang wedi tyfu'n gyflym, wedi'i sbarduno gan ofynion cynyddol gweithio o bell a gofynion diogelwch mentrau.

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. [4]

4. SAFONAU ARCHWILIO LLYM

Mae darparwyr VPN blaenllaw yn cyflogi archwilwyr allanol (fel Cure53 neu PwC) i gynnal adolygiadau cod annibynnol a dilysu nad ydynt yn cofnodi unrhyw weithgarwch defnyddwyr.

5. TARDDIAD CYNGHRAIR 5-EYES

Tyfodd cynghrair y Five Eyes o gytundeb cudd-wybodaeth signalau UKUSA 1946 rhwng yr Unol Daleithiau a'r DU, ac ymunodd Canada, Awstralia a Seland Newydd yn ddiweddarach.

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. DEFNYDD CORFFORAETHOL

Mae canran fawr o weithwyr mentrau ledled y byd yn defnyddio VPNau diogel i fewngofnodi i gronfeydd data mewnol, gan ei wneud yn safon ddiogelwch allweddol.

8. VPNAU DATGANOLEDIG

Mae VPNs datganoledig (dVPNs) yn dosbarthu traffig ar draws rhwydwaith o nodau a redir gan gymheiriaid, gan leihau dibyniaeth ar un darparwr canolog.

9. ANHYSBYSRWYDD TOR O'I GYMHARU Â VPN

Mae VPN yn twnelu traffig drwy un darparwr, tra bo Tor (The Onion Router) yn anfon traffig drwy dri chyfnewidydd gwirfoddol (gwarchod, canol ac allanfa) fel nad oes unrhyw gyfnewidydd unigol yn gwybod y ddau ben.

10. COST TORRI DATA

Mae defnyddio model mynediad diogel dim ymddiriedaeth (zero-trust) gyda VPN yn helpu sefydliadau i ddiogelu eiddo deallusol a lliniaru effaith ariannol toriadau data.

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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[4] 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/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Allwedd Atebion: Taflen Waith Beth yw VPN

1 **Prif Swyddogaeth** PROTOCOLAU — **Ateb Cywir: B**

NODYN ADDYSGU

Prif waith VPN yw sefydlu twnnel wedi'i amgryptio sy'n cysgodi data llwyth tâl pecynnau ac yn cuddio cyfeiriad IP cyhoeddus y defnyddiwr. Ffynhonnell: IETF Tunnel RFC.

2 **Twnelu Rhwydwaith** CUDDNI — **Ateb Cywir: D**

NODYN ADDYSGU

Mae protocolau twnelu yn crynhoi pecynnau data gwreiddiol y tu mewn i becynnau cludo allanol er mwyn croesi rhwydweithiau cyhoeddus yn ddiogel. Dyfyniad: IETF Tunnel RFC.

3 **Cwestiwn 3** — **Ateb Cywir: B**

NODYN ADDYSGU

Pa safon amgryptio a ddefnyddir yn eang i ddiogelu traffig VPN? → Safon AES-256 fodern

4 **Cydrannau wedi'u Hamgryptio** RHEOLAETHAU LLWYBRO — **Ateb Cywir: C**

NODYN ADDYSGU

Mae VPN yn amgryptio segment llwyth tâl cyflawn pecynnau data IP, gan gadw cynnwys y trosglwyddiad yn gyfrinachol. Ffynhonnell: IETF Tunnel RFC.

5 **Cwestiwn 5** — **Ateb Cywir: A**

NODYN ADDYSGU

Mae amgryptio yn defnyddio algorithm ac allwedd i droi testun plaen yn destun seiffr annarllenadwy.

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Rhwystro Clustfeinio** CUDDIO IP — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae twneli wedi'u hamgryptio yn sicrhau bod llwythi tâl pecynnau yn parhau'n annarllenadwy i actorion sy'n rhyng-gipio data ar rwydweithiau Wi-Fi lleol. Ffynhonnell: Deloitte Advisory.

7 **Newidiadau Caledwedd** CYFLYMDERAU — **Ateb Cywir: Gau**

NODYN ADDYSGU

Twneli rhwydwaith sy'n seiliedig ar feddalwedd yw VPNs ac nid ydynt yn addasu caledwedd llwybrydd eich porth yn ffisegol. Dyfyniad: Cure53 Audit.

8 **Twnelu Pecynnau** RISG CLUSTFEINIO — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae twnelu'n gweithio drwy lapio pecynnau rhwydwaith gwreiddiol y tu mewn i benynnau cludo ar gyfer y daith. Dyfyniad: IETF Tunnel RFC.

9 **Allweddi Cymesur** WALIAU TÂN — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae cryptograffeg gymesur yn defnyddio allwedd a rennir ar gyfer amgryptio a dadgryptio ffrydiau rhwydwaith. Ffynhonnell: WireGuard Project.

10 **Imiwnedd Pŵer** DIM LOGIAU — **Ateb Cywir: Gau**

NODYN ADDYSGU

Dim ond signalau cysylltiad gweithredol y mae VPN yn eu hamgryptio; ni all atal toriadau gwasanaeth a achosir gan doriadau pŵer lleol. Ffynhonnell: EDRi Retention Guidelines.

