Emri: _____ Data: _____ Pikët: _____

Udhëzuesi i VPN-së më të sigurt

Analizë teknike e dizajnit të VPN-së me siguri të lartë, serverët me memorie të paqëndrueshme vetëm me RAM, sigurinë e qasjes Zero Trust, mbrojtjet private të enkriptuara nga rrjedhjet e DNS-së dhe konfigurimet e audituara WireGuard.

PËRMBLEDHJE MËSIMORE PËR UDHËZUESIN E VPN-SË MË TË SIGURT

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 standardeve teknike të VPN-ve shumë të sigurta. Do të eksplorosh harduerin e serverëve vetëm me RAM, sigurinë e qasjes Zero Trust, zgjidhësit privatë të enkriptuar të DNS-së dhe konfigurimet e audituara të WireGuard.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro konfigurimet e VPN-së dhe të sigurisë së rrjetit.**
- [ ] **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-të më të mira

URL: https://www.vpn.com/sq/vpn/vpn-me-i-sigurt/

Udhërrëfyesi yt mësimor për VPN-në më të sigurt

- Analizo arkitekturën teknike dhe standardet e enkriptimit në udhëzuesin Most Secure VPN.
- Konfiguro cilësimet e klientit për të parandaluar rrjedhjet e trafikut IP, DNS dhe WebRTC.
- Krahaso protokollet pronësore të tunelimit me zbatimet standarde.

UDHËZIME PËR UDHËZUESIN E VPN-SË MË TË SIGURT

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 harduerin e serverëve vetëm me RAM dhe sistemet Zero Trust. Përfundo me aktivitetin bonus Mendo shpejt.

INFRASTRUKTURAT VETËM ME RAM DHE RRJETET ZERO TRUST (HYRJE)

Një VPN vërtet e sigurt mbështetet në një kornizë zero trust, serverë vetëm me RAM për të parandaluar që konfiskimet e disqeve të ekspozojnë regjistra, resolver-ë privatë të enkriptuar DNS dhe protokolle të audituara si WireGuard. Këto kontrolle të kombinuara mbrojnë asetet dixhitale me vlerë të lartë nga kërcënimet e përgjimit.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Cila arkitekturë është thelbësore për të garantuar sigurinë më të lartë brenda serverëve modernë të VPN-së?**

- A) Infrastrukturë serverësh vetëm me RAM
- B) Ruajtje e bazuar në disk
- C) Rrugëzim dinamik DNS
- D) Aktivizimi i përcjelljes së porteve

2 **2. Cili protokoll rekomandohet gjerësisht për konfigurimet VPN më të sigurta dhe më moderne?**

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3 **3. Cili kuadër sigurie kërkon verifikimin e vazhdueshëm të çdo lidhjeje pa përjashtim?**

- A) Arkitektura Zero Trust
- B) Firewall-e perimetri
- C) Rrugëzim dinamik
- D) Çelësa të fshehtë të përbashkët

4 **4. Cili është roli kryesor i mbrojtjes nga rrjedhjet DNS të një klienti VPN?**

- A) Drejto të gjitha kërkesat DNS përmes resolver-ëve privatë të enkriptuar
- B) Errëson paketat IP
- C) Ruajtja lokale në cache e kërkesave DNS
- D) Çaktivizo serverët e emrave

5 **5. Si e rrit rrugëzimi Multi-Hop sigurinë e përgjithshme të një tuneli VPN?**

- A) Drejton të dhënat përmes dy serverëve të veçantë në seri
- B) Rrit shpejtësinë e kompresimit
- C) Enkripton të dhënat me shifra me siguri të ulët
- D) Anashkalon firewall-et

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

6 Pyetja 6

6. Serverët vetëm me RAM i ruajnë skedarët e regjistrit në memorie të përkohshme, e cila fshihet gjatë rinisjes.

- ○ E vërtetë
- ○ E gabuar

7 Pyetja 7

7. WireGuard përdor algoritme kriptografike moderne që janë më pak të cenueshme ndaj ngushticave të shpejtësisë.

- ○ E vërtetë
- ○ E gabuar

8 Pyetja 8

8. Një kill switch i VPN-së funksionon duke bllokuar gjithë trafikun e rrjetit nëse tuneli bie.

- ○ E vërtetë
- ○ E gabuar

9 Pyetja 9

9. Auditimet e pavarura të palëve të treta nuk kanë lidhje me verifikimin e angazhimeve të sigurisë.

- ○ E vërtetë
- ○ E gabuar

10 Pyetja 10

10. Modelet Zero Trust supozojnë se të gjitha lidhjet e brendshme të rrjetit janë të sigurta si parazgjedhje.

- ○ 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. Administratorët zbatojnë sigurinë duke vendosur një kuadër të rreptë _____ .

