Enw: _____ Dyddiad: _____ Sgôr: _____

Procsi yn erbyn VPN Taflen Waith

Cymharu gweinyddion dirprwy a rhwydweithiau preifat rhithwir, gwahaniaethau amgryptio, a llwybro ar lefel rhaglen o'i gymharu â llwybro ar draws y system

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

- Cyferbynnwch ddirprwyon rhaglenni ag amgryptio VPN ar draws y system.
- Nodwch alluoedd SOCKS5 o'u cymharu â dirprwyon HTTP sylfaenol.
- Dadansoddwch sut mae dirprwyon mewn porwyr yn gadael apiau cefndir yn agored i risg.
- Deall sut mae ISPs yn cofnodi traffig heb ei amgryptio ar dwneli dirprwy.
- Dewiswch yr offeryn llwybro cywir yn seiliedig ar anghenion cyflymder a diogelwch.

CYFARWYDDIADAU'R DAFLEN WAITH CYMHARU PROCSI

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 gymharu dirprwyon a VPNs. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

PROCSI YN ERBYN VPN (CYFLWYNIAD)

Mae procsïau a VPNs yn cyflawni swyddogaethau preifatrwydd digidol gwahanol. Mae gweinydd procsi yn gweithredu fel ailgyfeiriad ar haen y rhaglen, gan guddio eich cyfeiriad IP ar gyfer rhaglenni penodol heb amgryptio'r data. Mae VPN yn gweithredu ar lefel y rhwydwaith, gan ddiogelu holl draffig y system gydag amgryptio. Mae dewis yr offeryn cywir yn dibynnu ar eich gofynion diogelwch.

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

Pwynt Gwirio 1: Her Amlddewis

1. **1. Ar ba haen o'r model OSI y mae dirprwy HTTP safonol yn gweithredu?**
   - A. Haen ffisegol
   - B. Haen rhwydwaith
   - C. Haen rhaglenni
   - D. Haen Cyswllt Data

2. **2. Beth yw un o fanteision protocol allweddol SOCKS5 dros ddirprwyon HTTP safonol?**
   - A. Mae'n gorfodi amgryptio llwyth tâl llawn
   - B. Mae'n cefnogi llwybro unrhyw draffig TCP/UDP
   - C. Mae'n imiwn i ollyngiadau DNS
   - D. Mae'n gweithredu'n uniongyrchol yng ngofod y cnewyllyn

3. **3. Pam mae VPN yn gyffredinol yn fwy diogel na gweinydd dirprwy?**
   - A. Mae'n rhedeg ar galedwedd pell cyflymach
   - B. Mae'n amgryptio'r holl draffig rhwydwaith ar draws y system
   - C. Nid oes angen tablau llwybro lleol arno
   - D. Mae'n dileu cuddni rhwydwaith yn llwyr

4. **4. Pa fath o ddirprwy sy'n ailgyfeirio traffig heb unrhyw amgryptio yn ddiofyn?**
   - A. Dirprwy HTTP sylfaenol
   - B. Dirprwy HTTPS wedi'i amgryptio
   - C. Cleient WireGuard diogel
   - D. Gweinydd VPN cuddiedig

5. **5. Beth sy'n digwydd i draffig rhaglenni cefndir wrth ddefnyddio dirprwy porwr?**
   - A. Caiff ei amgryptio'n awtomatig
   - B. Mae'n cael ei rwystro gan y gweinydd dirprwy
   - C. Caiff ei lwybro drwy dwnnel y dirprwy
   - D. Mae'n osgoi'r dirprwy ac yn datgelu eich IP

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae dirprwy SOCKS5 yn amgryptio holl lwythi tâl y pecynnau sy'n mynd drwy'r gweinydd.

Gwir Gau

7 Cwestiwn 7

7. Mae VPN yn gweithredu ar yr haen rwydwaith i ddiogelu holl draffig y system.

Gwir Gau

8 Cwestiwn 8

8. Yn gyffredinol mae procsïau'n gyflymach na VPNs oherwydd eu bod yn cyflawni amgryptio pecynnau dwfn.

Gwir Gau

9 Cwestiwn 9

9. Mae ffurfweddu dirprwy yn gofyn am sefydlu ailgyfeiriadau traffig mewn apiau penodol.

Gwir Gau

10 Cwestiwn 10

10. Nid yw defnyddio dirprwy yn diogelu eich traffig data rhag olrhain gan yr ISP lleol.

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 _____ haen rhaglen yn ailgyfeirio traffig porwr penodol heb ddiogelu apiau eraill.

