Emri: _____ Data: _____ Pikët: _____

Çfarë është një VPN
Fletë pune

Ushtrime praktike për protokollet e rrjetit, tunelimin dhe kontrollet e sigurisë.

PËRMBLEDHJE E TË MËSUARIT PËR VPN-NË

NXËNËSI
STATUSI I STUDENTIT
Rruga e mbrojtësit të rrjetit

I SIGURT
STATUSI I LIDHJES
Mbrojtja e paketave të të dhënave

AKTIV
MBROJTJE NGA RRJEDHJET
Mbrojtje nga rrjedhjet e DNS dhe IPv6

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes parimeve themelore të Rrjeteve Private Virtuale (VPN). Do të eksplorosh si i sigurojnë të dhënat e tua tunelet e enkriptuara, si funksionojnë protokollet e rrjetit dhe si të identifikosh e të zbutësh rrjedhjet e privatësisë.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro konceptet dhe protokollet e VPN-së.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për VPN-në

URL: https://www.vpn.com/sq/vpn/

Udhërrëfyesi yt mësimor për VPN-në

- Shpjego konceptin e tunelimit dhe të enkapsulimit të të dhënave.
- Identifiko konfigurimet standarde të protokolleve dhe metodat e enkriptimit.
- Analizo rolet e serverëve dhe të maskimit të IP-së në rrjetet private virtuale.
- Kupto se si ISP-të gjurmojnë shfletimin dhe si e parandalon këtë një VPN.
- Dallo kufijtë operativë të topologjisë virtuale të rrjetit.

UDHËZIME PËR UDHËZUESIN "ÇFARË ËSHTË NJË VPN"

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për skenarët reale në pjesën e studimeve të rastit. Përfundo me aktivitetin bonus Mendo shpejt.

ÇFARË ËSHTË NJË VPN? (HYRJE)

Një Rrjet Privat Virtual është më shumë se një çelës privatësie. Është një tunel i enkriptuar që e drejton trafikun tënd të internetit përmes një serveri të largët. Kjo ta fsheh adresën IP, e pengon ISP-në të përpilojë regjistra të veprimeve të tua online dhe siguron të dhënat e tua në rrjete publike. Të kuptuarit e terminologjisë është thelbësor për ruajtjen e sigurisë dixhitale.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Cili është funksioni kryesor i një rrjeti privat virtual (VPN)?**

- A. Për të rritur shpejtësinë e renderimit të shfletuesit të internetit
- B. Për të enkriptuar paketat e të dhënave dhe për të maskuar IP-në tënde publike
- C. Për të ruajtur lokalisht bazat e të dhënave të cookie-ve të faqes
- D. Për të zëvendësuar harduerin fizik të kompjuterit tënd

2 **2. Çfarë është tunelizimi i rrjetit në kontekstin e një VPN-je?**

- A. Fshirja e skedarëve dublikatë të regjistrave të rrjetit
- B. Instalimi i skedarëve lokalë të ruajtjes së bazës së të dhënave
- C. Ndarja e skedarëve me kompjuterë të tjerë lokalë
- D. Mbyllja e një pakete rrjeti brenda një pakete tjetër të sigurt

3 **3. Cili standard enkriptimi përdoret gjerësisht për të mbrojtur trafikun VPN?**

- A. Enkriptimi i vjetruar DES
- B. Standardi modern AES-256
- C. Kodimi base64 në tekst të thjeshtë
- D. Shifrimi standard rot13

4 **4. Cila pjesë e trafikut tënd të rrjetit enkriptohet nga një VPN?**

- A. Vetëm punët e printimit në rrjetin lokal të pajisjes
- B. Rruga fizike e kabllos ethernet
- C. I gjithë pjesa e ngarkesës së të dhënave të paketës së rrjetit
- D. Vetëm historitë e kërkimeve të shfletuesit tënd

5 **5. Çfarë do të thotë termi "enkriptim" në rrjete?**

- A. Shndërrimi i të dhënave në tekst të thjeshtë në tekst të shifruar të palexueshëm
- B. Fshirja e regjistrimeve të vjetra të komunikimit
- C. Rritja e kufijve lokalë të shpejtësisë së gjerësisë së brezit
- D. Ndarja publike e çelësave të qasjes në bazën e të dhënave

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetja 6

6. Një VPN enkripton trafikun tënd për të parandaluar përgjimin lokal në Wi-Fi publik.

- E vërtetë
- E gabuar

7 Pyetja 7

7. Një VPN ndryshon fizikisht konfigurimin e harduerit të router-it tënd.

- E vërtetë
- E gabuar

8 Pyetja 8

8. Protokollet e tunelimit i mbështjellin paketat e të dhënave në një shtresë transporti të enkriptuar.

- E vërtetë
- E gabuar

9 Pyetja 9

9. Enkriptimi simetrik përdor të njëjtin çelës për të enkriptuar dhe dekriptuar trafikun.

- E vërtetë
- E gabuar

10 Pyetja 10

10. Përdorimi i një VPN-je e bën lidhjen tënde të internetit fizikisht imune ndaj çdo ndërprerjeje korrenti jashtë linje.