2. Rrugëzimi i paketave përmes pikave të shumta hyrëse kërkon një konfigurim të sigurt _____ .

3. Për të parandaluar rrjedhjet e të dhënave nga disqet e vjedhura, përdorim një dizajn _____ .

4. Rrëmbimi nga ISP zbutet duke konfiguruar veçoritë vendase për _____ .

5. Për të bllokuar trafikun gjatë dështimeve të lidhjes, aktivizo mekanizmin _____ .

6. Për të minimizuar regjistrat e ruajtur në bazë të dhënash, zgjidh një ofrues plotësisht të _____ .

BANKA E FJALËVE TË LEKSIKUT

AUDITUAR ENKRIPTIM KILL SWITCH MBROJTJE DNS MULTI-HOP PROTOKOLL SERVER VETËM RAM ZERO TRUST

Shkruaj përgjigjet e tua këtu:

1. 2.

3. 4.

5. 6.

Pika e kontrollit 4: Përputhja e koncepteve të VPN-së dhe rrjetit

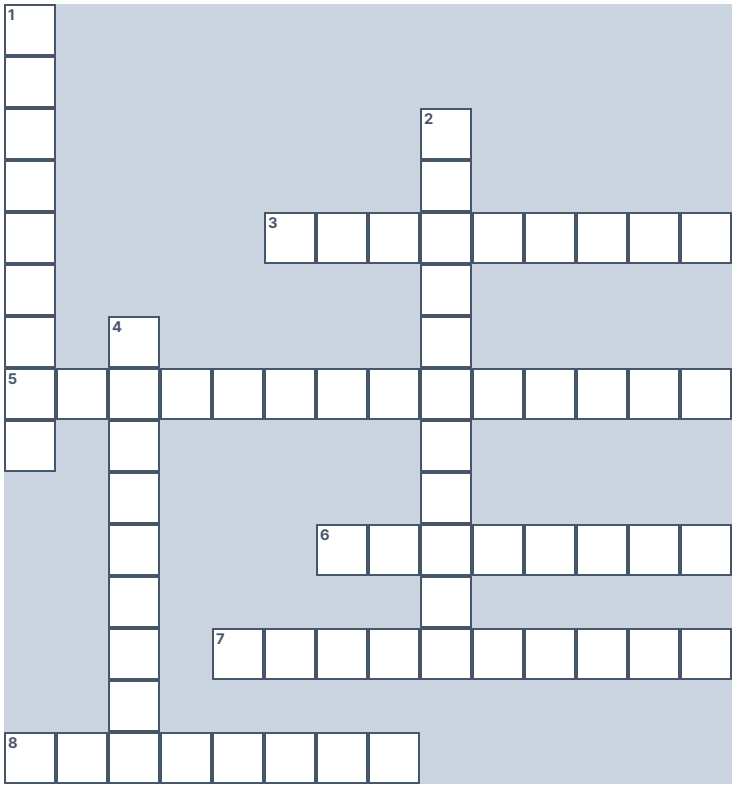
PËRPUTHJA E PËRKUFIZIMEVE

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. Zero Trust	A	Konfigurim i inspektuar në mënyrë të pavarur që konfirmon se nuk ruhet asnjë regjistër.
☐	2. Multi-Hop	B	Përzierja kriptografike e ngarkesave të të dhënave për të siguruar transitin.
☐	3. Server vetëm me RAM	C	Kornizë sigurie që kërkon autentikim të vazhdueshëm të të gjithë përdoruesve.
☐	4. Mbrojtja e DNS	D	Bashkësi rregullash teknike që përcaktojnë se si paketohen dhe dërgohen të dhënat.
☐	5. Kill switch	E	Rutim VPN në kaskadë që lidh dy nyje serverësh në zinxhir.
☐	6. Sistem i audituar	F	Arkitekturë serveri që përdor memorie të paqëndrueshme për të ruajtur ngarkesat e të dhënave.
☐	7. Enkriptimi	G	Zbatimi i kërkesave DNS private për të mbrojtur kërkimet e serverëve të emrave.
☐	8. Protokolli	H	Mekanizëm i sigurt në rast dështimi që bllokon trafikun nëse VPN-ja dështon.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