2. Mae _____ cadarn yn amgáu ac yn amgryptio holl becynnau data'r ddyfais.

3. Mae'r protocol _____ yn eistedd rhwng yr haen rhaglen a'r haen gludo.

4. Mae dirprwyon HTTP yn gweithredu ar haen _____ y model OSI.

5. Nid oes gan weinyddion dirprwy safonol _____ ar y llwyth, gan adael data'n agored i niwed.

6. Mae VPN yn darparu diogelwch ar lefel y _____ ar gyfer pob addasydd rhwydwaith.

BANC GEIRIAU GEIRFA

AMGRYPTIO | CYMORTH UDP | DIRPRWY | GWELEDEDD YR ISP | RHAGLEN | SOCKS5 | SYSTEM GYFAN | TWNNEL VPN

Ysgrifennwch eich atebion yma:

1.
2.
3.
4.
5.
6.

Pwynt Gwirio 4: Paru Cysyniadau Rhwydwaith

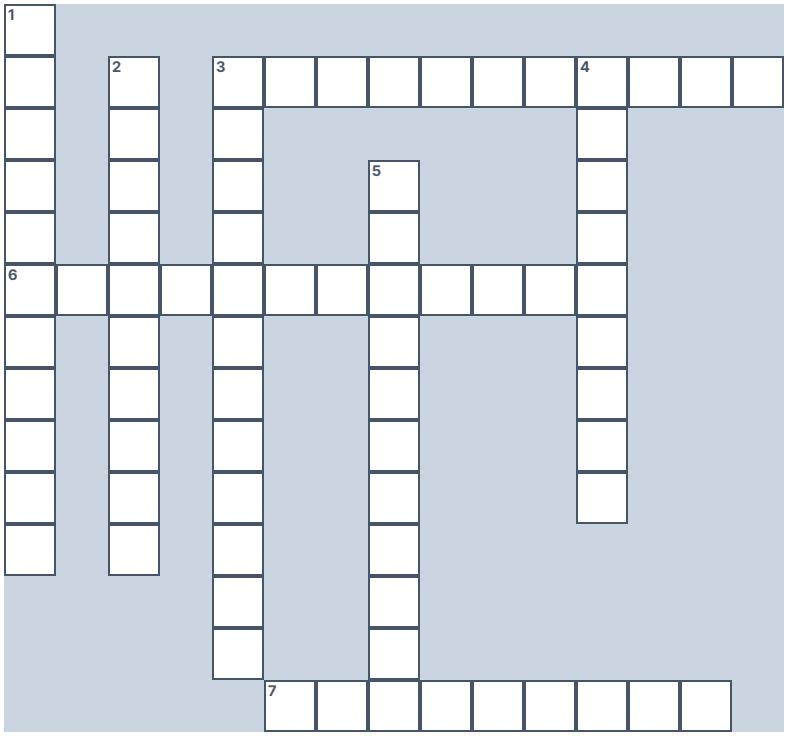
PARU DIFFINIADAU

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. Dirprwy HTTP	A	Llwybro ar lefel y system weithredu sy'n amgryptio traffig pob rhaglen.
☐	2. Dirprwy SOCKS5	B	Yr haen Gymhwysiad lle mae protocolau dirprwy gwe safonol yn gweithredu.
☐	3. Twnnel VPN	C	Gallu SOCKS5 i gyfnewid UDP yn ogystal â TCP, yn wahanol i ddirprwyon HTTP plaen.
☐	4. Ar draws y system,	D	Estyniad cleient sydd ond yn cuddio traffig y tu mewn i flwch tywod y porwr.
☐	5. Haen 7 OSI	E	Amgryptio ac amgáu sy'n lapio holl draffig cefndir y ddyfais.
☐	6. Cefnogaeth UDP	F	Cyflwr traffig lle mae data dirprwy heb ei amgryptio yn parhau'n weladwy i ISPs.
☐	7. Dirprwy Porwr	G	Dirprwy haen rhaglenni sy'n ailgyfeirio traffig porwr gwe penodol.
☐	8. Gweledegdd yr ISP	H	Protocol dirprwy rhwng yr haenau rhaglen a thrafnidiaeth, heb amgryptio.