- E vërtetë
- E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Për të siguruar trafikun tënd, VPN-ja i mbështjell paketat e të dhënave brenda një protokolli tjetër, proces që njihet si _____ .

2. Nëse ke shpejtësi të ngadalta shkarkimi gjatë transmetimit, mund të jetë për shkak të një faktori: _____ i kufizuar i rrjetit.

3. Një shërbim transmetimi që është i disponueshëm vetëm në një vend të caktuar përdor një _____ për të kufizuar përdoruesit globalë.

4. Rregullat e lidhjes që përcaktojnë parametrat e enkriptimit dhe të lidhjes quhen _____ i VPN-së.

5. Kompjuteri yt përdor një _____ lokal për të monitoruar trafikun e rrjetit dhe për të bllokuar lidhjet e pasigurta.

6. Kur lidhesh me një VPN, të dhënat e tua rrugëzohen përmes një _____ të largët për të fshehur IP-në tënde publike.

BANKA E FJALËVE TË LEKSIKUT

FIREWALL GJEOBLLOKIM GJERËSI BANDE OFRUES ISP PRIVATËSI PROTOKOLL SERVER TUNELIM

Shkruaj përgjigjet e tua këtu:

1. **2.**

3. **4.**

5. **6.**

Pika e kontrollit 4: Përputhja e koncepteve të rrjetit

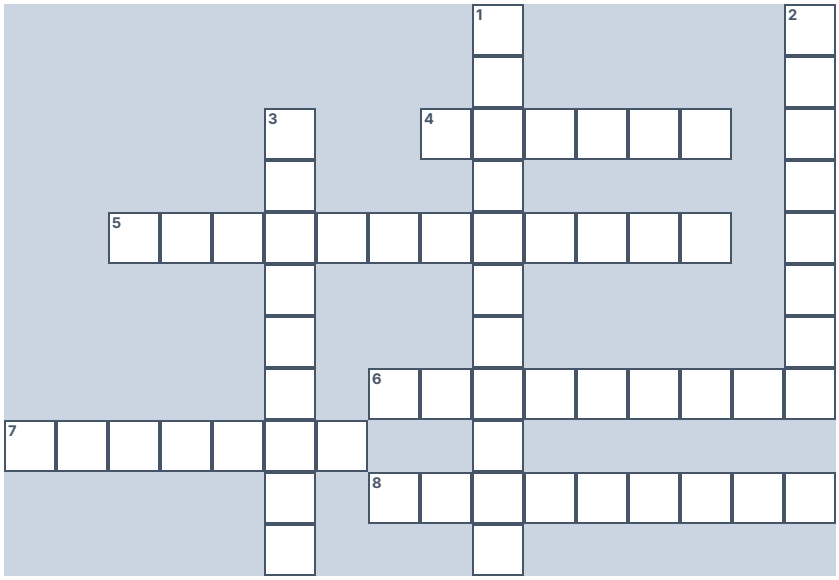
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. Tunelimi	A	Një kompjuter i largët që e drejton trafikun tënd dhe maskon IP-në tënde.
☐	2. Protokolli	B	Ofruesi i shërbimit të internetit që mbart trafikun tënd dhe mund të shohë aktivitetin e paenkriptuar.
☐	3. Gjerësia e brezit	C	Një kufizim që pengon qasjen në ueb bazuar në vendndodhjen fizike.
☐	4. Serveri	D	Një sistem sigurie që monitoron dhe bllokon trafikun e paautorizuar.
☐	5. Bllokimi gjeografik	E	Një bashkësi rregullash që përcaktojnë mënyrën e transmetimit të të dhënave nëpër rrjet.
☐	6. Firewall	F	Gjendja e lirë nga gjurmimi ose survejimi publik.
☐	7. Privatësia	G	Shpejtësia maksimale e transferimit të të dhënave përmes një lidhjeje.
☐	8. ISP	H	Mbështjellja e paketave të të dhënave brenda një pakete tjetër për tranzit të sigurt.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