3. Përzierje kriptografike e ngarkesave të të dhënave për të siguruar tranzitin (9)

5. Arkitekturë serveri që përdor memorie të paqëndrueshme për të ruajtur ngarkesat e të dhënave (14)

6. Konfigurim i inspektuar në mënyrë të pavarur që konfirmon se nuk ruhen regjistra (8)

7. Mekanizëm mbrojtës që bllokon trafikun nëse VPN-ja dështon (10)

8. Rrugëzim VPN në kaskadë që lidh së bashku dy nyje serveri (8)

VERTIKALISHT

1. Kuadër sigurie që kërkon autentikim të vazhdueshëm të të gjithë përdoruesve (9)

2. Zbatimi i pyetjeve private DNS për të mbrojtur kërkimet e serverëve të emrave (11)

4. Bashkësi rregullash teknike që përcaktojnë si paketohen dhe dërgohen të dhënat (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

3 horizontalisht: Përzierje kriptografike e ngarkesave të të dhënave për të siguruar tranzitin (9 shkronja):

5 horizontalisht: Arkitekturë serveri që përdor memorie të paqëndrueshme për të ruajtur ngarkesat e të dhënave (14 shkronja):

6 horizontalisht: Konfigurim i inspektuar në mënyrë të pavarur që konfirmon se nuk ruhen regjistra (8 shkronja):

7 horizontalisht: Mekanizëm mbrojtës që bllokon trafikun nëse VPN-ja dështon (10 shkronja):

8 horizontalisht: Rrugëzim VPN në kaskadë që lidh së bashku dy nyje serveri (8 shkronja):

VERTIKALISHT

1 vertikalisht: Kuadër sigurie që kërkon autentikim të vazhdueshëm të të gjithë përdoruesve (9 shkronja):

2 vertikalisht: Zbatimi i pyetjeve private DNS për të mbrojtur kërkimet e serverëve të emrave (11 shkronja):

4 vertikalisht: Bashkësi rregullash teknike që përcaktojnë si paketohen dhe dërgohen të dhënat (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.

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

LISTA E FJALËVE TË LEKSIKUT

ZEROTRUST MULTIHOP SERVERVETËMRAM MBROJTJEDNS KILLSWITCH
AUDITUAR ENKRIPTIM PROTOKOLL

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. ZEROTRUST**
- **B. MULTIHOP**
- **C. SERVERVETËMRAM**
- **D. MBROJTJEDNS**
- **E. KILLSWITCH**
- **F. AUDITUAR**
- **G. ENKRIPTIM**
- **H. PROTOKOLL**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Mekanizëm mbrojtës që bllokon trafikun nëse VPN-ja dështon.
2. Zbatimi i pyetjeve private DNS për të mbrojtur kërkimet e serverëve të emrave.
3. Rrugëzim VPN në kaskadë që lidh së bashku dy nyje serveri.
4. Bashkësi rregullash teknike që përcaktojnë si paketohen dhe dërgohen të dhënat.
5. Përzierje kriptografike e ngarkesave të të dhënave për të siguruar tranzitin.
6. Arkitekturë serveri që përdor memorie të paqëndrueshme për të ruajtur ngarkesat e të dhënave.
7. Konfigurim i inspektuar në mënyrë të pavarur që konfirmon se nuk ruhen regjistra.
8. Kuadër sigurie që kërkon autentikim të vazhdueshëm të të gjithë përdoruesve.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të rrjetit privat virtual (VPN). Shkruaji përgjigjet në kutitë e dhëna.

1. **RTOEZUSTR** _____
2. **EERRVASREMËMTV** _____
3. **KWCIISHLTL** _____
4. **IMIRTPENK** _____
5. **IHUPTMOL** _____
6. **JSTENDMBJRO** _____
7. **ARTUAUID** _____
8. **LOLPTRKOO** _____