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

3. Gwasanaeth haen rhaglen sy'n ailgyfeirio traffig porwr gwe penodol (11)

6. Protocol rhwng yr haen rhaglen a'r haen gludo, heb amgryptio (12)

7. Amgryptio ac amgáu sy'n lapio holl draffig cefndir y ddyfais (9)

CLIWIAU I LAWR

1. Cyflwr traffig lle mae data dirprwy heb ei amgryptio yn parhau'n weladwy i ISPau (11)

2. Gallu SOCKS5 i drosglwyddo UDP yn ogystal â TCP, yn wahanol i ddirprwyon HTTP plaen (10)

3. Estyniad cleient sydd ond yn cuddio traffig y tu mewn i flwch tywod y porwr (12)

4. Yr haen Rhaglen lle mae protocolau dirprwy gwe safonol yn gweithredu (9)

5. Llwybro ar lefel y system weithredu sy'n amgryptio traffig pob rhaglen (11)

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

3 ar draws: Gwasanaeth haen rhaglen sy'n ailgyfeirio traffig porwr gwe penodol (11 llythyren):

6 ar draws: Protocol rhwng yr haen rhaglen a'r haen gludo, heb amgryptio (12 llythyren):

7 ar draws: Amgryptio ac amgáu sy'n lapio holl draffig cefndir y ddyfais (9 llythyren):

CLIWIAU I LAWR

1 i lawr: Cyflwr traffig lle mae data dirprwy heb ei amgryptio yn parhau'n weladwy i ISPau (11 llythyren):

2 i lawr: Gallu SOCKS5 i drosglwyddo UDP yn ogystal â TCP, yn wahanol i ddirprwyon HTTP plaen (10 llythyren):

3 i lawr: Estyniad cleient sydd ond yn cuddio traffig y tu mewn i flwch tywod y porwr (12 llythyren):

4 i lawr: Yr haen Rhaglen lle mae protocolau dirprwy gwe safonol yn gweithredu (9 llythyren):

5 i lawr: Llwybro ar lefel y system weithredu sy'n amgryptio traffig pob rhaglen (11 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.

R Y O Y W S H T X A P U N N Z

W D D E Y W D A L E W G O I Q

R T I P T W N N E L V P N V U

O O U U K A E P M K A N V G G

P P Q X Y J K V J Y W Y P D J

Y I Z I J N A E I A S A J I F

W W E K Z K E K Q N J A F R O

R K N D N C D H I B A P R P L

P P W T I Y F Y S G X W H R F

R R P D U H T R O M Y C T W N

I D I R P R W Y S O C K S Y U

D K R H A E N S A I T H D H T

S L S Y S T E M G Y F A N T P

L M S H K P H Y P L W U N T Y

Q Q B A L P M B L I F I N P Y

RHESTR GEIRIAU GEIRFA

DIRPRWYHTTP, DIRPRWYSOCKS, TWNNELVPN, SYSTEMGYFAN, HAENSAITH, CYMORTHUDP, DIRPRWYPORWR, GWELADWYEDD

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. DIRPRWYHTTP
B. DIRPRWYSOCKS
C. TWNNELVPN
D. SYSTEMGYFAN
E. HAENSAITH
F. CYMORTHUDP
G. DIRPRWYPORWR
H. GWELADWYEDD

DIFFINIADAU A MEYSYDD PARU	
	1. Yr haen Rhaglen lle mae protocolau dirprwy gwe safonol yn gweithredu.
	2. Gallu SOCKS5 i drosglwyddo UDP yn ogystal â TCP, yn wahanol i ddirprwyon HTTP plaen.
	3. Gwasanaeth haen rhaglen sy'n ailgyfeirio traffig porwr gwe penodol.
	4. Estyniad cleient sydd ond yn cuddio traffig y tu mewn i flwch tywod y porwr.
	5. Amgryptio ac amgáu sy'n lapio holl draffig cefndir y ddyfais.
	6. Llwybro ar lefel y system weithredu sy'n amgryptio traffig pob rhaglen.
	7. Cyflwr traffig lle mae data dirprwy heb ei amgryptio yn parhau'n weladwy i ISPau.
	8. Protocol rhwng yr haen rhaglen a'r haen gludo, heb amgryptio.