4. Kompjuter i largët që rrugëzon trafikun tënd dhe maskon IP-në tënde (6)

5. Shpejtësia maksimale e transferimit të të dhënave nëpër një lidhje (12)

6. Bashkësi rregullash që përcaktojnë si transmetohen të dhënat nëpër rrjet (9)

7. Mbështjellja e paketave të të dhënave brenda një pakete tjetër për tranzit të sigurt (7)

8. Gjendja e lirisë nga gjurmimi ose survejimi publik (9)

VERTIKALISHT

1. Kufizim që parandalon qasjen në ueb sipas vendndodhjes fizike (11)

2. Sistem sigurie që monitoron dhe bllokon trafikun e paautorizuar (8)

3. Ofruesi i shërbimit të internetit, i cili regjistron trafikun tënd nëse nuk është i enkriptuar (9)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

4 horizontalisht: Kompjuter i largët që rrugëzon trafikun tënd dhe maskon IP-në tënde (6 shkronja):

5 horizontalisht: Shpejtësia maksimale e transferimit të të dhënave nëpër një lidhje (12 shkronja):

6 horizontalisht: Bashkësi rregullash që përcaktojnë si transmetohen të dhënat nëpër rrjet (9 shkronja):

7 horizontalisht: Mbështjellja e paketave të të dhënave brenda një pakete tjetër për tranzit të sigurt (7 shkronja):

8 horizontalisht: Gjendja e lirisë nga gjurmimi ose survejimi publik (9 shkronja):

VERTIKALISHT

1 vertikalisht: Kufizim që parandalon qasjen në ueb sipas vendndodhjes fizike (11 shkronja):

2 vertikalisht: Sistem sigurie që monitoron dhe bllokon trafikun e paautorizuar (8 shkronja):

3 vertikalisht: Ofruesi i shërbimit të internetit, i cili regjistron trafikun tënd nëse nuk është i enkriptuar (9 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

T U N E L I M P R Z T C Z U Ë

M L I F Z Ç L R D P O X O C T

I L B A Z M Ç I J A F D M D E

K A F G Ç Q P V K D R G Q Z R

O W E P U E A A A P U N L P O

L E S X P I Q T S Q E Ç L R Y

L R B Ë Q X V Ë H A S Q Z O Y

B I Y J Ë G L S P I I K K T S

O F N F O P F I Z A S N U O Ë

E T C Y Q Y B F K Z P Ë I K M

J G J E R Ë S I B A N D E O O

G M V C K Z Y Ë Y N V T J L T

O B S E R V E R M U S K F L T

Ç Y T I Q B V Z Y K Q P X G N

Ç A Ç I P U V V J H G S G Ë B

LISTA E FJALËVE TË LEKSIKUT

TUNELIM, PROTOKOLL, GJERËSIBANDE, PRIVATËSI, SERVER, OFRUESISP, GJEOBLLOKIM, FIREWALL

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

- **A. TUNELIM**
- **B. PROTOKOLL**
- **C. GJERËSIBANDE**
- **D. SERVER**
- **E. GJEOBLLOKIM**
- **F. FIREWALL**
- **G. PRIVATËSI**
- **H. OFRUESISP**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Bashkësi rregullash që përcaktojnë si transmetohen të dhënat nëpër rrjet.
2. Kufizim që parandalon qasjen në ueb sipas vendndodhjes fizike.
3. Sistem sigurie që monitoron dhe bllokon trafikun e paautorizuar.
4. Gjendja e lirisë nga gjurmimi ose survejimi publik.
5. Ofruesi i shërbimit të internetit, i cili regjistron trafikun tënd nëse nuk është i enkriptuar.
6. Mbështjellja e paketave të të dhënave brenda një pakete tjetër për tranzit të sigurt.
7. Kompjuter i largët që rrugëzon trafikun tënd dhe maskon IP-në tënde.
8. Shpejtësia maksimale e transferimit të të dhënave nëpër një lidhje.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të VPN-së. Shkruaji përgjigjet në kutitë e plotësueshme.