Aktivitet bonus: Mendo shpejt

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

1	Brava ose çelësa që përdor çdo ditë			
2	Gjëra që mund t'i fshehë një VPN			
3	Gjëra që e bëjnë një VPN të sigurt			
4	Mite për VPN-të			
5	Arsye për të përdorur një VPN gjatë udhëtimit			
6	Vende të sigurta në botën reale			
7	Fjalë që nënkuptojnë 'i mbrojtur'			
8	Premtime që jep një ofrues i mirë VPN			
9	Fjalë që lidhen me privatësinë			
10	Lloje auditimi ose inspektimi			
11	Fjalë nga kjo fletë pune që dëshiron t'i mbash mend			
12	Gjëra që dëshiron të vjedhë një haker			
13	Mënyra për të dalluar një rrjet Wi-Fi të rremë			
14	Vende ku do të përdorje një VPN			
15	Gjëra që mund të shohë ofruesi yt i internetit			

Pika e kontrollit 8: Studime rasti për VPN-në dhe rrjetin

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

STUDIMI I RASTIT 1: FORCIMI I INFRASTRUKTURËS SË NDËRMARRJES



Skenari: Një bankë korporative po ridizajnon topologjinë e saj të qasjes në distancë. Ajo kërkon një arkitekturë zero trust që i lidh të gjitha pajisjet klient me serverë të sigurt.

Pyetje për diskutim: Cili është përfitimi kryesor i mikrosegmentimit të rrjetit nën një model VPN Zero Trust?

STUDIMI I RASTIT 2: MBROJTJET E SERVERËVE VETËM ME RAM



Skenari: Një ofrues VPN i fokusuar te siguria po përmirëson serverët e tij për të parandaluar që marrja fizike e serverëve të ekspozojë historitë e regjistrave të përdoruesve.

Pyetje për diskutim: Shpjego si e parandalojnë konfigurimet e harduerit vetëm me RAM nxjerrjen forenzike të të dhënave gjatë marrjes fizike të serverëve.

Pika e kontrollit 9: Deshifrimi i kodit

Një inxhinier rrjeti siguron kanalet e drejtimit dhe tunelet e klientëve. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin 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

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

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 për Rrjetet Private Virtuale (VPN) dhe tunelimin.

Q1: Çfarë e bën një VPN 'më të sigurt'?

Një kombinim i Zero Trust, serverëve vetëm me RAM dhe protokolleve të audituara.

Q2: Çfarë janë serverët vetëm me RAM?

Serverë që funksionojnë në memorie të paqëndrueshme, të projektuar të mos ruajnë regjistra në disk.

Q3: Çfarë është një VPN Zero Trust?

Një kornizë që verifikon vazhdimisht çdo kërkesë qasjeje dhe çdo lidhje.

Q4: Pse konsiderohet i sigurt WireGuard?

Ka një bazë kodi të vogël, lehtësisht të audituesshme dhe përdor shifra moderne.

Q5: Si i parandalojnë VPN-të e sigurta rrjedhjet e DNS-së?

Duke rrugëzuar të gjitha kërkesat përmes zgjidhësve privatë të enkriptuar DNS.

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

Rishiko pyetjet dhe përgjigjet më të zakonshme për Rrjetet Private Virtuale (VPN) dhe tunelimin.

Q6: A kërkon një VPN i sigurt auditime?

Po, auditimet e pavarura verifikojnë pretendimet për zero regjistra dhe sigurinë e kodit.

Q7: Cili është roli i një kill switch?

Ndalon menjëherë trafikun e rrjetit nëse lidhja VPN ndërpritet.

Q8: Çfarë enkriptimi përdoret në VPN-të e sigurta?

AES-256 dhe ChaCha20 janë standardet e industrisë për enkriptim.

Q9: A është i sigurt ruterimi Multi-Hop?

Po, ai lidh në zinxhir dy ose më shumë serverë për të parandaluar analizën e trafikut.

Q10: Si ndihmon juridiksioni offshore?

Mund të kufizojë cilat ligje zbatohen, por nuk ofron imunitet absolut.

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

Eksploro aspektet e avancuara teknike të protokolleve të tunelimit të VPN-ve, integrimeve të klientëve mobil dhe zbatimit në ndërmarrje.

Q1: Si i parandalojnë serverët vetëm me RAM rreziqet e konfiskimit të të dhënave?

Sepse funksionojnë në RAM, heqja e prizës fshin të dhënat e mbajtura në memorie.

Q2: Si e zëvendëson Zero Trust sigurinë standarde të perimetrit?

Çdo klient e trajton si armiqësor, duke kërkuar autentikim të vazhdueshëm.

Q3: Çfarë e bën kodin e WireGuard më të lehtë për t'u audituar?