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

H 1. Twnelu	E 2. Protocol	G 3. Lled Band	A 4. Gweinydd
C 5. GEO-FLOCIO	D 6. Wal dân	F 7. Preifatrwydd	B 8. ISP

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 TWNELU	2 LLED BAND	3 GEO-FLOCIO	4 PROTOCOL
5 WAL DÂN	6 GWEINYDD		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 B – PROTOCOL	2 E – GEOFLOCIO	3 F – WALDAN	4 G – PREIFATRWYDD
5 H – DARPARWR	6 A – TWNELU	7 D – GWEINYDD	8 C – LLEDBAND

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio Twnelu, Protocol a Lled Band 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.

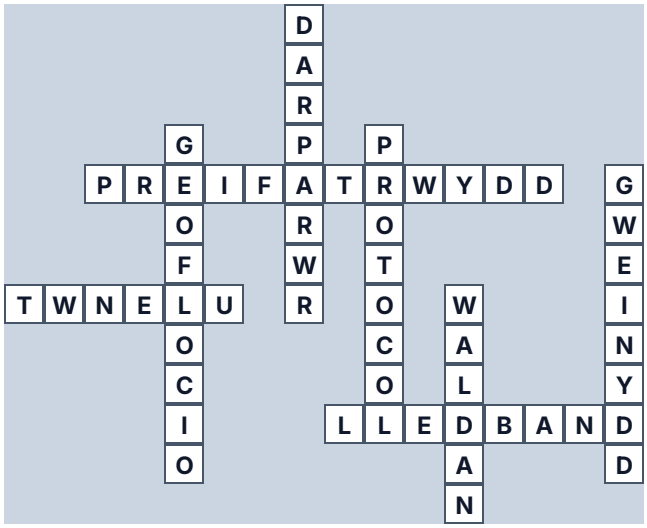
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

4 ar draws: PREIFATRWYDD Y cyflwr o fod yn rhydd rhag cael eich tracio neu rhag gwyliadwriaeth gyhoeddus (12 llythyren)

6 ar draws: TWNELU Lapio pecynnau data y tu mewn i becyn arall er mwyn eu cludo'n ddiogel (6 llythyren)

8 ar draws: LLEDBAND Y gyfradd uchaf o drosglwyddo data ar draws cysylltiad (8 llythyren)

CLIWIAU I LAWR

1 i lawr: DARPARWR Y cwmni gwasanaeth rhyngrwyd (ISP), sy'n logio eich traffig oni bai ei fod wedi'i amgryptio (8 llythyren)

2 i lawr: GEOFLOCIO Cyfyngiad sy'n atal mynediad i'r we yn seiliedig ar leoliad ffisegol (9 llythyren)

3 i lawr: PROTOCOL Set o reolau sy'n pennu sut caiff data ei drosglwyddo dros y rhwydwaith (8 llythyren)

5 i lawr: GWEINYDD Cyfrifiadur pell sy'n llwybro eich traffig ac yn cuddio eich IP (8 llythyren)

7 i lawr: WALDAN System ddiogelwch sy'n monitro ac yn rhwystro traffig heb awdurdod (6 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. NTELUW — **TWNELU**
2. DLDLNABE — **LLEDBAND**
3. GOLECOFIO — **GEOFLOCIO**
4. DRFETDAYWPRI — **PREIFATRWYDD**
5. OCRLTPOO — **PROTOCOL**
6. DDIYGNWE — **GWEINYDD**
7. AWDNLA — **WALDAN**
8. PAARDWRR — **DARPARWR**

ALLWEDD HER Y SEIFFR CYFRINACHOL

"DIOGELWCH EICH PREIFATRWYDD GYDA THWNNEL DIOGEL"

Allwedd Atebion yr Astudiaethau Achos

A Senario A: Diogelwch Rhwydweithiau Cyhoeddus

CLUSTFEINIO AC AMGRYPTIO | Cyfyng-gyngor Sarah

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Risgiau: Clustfeinio ar becynnau, rhyng-gipio data, ac ymosodiadau dyn-yn-y-canol. Gallai rhywun ar yr un rhwydwaith siop goffi gipio ei manylion mewngofnodi neu ei ffeil gwaith cartref.
- Diogelwch VPN: Yn amgryptio llwythi pecynnau'r rhwydwaith, gan wneud traffig twnnel a ryng-gipiwyd yn annarllenadwy i snwpwyr goddefol ar y rhwydwaith lleol pan fo'r VPN wedi'i ffurfweddu'n gywir.

B Senario B: Cyrchu Adnoddau sydd wedi'u Blocio

GEO-RWYSTRO A CHYFEIRIADAU IP | Dilema Alex

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Pam Mae Wedi'i Flocio: Mae'r gwesteiwr ffrydio yn defnyddio geoflocio, sy'n mapio cyfeiriad IP lleol y teithiwr i'w wlad ffisegol ac yn ei flocio ar sail trwyddedu tiriogaethol.
- Sut mae VPN yn Helpu: Cuddio ei leoliad go iawn drwy lwybro traffig drwy weinydd yn ei famwlad. Mae'r wefan yn gweld IP y famwlad, gan ganiatáu mynediad.