1. EITLMNU
2. EJËSGNDEBAIR
3. GLLOEJIMBKO
4. AISVËTPRI
5. OORLKTPLO
6. EVSRRE
7. FLWALIER
8. PESOUFSIR

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Gjëra që mund të zbulojë një adresë IP			
2	Mite për VPN-të			
3	Gjëra që udhëtojnë nëpër internet			
4	Premtime që jep një ofrues i mirë VPN			
5	Sekrete që do t'i enkriptoje			
6	Gjëra nga të cilat një VPN nuk mund të të mbrojë			
7	Mënyra për të dalluar një rrjet Wi-Fi të rremë			
8	Fjalë që lidhen me privatësinë			
9	Pajisje që mund të përdorin një VPN			
10	Gjëra që ndodhin kur shtyp 'Lidhu'			
11	Vende ku do të përdorje një VPN			
12	Arsye për të përdorur një VPN gjatë udhëtimit			
13	Gjëra të jetës reale që duken si një tunel			
14	Fjalë nga kjo fletë pune që dëshiron t'i mbash mend			
15	Fjalë për t'i shpjeguar një fëmije çfarë është një VPN			

Pika e kontrollit 8: Studime rasti për VPN-në

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

SARAH (STUDENTJA NË KAFENE)

👩‍💻 "Hej! Jam ulur te Coffee & Bytes. Ka një rrjet publik të pasigurt me emrin 'Free_Wi-Fi_No_Password'. Dua të hyj në emailin e shkollës dhe të ngarkoj detyrën, por kam frikë nga hakerët. Cilat janë rreziqet e përdorimit të këtij rrjeti pa VPN, dhe si i siguron një VPN të dhënat e mia?"

ALEX (STUDENT UDHËTAR)

👩‍💻 "Ç'fatkeqësi! Jam duke udhëtuar jashtë shtetit për një projekt dhe po provoj të shoh një dokumentar biologjie të strehuar në një server në vendin tim. Por faqja thotë 'Ky video nuk është i disponueshëm në vendndodhjen tënde aktuale.' Pse jam i bllokuar, dhe si mund të më ndihmojë një VPN ta shoh?"

Pika e kontrollit 9: Deshifrimi i kodit

Një VPN enkripton trafikun tënd për ta siguruar. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin e sigurisë kibernetike duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

15	2	20	17	12		18	20	11	24	1	22	7	21	11	16	7
22	7	16	5	6		15	6		16	12	7		22	23	16	6	14		22	7
						21	11	9	23	20	22									

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për VPN-në (Pjesa A)

Rishiko pyetjet dhe përgjigjet më të zakonshme që kanë klientët e mundshëm për përdorimin e rrjeteve private virtuale.

Q1: Çfarë është një VPN dhe si funksionon?

Një Rrjet Privat Virtual (VPN) enkripton lidhjen tënde të internetit dhe e drejton trafikun tënd përmes një serveri të sigurt të largët. Kjo maskon adresën tënde publike IP dhe kufizon atë që vëzhguesit e rrjetit lokal dhe ISP-ja jote mund të shohin për trafikun e drejtuar përmes tunelit të VPN-së.

Q2: Pse duhet të përdor një VPN?

Një VPN mbron privatësinë tënde dixhitale, siguron lidhjen tënde në rrjete Wi-Fi publike (si kafenetë ose aeroportet), mund të zvogëlojë ngadalësimin e bazuar në aktivitet kur ISP-ja nuk mund ta identifikojë llojin e trafikut të enkriptuar, anashkalon kufizimet gjeografike për të hyrë në përmbajtje globale dhe ndihmon në sigurimin e burimeve të punës në distancë.

Q3: A më bën një VPN plotësisht anonim në internet?

Jo. Ndërsa një VPN e fsheh adresën tënde IP dhe enkripton trafikun, mund të gjurmohesh ende përmes cookie-ve të shfletuesit, llogarive aktive (si Google ose Facebook), fingerprinting-ut të shfletuesit, ose nëse ofruesi yt VPN regjistron të dhënat e tua.

Q4: A do ta ngadalësojë një VPN shpejtësinë e internetit tim?

Po, pak. Procesi i enkriptimit dhe distanca fizike deri te serveri VPN shtojnë vonesë dhe ngarkesë shtesë. Ndikimi ndryshon sipas ofruesit, protokollit, distancës së serverit, pajisjes dhe kushteve të rrjetit.

Q5: A është e ligjshme përdorimi i një VPN-je?

Përdorimi i VPN-së është i ligjshëm në shumë vende, por disa juridiksione i kufizojnë, i rregullojnë ose i bllokojnë shërbimet VPN. Përdoruesit duhet të verifikojnë ligjet aktuale lokale para përdorimit. Për më shumë detaje, konsulto udhëzuesit e ligjshmërisë në VPN.com.