Kodi i tij për Linux është nën 4,000 rreshta, shumë më i vogël se paketat tipike VPN. [4]

Q4: Si i mbron DNSSEC kërkesat DNS?

Nënshkruan regjistrat DNS që zgjidhësit të mund të zbulojnë përgjigje të falsifikuara ose të manipuluara.

Q5: Si e ndërlikon Multi-Hop korrelacionin e trafikut?

Duke i ndarë IP-të hyrëse dhe dalëse në ofrues të ndryshëm hostimi.

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

Eksploro aspektet e avancuara teknike të protokolleve të tunelimit të VPN-ve, integrimeve të klientëve mobil dhe zbatimit në ndërmarrje.

Q6: Pse janë të rrezikshme për VPN-të juridiksionet e Five Eyes?

Shtetet anëtare ndajnë inteligjencë dhe mund të përdorin urdhra ligjorë për të kërkuar të dhëna të përdoruesve.

Q7: Si implementohet një kill switch në nivel kerneli?

Përdor rregulla firewall-i të sistemit (si iptables ose WFP) për të bllokuar egress-in.

Q8: Çfarë është forward secrecy në shtrëngimet e duarve të VPN-së?

Gjeneron çelësa unikë sesioni që sesionet e kaluara të mos mund të dekriptohen.

Q9: Si i zbusin VPN-të e sigurta rrjedhjet e WebRTC?

Duke bllokuar kërkesat WebRTC ose duke i rrugëzuar përmes tunelit.

Q10: Si e sigurojnë auditimet e pavarura pajtueshmërinë me privatësinë?

Audituesit kryejnë testime depërtimi dhe inspektojnë konfigurimet e serverit.

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

Rishiko fakte reale për shpejtësitë e enkriptimit të VPN-së, auditimet e protokolleve, lidhjen mobile dhe punën në distancë të ndërmarrjeve.

1. PERSPEKTIVË PËR VPN-NË

Serverët vetëm me RAM e ngarkojnë sistemin operativ në memorie gjatë ndezjes, ndaj asgjë nuk mbetet në disk pas rinisjes.

2. PERSPEKTIVË PËR VPN-NË

WireGuard përdor kornizën Noise me Curve25519, ChaCha20, Poly1305, BLAKE2s dhe HKDF. [3]

3. PERSPEKTIVË PËR VPN-NË

Zero Trust jep qasje për çdo burim dhe nuk jep besim të nënkuptuar bazuar në vendndodhjen në rrjet (NIST SP 800-207). [1]

4. PERSPEKTIVË PËR VPN-NË

Aleanca e inteligjencës Five Eyes përfshin SHBA-në, Mbretërinë e Bashkuar, Kanadanë, Australinë dhe Zelandën e Re.

5. PERSPEKTIVË PËR VPN-NË

Rrjedhjet WebRTC ndodhin kur shfletuesit zbulojnë IP-në reale publike të klientit përmes kërkesave STUN.

6. PERSPEKTIVË PËR VPN-NË

Perfect forward secrecy (PFS) siguron që kompromentimi i një çelësi afatgjatë nuk i ekspozon çelësat e seancave të kaluara. [3]

7. NJOHURI PËR VPN-NË

Cure53, një firmë sigurie me bazë në Berlin, ka botuar auditime për disa ofrues VPN.

8. NJOHURI PËR VPN-NË

Rrjedhjet e DNS ndodhin kur kërkesat DNS anashkalojnë tunelin e VPN-së dhe shkojnë te serverët e emrave të ISP-së lokale.

9. NJOHURI PËR VPN-NË

Çipat RAM të paqëndrueshëm kërkojnë energji elektrike të vazhdueshme për të ruajtur të dhënat dhe e humbasin përmbajtjen kur fiken.

10. PERSPEKTIVË PËR VPN-NË

Sistemet Zero Trust për ndërmarrje zbatojnë kontrolle të gjendjes së pajisjes para se të lejojnë lidhjen me burime të sigurta. [1]

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet teknike globale, specifikimet dhe kuadrot rregullatore.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Server vetëm me RAM** VETËM RAM — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Serverët vetëm me RAM nuk ruajnë regjistra në disk dhe i fshijnë të dhënat gjatë rinisjes. Citim: Most Secure VPN.

2 **Pyetja 2** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

WireGuard e çiftëzon një bazë kodi të vogël e të audituar me shifra moderne.