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. RYTIWHDTRPP
2. NTPNWLVEN
3. HASAIHNTE
4. WPRRYRWRODIP
5. ICSYSRROWDKP
6. ENMYAFSYGST
7. YOCHTUDPRM
8. EWDDEGAWDYL

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Gwahaniaethau rhwng dirprwy a VPN			
2	Pethau sy'n cael eu gadael heb eu hamgryptio heb VPN			
3	Ffyrdd o adnabod rhwydwaith Wi-Fi ffug			
4	Pethau y mae canolwr yn eu gwneud ym mywyd bob dydd			
5	Sefyllfaoedd lle mae dirprwy yn ddigon			
6	Dyfeisiau sy'n gallu defnyddio VPN			
7	Mathau o ddirprwy rydych chi'n eu hadnabod			
8	Pethau y gall VPN eu cuddio			
9	Mythau am VPNs			
10	Addewidion y mae darparwr VPN da yn eu gwneud			
11	Pethau na all VPN eich diogelu rhagddynt			
12	Geiriau o'r daflen waith hon rydych chi am eu cofio			
13	Rhesymau dros ddefnyddio VPN wrth deithio			
14	Sefyllfaoedd lle rydych chi eisiau VPN			
15	Mannau lle byddech chi'n defnyddio VPN			

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 yn Coffee & Bytes ar rwydwaith agored o'r enw 'Free_Wi-Fi_No_Password'. Mae angen i mi fewngofnodi i'm e-bost ysgol, ac mae ffrind yn dweud bod dirprwy porwr am ddim yn ddigon i aros yn ddiogel. A fyddai dirprwy yn diogelu fy manylion mewngofnodi a'm ffeiliau, neu oes angen VPN arnaf?"

ALEX (MYFYRIWR SY'N TEITHIO)

👩‍💻 "Rwy dramor ac mae rhaglen ddogfen bioleg sy'n cael ei chynnal yn fy ngwlad gartref yn dweud 'Nid yw'r fideo hwn ar gael yn eich lleoliad presennol.' Mae cyd-ddisgybl yn defnyddio dirprwy, ac mae gen i VPN. Pam rwy wedi fy rhwystro, a pha offeryn fyddai'n gweithio'n well?"

Pwynt Gwirio 9: Dadgryptio'r Seiffr

I gwblhau eich hyfforddiant ar gymharu dirprwyon, dadgryptiwch y neges gyfrinachol hon am dwnelu diogel.

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

1	9	12	7	25	6	5	9	18	9	23	3	8		5	9	3	8	
20	18	1	6	6	9	7		7	25	4	1		4	9	18	16	18	23	25

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: Beth yw gweinydd procsi?

Cyfryngwr sy'n anfon ceisiadau ymlaen rhwng eich rhaglen a'r gweinydd cyrchfan yw gweinydd dirprwy. Mae'r wefan yn gweld cyfeiriad IP y dirprwy yn lle eich un chi, ond dim ond traffig o apiau sydd wedi'u ffurfweddu i ddefnyddio'r dirprwy sy'n cael ei ailgyfeirio, ac nid yw dirprwy sylfaenol yn amgryptio'r traffig hwnnw.

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 dirprwy yn VPN?

Na. Mae dirprwy yn trosglwyddo traffig ar gyfer apiau penodol, fel arfer heb amgryptio. Mae VPN yn adeiladu twnnel wedi'i amgryptio ar haen y rhwydwaith sy'n cario holl draffig y ddyfais, gan gynnwys apiau cefndir.

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 dirprwy am ddim?