Pika e kontrollit 10: Pyetje të shpeshta bazë për VPN-në (Pjesa B)

Rishiko pyetjet dhe përgjigjet më të zakonshme që kanë klientët e mundshëm për përdorimin e rrjeteve private virtuale.

Q6: A mund të përdor një VPN falas?

VPN-të falas mund të mbështeten te reklamat, veçoritë e kufizuara, analitika e përdorimit, kufijtë e të dhënave ose modele të tjera monetizimi. Përdoruesit duhet të shqyrtojnë politikën e privatësisë, pronësinë, auditimet dhe modelin e biznesit të ofruesit përpara përdorimit.

Q7: Çfarë është një politikë "no-logs"?

Një politikë no-logs përshkruan cilat të dhëna aktiviteti dhe lidhjeje thotë një ofrues se nuk i ruan. Shtrirja e saktë ndryshon, ndaj lexuesit duhet të shqyrtojnë politikën dhe gjetjet e auditimeve të pavarura.

Q8: Si ta zgjedh VPN-në më të mirë?

Kërko politika no-logs të audituara, protokolle të forta (WireGuard, OpenVPN), vendndodhje të sigurta serverësh, shpejtësi të larta, serverë vetëm me RAM, funksion kill switch dhe juridiksion jashtë aleancave të ndarjes së inteligjencës (si 5/9/14 Eyes).

Q9: A mund ta përdor një VPN në telefonin dhe televizorin tim smart?

Po. Ofruesit modernë të VPN-ve ofrojnë aplikacione të dedikuara për iOS, Android, macOS, Windows, Linux dhe televizorë inteligjentë, si dhe konfigurime në ruter për të mbrojtur të gjitha pajisjet në rrjetin e shtëpisë sate.

Q10: Çfarë është një Kill Switch?

Kill Switch është një veçori sigurie që e shkëput automatikisht pajisjen tënde nga interneti nëse lidhja VPN bie. Kjo parandalon rrjedhjen e të dhënave të tua të pa enkriptuara ose të adresës reale IP.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për VPN-në (Pjesa C)

Eksploro aspektet teknike dhe strukturore të rrjeteve private virtuale dhe të protokolleve të sigurta të tunelimit.

Q1: Cili është ndryshimi midis WireGuard, OpenVPN dhe IKEv2?

WireGuard është një protokoll modern dhe i lehtë (vetëm ~4,000 rreshta kodi) që ofron shpejtësi të larta dhe kohë të shpejta lidhjeje. OpenVPN është një protokoll me kod të hapur shumë i sigurt dhe i provuar. IKEv2 është i shkëlqyer për pajisjet celulare falë aftësisë për t'u rilidhur shpejt kur ndërrohen rrjetet. [4]

Q2: Çfarë është rrugëzimi double VPN ose Multi-Hop?

Multi-Hop e rutuon trafikun tënd nëpër dy ose më shumë serverë VPN në sekuencë. Kjo shton një shtresë të dytë enkriptimi dhe ndihmon ta mbajë të fshehur adresën tënde të vërtetë IP nga hop-i i dytë nëse një server kompromentohet.

Q3: Çfarë është rrjedhja e WebRTC dhe si e parandalon një VPN?

WebRTC është një protokoll i shfletuesit që mund të zbulojë adresat e tua reale IP lokale dhe publike edhe kur një VPN është aktive. VPN-të premium bllokojnë ose falsifikojnë kërkesat WebRTC në aplikacionet e tyre për desktop/celular dhe në shtesat e shfletuesit.

Q4: Çfarë janë serverët vetëm me RAM dhe pse kanë rëndësi?

Serverët tradicionalë i shkruajnë të dhënat në disqet e ngurtë, të cilët mund të konfiskohen ose kompromentohen. Serverët vetëm me RAM (pa disk) funksionojnë tërësisht në memorie të paqëndrueshme (RAM). Kur serveri riniset ose fiket, të dhënat e mbajtura në memorie fshihen.

Q5: Si i anashkalon Obfuscation bllokimet e VPN-ve?

Maskimi (obfuscation, ose "Stealth VPN") e shndërron trafikun VPN që të duket si trafik i zakonshëm HTTPS (porti 443). Kjo mund ta ndihmojë të kalojë Inspektimin e Thellë të Paketave (DPI) që përdorin qeveritë ose rrjetet e shkollave/zyrave për të bllokuar VPN-të.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për VPN-në (Pjesa D)

Eksploro aspektet teknike dhe strukturore të rrjeteve private virtuale dhe të protokolleve të sigurta të tunelimit.