Gallwch, ond yn aml mae dirprwyon am ddim yn cael eu rhedeg gan weithredwyr anhysbys. Gan nad yw dirprwy sylfaenol yn amgryptio traffig, gall ei weithredwr weld a hyd yn oed newid tudalennau heb eu hamgryptio. Gwiriwch pwy sy'n rhedeg y gwasanaeth cyn ei ddefnyddio.

Q7: A yw dirprwy yn cadw logiau?

Gall wneud hynny. Mae dirprwy yn ymdrin â phob cais y mae'n ei anfon ymlaen, felly gall ei weithredwr gofnodi eich cyfeiriad IP, y gwefannau rydych chi'n ymweld â nhw a phryd. Gwiriwch pwy sy'n ei redeg a beth mae ei bolisi preifatrwydd yn ei ddweud.

Q8: Pryd mae dirprwy yn ddigon?

Gall dirprwy fod yn ddigon ar gyfer tasgau risg isel, fel newid lleoliad ymddangosiadol un porwr. Ar gyfer bancio, Wi-Fi cyhoeddus neu ddiogelu pob ap ar ddyfais, VPN yw'r dewis mwy diogel gan ei fod yn amgryptio'r holl draffig.

Q9: A all dirprwy ddiogelu holl apiau fy ffôn?

Na. Dim ond apiau sy'n parchu gosodiad y dirprwy sy'n ei ddefnyddio; mae'r gweddill yn cysylltu'n uniongyrchol. Mae ap VPN yn llwybro holl apiau'r ffôn drwy ei dwnnel wedi'i amgryptio yn lle hynny.

Q10: Beth yw procsi SOCKS5?

Mae SOCKS5, a ddiffinnir yn RFC 1928, yn brotocol dirprwy sy'n eistedd rhwng haen y rhaglen a'r haen gludo. Gall drosglwyddo cysylltiadau TCP a datagramau UDP ac mae'n cefnogi dilysu, ond nid oes ganddo amgryptio adeiledig. [1]

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

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

Q1: Ar ba haenau rhwydwaith mae procsïau a VPNs yn gweithredu?

Mae dirprwy HTTP yn gweithio ar yr haen rhaglenni (Haen 7) ac yn deall ceisiadau gwe. Mae SOCKS5 yn eistedd rhwng yr haen rhaglenni a'r haen gludo. Mae protocolau VPN fel IPsec neu WireGuard yn gweithio ar yr haen rwydwaith, felly gallant gario holl draffig IP y ddyfais.

Q2: A yw gwefan HTTPS yn aros wedi'i hamgryptio drwy brocsi?

Ie. Pan fyddwch yn agor gwefan HTTPS drwy ddirprwy, mae amgryptio TLS yn rhedeg o un pen i'r llall rhwng eich porwr a'r wefan, felly mae'r dirprwy'n gweld y parth ond nid cynnwys y dudalen. Mae tudalennau HTTP plaen yn dal yn ddarllenadwy.

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 dirprwy tryloyw a phwy sy'n ei ddefnyddio?

Mae dirprwy tryloyw yn rhyng-gipio traffig heb unrhyw osod ar ddyfais y defnyddiwr. Mae ysgolion, cwmnïau ac ISPs yn eu defnyddio ar gyfer storio dros dro neu hidlo cynnwys. Yn aml nid yw defnyddwyr yn gwybod bod un ar waith, ac nid yw'n rhoi unrhyw breifatrwydd iddynt.

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: Pam gall dirprwy deimlo'n gyflymach na chysylltiad VPN?

Mae dirprwy sylfaenol yn hepgor amgryptio ac yn ymdrin â thraffig o un ap yn unig, felly mae'n ychwanegu llai o brosesu. Mae VPN yn amgryptio pob pecyn o'r ddyfais. Gyda phrotocolau modern mae'r gwahaniaeth yn aml yn fach, ac mae'r dirprwy yn cynnig llawer llai o ddiogelwch.

Q8: A all gwefannau ddweud fy mod yn defnyddio dirprwy neu VPN?