Q6: Çfarë është Split Tunneling dhe kur duhet ta përdor?

Split Tunneling të lejon të zgjedhësh cilat aplikacione rrugëzohen përmes tunelit të enkriptuar VPN dhe cilat lidhen drejtpërdrejt me internetin. Përdore për të drejtuar aplikacionet e ndjeshme bankare përmes VPN-së, ndërsa lojërat lokale lidhen drejtpërdrejt, duke shmangur vonesën e shtuar nga VPN-ja.

Q7: Si funksionon Forward Secrecy (Perfect Forward Secrecy)?

PFS siguron që për çdo seancë të krijohet një çelës enkriptimi unik e i përkohshëm. Edhe nëse një çelës privat kompromentohet në të ardhmen, ai nuk mund të përdoret për të deshifruar seancat e kaluara ose të ardhshme, sepse ato përdorën çelësa të pavarur.

Q8: Çfarë janë aleancat 5/9/14 Eyes dhe pse duhet të më interesojnë?

Juridiksioni mund të ndikojë në procesin ligjor me të cilin përballet një ofrues, por rreziku praktik i privatësisë varet edhe nga të dhënat që ruan ofruesi, arkitektura e tij teknike, pronësia, raportimi i transparencës dhe historiku i auditimeve.

Q9: Çfarë është mbrojtja nga rrjedhjet e DNS-së?

Mbrojtja nga rrjedhjet e DNS e detyron pajisjen tënde t'i dërgojë kërkesat e kërkimit të faqeve të internetit (kërkesat DNS) nëpërmjet serverëve DNS privatë dhe të enkriptuar të VPN-së, në vend të serverëve të ISP-së sate. Kjo e pengon ISP-në tënde të gjurmojë se cilat faqe vizitoni.

Q10: A mund ta kapërcejë një VPN ngadalësimin e internetit nga ISP-ja?

Ndonjëherë. Një VPN mund të ndihmojë kur një ISP ngadalëson në mënyrë selektive veprimtari të identifikueshme, por nuk do ta kapërcejë mbingarkesën, kufijtë e të dhënave, kufizimet e shpejtësisë në nivel llogarie ose cilësinë e dobët të rrjetit.

Pjesa 11: 10 fakte interesante për VPN-të dhe njohuri nga bota reale

Rishiko këto fakte dhe njohuri reale shumë të vlefshme për historinë, tregun dhe teknologjinë e VPN-ve.

1. PROTOKOLLI I PARË VPN

PPTP (Point-to-Point Tunneling Protocol) u zhvillua nga një grup shitësish përfshirë Microsoft dhe u publikua si RFC 2637 në korrik 1999 për të mbështetur VPN-të e qasjes në distancë. [6]

2. VLERËSIMI I TREGUT

Tregu global i VPN-ve ka përjetuar rritje të shpejtë, të nxitur nga kërkesat në rritje për punë në distancë dhe nevojat e sigurisë së ndërmarrjeve.

3. REVOLUCIONI WIREGUARD

WireGuard ka një bazë kodi shumë të thjeshtuar, të projektuar për efikasitet, që e bën më të lehtë për t'u audituar për cenueshmëri sigurie se protokollet tradicionale. [4]

4. STANDARDE TË RREPTA AUDITIMI

Ofruesit kryesorë të VPN-ve punësojnë audituesa të jashtëm (si Cure53 ose PwC) për të kryer rishikime të pavarura të kodit dhe për të verifikuar se nuk regjistrojnë asnjë aktivitet të përdoruesve.

5. ORIGJINA E ALEANCËS 5-EYES

Aleanca Five Eyes u zhvillua nga marrëveshja e vitit 1946 UKUSA për inteligjencën e sinjaleve mes SHBA-së dhe Mbretërisë së Bashkuar, të cilës më vonë iu bashkuan Kanadaja, Australia dhe Zelanda e Re.

6. INSPEKTIMI I THELLË I PAKETAVE

Inspektimi i thellë i paketave (DPI) shqyrton përmbajtjen e paketave dhe modelet e trafikut, jo vetëm kokat, dhe disa firewall-e e përdorin për të zbuluar dhe bllokuar protokollet e zakonshme të VPN-së.

7. PËRDORIMI KORPORATIV

Një përqindje e madhe e punonjësve të ndërmarrjeve në mbarë botën përdorin VPN të sigurta për t'u identifikuar në baza të dhënash të brendshme, çka e bën një standard kyç sigurie.

8. VPN-TË TË DECENTRALIZUARA

VPN-të e decentralizuara (dVPN) e shpërndajnë trafikun nëpër një rrjet nyjesh të drejtuara nga bashkëveta (peer), duke zvogëluar varësinë nga një ofrues i vetëm i centralizuar.

9. ANONIMITETI I TOR KUNDRAS VPN-SË

Një VPN e tunelon trafikun përmes një ofruesi të vetëm, ndërsa Tor (The Onion Router) e dërgon trafikun përmes tre releve vullnetare (guard, middle dhe exit), ndaj asnjë rele i vetëm nuk i njeh të dy skajet.

10. KOSTOJA E SHKELJEVE TË TË DHËNAVE

Përdorimi i një modeli qasjeje të sigurt zero-trust me një VPN ndihmon organizatat të mbrojnë pronësinë intelektuale dhe të zbusin ndikimin financiar të shkeljeve të të dhënave.

Referenca teknike dhe burime

Botime të cituara, specifikime kriptografike dhe standarde zyrtare dokumentesh të përdorura në këtë fletë pune.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[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

Çelësi i përgjigjeve: Fletë pune "Çfarë është një VPN"

1 **Funksioni kryesor** PROTOKOLLE — **Përgjigjja e saktë: B**

SHËNIM PËR MËSUESIN

Detyra kryesore e një VPN-je është të krijojë një tunel të enkriptuar që mbron të dhënat e ngarkesës së paketave dhe maskon IP-në publike të përdoruesit. Citim: IETF Tunnel RFC.

2 **Tunelimi i rrjetit** VONESA — **Përgjigjja e saktë: D**

SHËNIM PËR MËSUESIN

Protokollet e tunelimit i përmbledhin paketat origjinale të të dhënave brenda paketave të jashtme bartëse për të kaluar me siguri nëpër rrjetet publike. Citim: IETF Tunnel RFC.

3 **Pyetja 3** — **Përgjigjja e saktë: B**

SHËNIM PËR MËSUESIN

Cili standard enkriptimi përdoret gjerësisht për të mbrojtur trafikun VPN? → Standardi modern AES-256

4 **Komponentët e enkriptuar** KONTROLLET E RUTERIMIT — **Përgjigjja e saktë: C**

SHËNIM PËR MËSUESIN

Një VPN enkripton segmentin e plotë të ngarkesës së paketave të të dhënave IP, duke e mbajtur konfidenciale përmbajtjen e transmetimit. Citim: IETF Tunnel RFC.

5 **Pyetja 5** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Enkriptimi përdor një algoritëm dhe një çelës për ta kthyer tekstin e thjeshtë në tekst të shifruar të palexueshëm.

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Bllokimi i përgjimit** MASKIMI I IP-SË **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Tunelet e enkriptuara sigurojnë që ngarkesat e paketave të mbeten të palexueshme për aktorët që përgjojnë të dhënat në rrjetet lokale Wi-Fi. Citim: Deloitte Advisory.

7 **Ndryshimet e harduerit** SHPEJTËSITË **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

VPN-të janë tunele rrjeti të bazuara në softuer dhe nuk e modifikojnë fizikisht harduerin e ruterit tënd portë. Citim: Cure53 Audit.

8 **Paketat e tunelimit** RREZIKU I PËRGJIMIT **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Tunelimi funksionon duke i mbështjellë paketat origjinale të rrjetit brenda kokave të transportit për tranzit. Citim: IETF Tunnel RFC.

9 **Çelësat simetrikë** FIREWALL-E **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Kriptografia simetrike përdor një çelës të përbashkët si për enkriptimin, ashtu edhe për dekriptimin e rrjedhave të rrjetit. Burimi: WireGuard Project.

10 **Imuniteti i fuqisë** PA REGJISTRA **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Një VPN enkripton vetëm sinjalet aktive të lidhjes; nuk mund të parandalojë ndërprerjet e shërbimit të shkaktuara nga ndërprerjet lokale të energjisë. Citim: EDRi Retention Guidelines.