Yn aml, ydy. Mae llawer o wefannau'n gwirio cyfeiriadau IP yn erbyn rhestrau o weinyddion procsi a VPN hysbys, a gall procsïau HTTP ychwanegu penynnau fel Via neu X-Forwarded-For. Mae gwasanaethau ffrydio'n aml yn rhwystro'r ddau.

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 procsi atal sbarduno gan ISP?

Anaml. Nid yw dirprwy sylfaenol yn amgryptio traffig, felly gall yr ISP weld pa fath o weithgarwch ydyw o hyd. Mae VPN yn cuddio mathau o draffig, ond nid yw'r naill offeryn na'r llall yn datrys tagfeydd na chapiau data.

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. SAFON SOCKS

Cyhoeddwyd SOCKS Protocol Version 5 gan yr IETF fel RFC 1928 ym mis Mawrth 1996, ac mae'n dal i fod yn fanyleb gyfeirio ar gyfer y dirprwyon SOCKS5 a ddefnyddir gan borwyr ac apiau heddiw. [1]

2. HAEN SHIM

Mae RFC 1928 yn disgrifio SOCKS fel haen shim rhwng yr haen rhaglenni a'r haen gludo, felly ni all anfon traffig haen rhwydwaith fel ICMP ymlaen. [1]

3. CYFNEWID UDP

Ychwanegodd SOCKS5 y gorchymyn UDP ASSOCIATE, gan adael i ddirprwy drosglwyddo datagramau UDP yn ogystal â chysylltiadau TCP, rhywbeth nad yw dirprwyon HTTP plaen yn ei drin. [1]

4. PORTH SOCKS RHAGOSODEDIG

Mae cleientiaid SOCKS5 yn cysylltu â'r gweinydd dirprwyol ar borth TCP 1080 yn ddiofyn, fel y'i diffinnir yn RFC 1928; mae llawer o wasanaethau dirprwy yn gadael i ddefnyddwyr ddewis pyrth eraill. [1]

5. CYFRYNGWYR HTTP

Mae safon HTTP (RFC 9110) yn diffinio dirprwy fel asiant anfon negeseuon a ddewisir gan y cleient, sy'n trosglwyddo ceisiadau tuag at y gweinydd tarddiad.

6. ARCHWILIO PECYNNAU DWFN

Mae Archwilio Pecynnau Dwfn (DPI) yn archwilio cynnwys pecynnau a phatrymau traffig; mae traffig dirprwy heb ei amgryptio yn gwbl weladwy iddo, tra bo traffig VPN yn datgelu llawer llai.

7. VPNAU HAEN RHWYDWAITH

Mae IPsec, a ddisgrifir yn NIST SP 800-77, yn diogelu traffig ar haen y rhwydwaith, felly gellir diogelu pecynnau IP pob rhaglen heb osod pob rhaglen ar wahân. [2]

8. CWMPAS PORWR YN UNIG

Mae dirprwy a osodir mewn un porwr yn effeithio ar y porwr hwnnw yn unig; mae cleientiaid e-bost, gemau a diweddariadau system yn parhau i ddefnyddio cysylltiad arferol y ddyfais.

9. TOR O'I GYMHARU Â DIRPRWYON

Mae Tor yn anfon traffig drwy dri chyfnewidydd gwirfoddol (gwarchod, canol ac allanfa) ac fel arfer fe'i cyrhaeddir drwy ddirprwy SOCKS lleol, gan ychwanegu haenau na all un dirprwy eu darparu.

10. CYFADDAWD CYFLYMDER

Gall procsïau ymddangos yn gyflymach oherwydd eu bod yn hepgor amgryptio, ond mae protocolau VPN modern fel WireGuard yn ychwanegu ychydig iawn o orbenion wrth amddiffyn holl draffig y ddyfais.

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] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Allwedd Atebion: Cymharu gweinyddion dirprwy a rhwydweithiau preifat rhithwir, gwahaniaethau amgryptio, a llwybro ar lefel rhaglen yn erbyn llwybro ar draws y system

1 **Haen OSI Procsi** PROTOCOLAU — **Ateb Cywir: C**

NODYN ADDYSGU

Mae dirprwyon HTTP/HTTPS safonol yn gweithredu ar yr haen Rhaglenni (Haen 7) ac yn ailgyfeirio traffig porwr penodol. Nid oes ganddynt lwybro rhwydwaith ar draws y system. Ffynhonnell: Tor Project Foundation.