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

H 1. Tunelimi	E 2. Protokolli	G 3. Gjerësia e brezit	A 4. Serveri
C 5. Bllokimi gjeografik	D 6. Firewall	F 7. Privatësia	B 8. ISP

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 TUNELIM	2 GJERËSI BANDE	3 GJEOBLLOKIM	4 PROTOKOLL
5 FIREWALL	6 SERVER		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 B – PROTOKOLL	2 E – GJEOBLLOKIM	3 F – FIREWALL	4 G – PRIVATËSI
5 H – OFRUESISP	6 A – TUNELIM	7 D – SERVER	8 C – GJERËSIBANDE

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë Tunelimi, Protokolli dhe Gjerësia e brezit me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

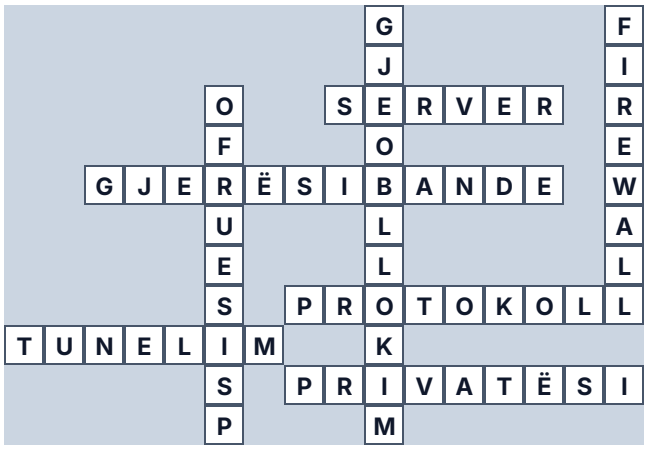
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

4 horizontalisht: SERVER Kompjuter i largët që rrugëzon trafikun tënd dhe maskon IP-në tënde (6 shkronja)

5 horizontalisht: GJERËSIBANDE Shpejtësia maksimale e transferimit të të dhënave nëpër një lidhje (12 shkronja)

6 horizontalisht: PROTOKOLL Bashkësi rregullash që përcaktojnë si transmetohen të dhënat nëpër rrjet (9 shkronja)

7 horizontalisht: TUNELIM Mbështjellja e paketave të të dhënave brenda një pakete tjetër për tranzit të sigurt (7 shkronja)

8 horizontalisht: PRIVATËSI Gjendja e lirisë nga gjurmimi ose survejimi publik (9 shkronja)

VERTIKALISHT

1 vertikalisht: GJEOBLLOKIM Kufizim që parandalon qasjen në ueb sipas vendndodhjes fizike (11 shkronja)

2 vertikalisht: FIREWALL Sistem sigurie që monitoron dhe bllokon trafikun e paautorizuar (8 shkronja)

3 vertikalisht: OFRUESISP Ofruesi i shërbimit të internetit, i cili regjistron trafikun tënd nëse nuk është i enkriptuar (9 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1. EITLMNU — **TUNELIM**
2. EJËSGNDEBAIR — **GJERËSIBANDE**
3. GLLOEJIMBKO — **GJEOBLLOKIM**
4. AISVËTPRI — **PRIVATËSI**
5. OORLKTPLO — **PROTOKOLL**
6. EVSRRE — **SERVER**
7. FLWALIER — **FIREWALL**
8. PESOUFSIR — **OFRUESISP**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"MBROJ PRIVATËSINË TËNDE ME NJË TUNEL TË SIGURT"

Çelësi i studimeve të rastit

A Skenari A: Siguria në rrjete publike

PËRGJIMI DHE ENKRIPTIMI | Dilema e Sarës

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Rreziqet: Përgjimi i paketave, përgjimi i të dhënave dhe sulmet man-in-the-middle. Dikush në të njëjtin rrjet të kafenesë mund të kapte detajet e hyrjes ose skedarin e detyrave të saj.
- Mbrojtja e VPN-së: Enkripton ngarkesat e paketave të rrjetit, duke e bërë trafikun e përgjuar të tunelit të palexueshëm për përgjuesit pasivë të rrjetit lokal kur VPN-ja është konfiguruar saktë.

B Skenari B: Qasja te burimet e bllokuara

BLLOKIMI GJEOGRAFIK DHE IP-TË | Dilema e Alexit

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Pse u bllokua: Hosti i transmetimit përdor gjeobllokimin, që e lidh adresën lokale IP të udhëtarit me shtetin e tij fizik dhe e bllokon sipas licencimit territorial.
- Si ndihmon VPN-ja: Maskon vendndodhjen e tij reale duke rrugëzuar trafikun përmes një serveri në vendin e tij. Faqja shikon IP-në e vendit të tij dhe lejon qasjen.