2 **Cwestiwn 2** — **Ateb Cywir: B**

NODYN ADDYSGU

Mae SOCKS5 yn cyfnewid traffig TCP ac UDP rhwng yr haenau rhaglen a thrafnidiaeth ond nid yw'n amgryptio yn ddiofyn, tra bod dirprwyon HTTP yn delio â cheisiadau gwe.

3 **Amgryptio System VPN** DIOGELWCH WI-FI — **Ateb Cywir: B**

NODYN ADDYSGU

Mae VPN yn amgáu ac yn amgryptio holl draffig y system weithredu ar draws y system gyfan, ond dim ond ar gyfer rhaglenni penodol sydd wedi'u ffurfweddu y mae dirprwy yn ailgyfeirio traffig. Ffynhonnell: Deloitte Advisory.

4 **Diffyg Amgryptio Procsi** RHEOLAETHAU LLWYBRO — **Ateb Cywir: A**

NODYN ADDYSGU

Mae procsis HTTP yn anfon traffig porwr ymlaen ar yr haen rhaglenni heb amgryptio llwythi tâl pecynnau, sy'n golygu y gall gweithredwr eich rhwydwaith neu eich ISP olrhain traffig eich cynnwys o hyd. Ffynhonnell: IETF Proxy Vulnerabilities.

5 **Gwendid Osgoi** PREIFATRWYDD — **Ateb Cywir: D**

NODYN ADDYSGU

Dim ond i'r porwr gwe ei hun y mae dirprwyon porwr yn cymhwyso rheolau. Mae apiau cefndir, diweddariadau'r system weithredu, a chleientiaid e-bost yn osgoi'r dirprwy, gan ddatgelu eich cyfeiriad IP brodorol. Ffynhonnell: W3C Consortium.

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

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

NODYN ADDYSGU

Mae SOCKS5 yn cyfnewid traffig rhwng yr haenau rhaglen a thrafnidiaeth ond nid yw'n amgryptio yn ddiofyn, felly mae cynnwys pecynnau'n parhau'n ddarllenadwy wrth eu trosglwyddo.

7 **Twneli Haen Rhwydwaith** CYFLYMDERAU — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Drwy redeg ar haen y rhwydwaith, mae VPN yn llwybro ac yn amgryptio traffig sy'n gadael eich dyfais, gan helpu i ddiogelu traffig ar draws y system. Ffynhonnell: Deloitte Advisory.

8 **Terfyn Amgryptio Procsi** RISG CLUSTFEINIO — **Ateb Cywir: Gau**

NODYN ADDYSGU

Weithiau gall procsïau fod yn gyflymach, ond mae hyn oherwydd NAD ydynt yn amgryptio. Mae'r diffyg amgryptio hwn yn gadael data'n agored i gael ei archwilio. Ffynhonnell: IETF Proxy Vulnerabilities.

9 **Ailgyfeirio ar Lefel Apiau** WALIAU TÂN — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Yn wahanol i VPNs ar draws y system, mae angen gosod gweinyddion dirprwy â llaw yng ngosodiadau'r porwr neu mewn meysydd dirprwy rhaglenni penodol. Dyfyniad: W3C Consortium.

10 **Risg Tracio gan ISP** DIM LOGIAU — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gan nad yw dirprwyon HTTP/SOCKS5 safonol yn amgryptio data'r llwyth, mae eich ISP lleol yn cadw gweledd llawn o'ch gweithredoedd ar-lein. 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

G 1. Dirprwy HTTP	H 2. Dirprwy SOCKS5	E 3. Twnnel VPN	A 4. Ar draws y system,
B 5. Haen 7 OSI	C 6. Cefnogaeth UDP	D 7. Dirprwy Porwr	F 8. Gweledegd yr ISP

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 DIRPRWY	2 TWNNEL VPN	3 SOCKS5	4 RHAGLEN
5 AMGRYPTIO	6 SYSTEM GYFAN		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 E – HAENSAITH	2 F – CYMORTHUDP	3 A – DIRPRWYHTTP	4 G – DIRPRWYPORWR
5 C – TWNNELVPN	6 D – SYSTEMGYFAN	7 H – GWELADWYEDD	8 B – DIRPRWYSOCKS

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio Dirprwy HTTP, Dirprwy SOCKS5 a Twnnel VPN 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.

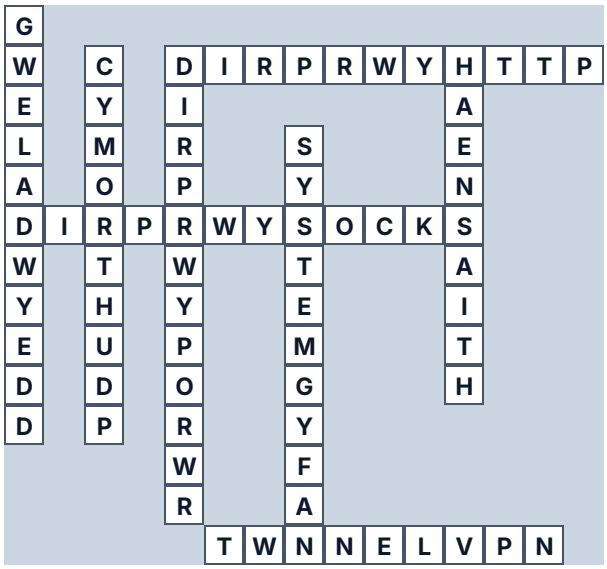
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

3 ar draws: DIRPRWYHTTP Gwasanaeth haen rhaglen sy'n ailgyfeirio traffig porwr gwe penodol (11 llythyren)

6 ar draws: DIRPRWYSOCKS Protocol rhwng yr haen rhaglen a'r haen gludo, heb amgryptio (12 llythyren)

7 ar draws: TWNNELVPN Amgryptio ac amgáu sy'n lapio holl draffig cefndir y ddyfais (9 llythyren)

CLIWIAU I LAWR

1 i lawr: GWELADWYEDD Cyflwr traffig lle mae data dirprwy heb ei amgryptio yn parhau'n weladwy i ISPau (11 llythyren)

2 i lawr: CYMORTHUDP Gallu SOCKS5 i drosglwyddo UDP yn ogystal â TCP, yn wahanol i ddirprwyon HTTP plaen (10 llythyren)

3 i lawr: DIRPRWYPORWR Estyniad cleient sydd ond yn cuddio traffig y tu mewn i flwch tywod y porwr (12 llythyren)

4 i lawr: HAENSAITH Yr haen Rhaglen lle mae protocolau dirprwy gwe safonol yn gweithredu (9 llythyren)

5 i lawr: SYSTEMGYFAN Llwybro ar lefel y system weithredu sy'n amgryptio traffig pob rhaglen (11 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. RYTIWHDTRPP — DIRPRWYHTTP
2. NTPNWLVEN — TWNNELVPN
3. HASAIHNTE — HAENSAITH
4. WPRRYRWRODIP — DIRPRWYPORWR
5. ICSYSRROWDKP — DIRPRWYSOCKS
6. ENMYAFSYGST — SYSTEMGYFAN
7. YOCHTUDPRM — CYMORTHUDP
8. EWDDEGAWDYL — GWELADWYEDD

ALLWEDD HER Y SEIFFR CYFRINACHOL

"AILGYFEIRIWCH EICH TRAFFIG GYDA DIRPRWY"

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.
- Procsi yn erbyn VPN: Nid yw procsi porwr sylfaenol yn amgryptio ei thraffig. Mae VPN yn amgryptio popeth ar y ddyfais, gan wneud pecynnau a ryng-gipiwyd yn annarllenadwy i snwpwyr lleol.

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.
- Pa Un Sy'n Gweithio'n Well: Mae'r ddau yn rhoi IP o'i famwlad iddo, ond dim ond yr ap sydd wedi'i ffurfweddu y mae dirprwy yn ei gwmpasu, tra bod VPN hefyd yn amgryptio holl draffig ei ddyfais.