3 **Modeli Zero Trust** ZERO TRUST — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Modelet Zero Trust verifikojnë vazhdimisht përputhshmërinë e pajisjes para qasjes. Citim: Most Secure VPN.

4 **Mbrojtja e DNS** MBROJTJA E DNS — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Mbrojtja nga rrjedhjet e DNS i drejton kërkesat e kërkimit nëpërmjet zgjidhësve privatë. Citim: Most Secure VPN.

5 **Tunelet Multi-Hop** MULTI-HOP — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Rutimi Multi-Hop lidh në zinxhir dy nyje serverësh të veçanta në seri. Citim: Most Secure VPN.

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

6 **Server vetëm me RAM** VETËM RAM — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Hardueri i serverit vetëm me RAM nuk shkruan asnjë të dhënë në disk dhe fshihet gjatë rinisjes. Citim: Most Secure VPN.

7 **Shpejtësia e WireGuard** WIREGUARD — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

WireGuard përdor kriptografi moderne që shmang ngushticat e përpunimit. Citim: Most Secure VPN.

8 **Kill switch** NDËRPRERËS I SIGURISË — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Një kill switch i bllokon të gjithë trafikun nëse lidhja VPN bie. Citim: Most Secure VPN.

9 **Audite nga palë të treta** AUDITIMET JANË THELBËSORE — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Auditet nga palë të treta janë thelbësore për të verifikuar pretendimet e korporatave për privatësinë. Citim: Most Secure VPN.

10 **Pyetja 10** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Zero Trust nuk jep asnjë besim të nënkuptuar bazuar në vendndodhjen e rrjetit. [1]

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

C 1. Zero Trust	E 2. Multi-Hop	F 3. Server vetëm me RAM	G 4. Mbrojtja e DNS
H 5. Kill switch	A 6. Sistem i audituar	B 7. Enkriptimi	D 8. Protokolli

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 ZERO TRUST	2 MULTI-HOP	3 SERVER VETËM RAM	4 MBROJTJE DNS
5 KILL SWITCH	6 AUDITUAR		

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

1 E – KILLSWITCH	2 D – MBROJTJEDNS	3 B – MULTIHOP	4 H – PROTOKOLL
5 G – ENKRIPTIM	6 C – SERVERVETËMRAM	7 F – AUDITUAR	8 A – ZEROTRUST

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë Zero Trust, Multi-Hop dhe Server vetëm me RAM 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.

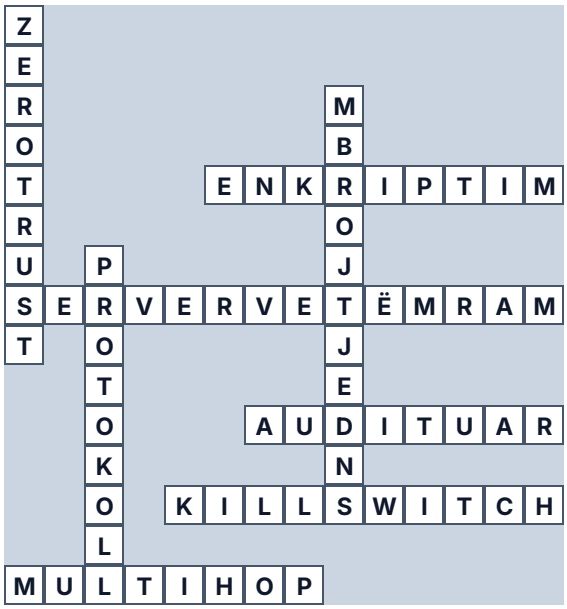
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

3 horizontalisht: ENKRIPTIM Përzierje kriptografike e ngarkesave të të dhënave për të siguruar tranzitin (9 shkronja)

5 horizontalisht: SERVERVETËMRAM Arkitekturë serveri që përdor memorie të paqëndrueshme për të ruajtur ngarkesat e të dhënave (14 shkronja)

6 horizontalisht: AUDITUAR Konfigurim i inspektuar në mënyrë të pavarur që konfirmon se nuk ruhen regjistra (8 shkronja)

7 horizontalisht: KILLSWITCH Mekanizëm mbrojtës që bllokon trafikun nëse VPN-ja dështon (10 shkronja)

8 horizontalisht: MULTIHOP Rrugëzim VPN në kaskadë që lidh së bashku dy nyje serveri (8 shkronja)

VERTIKALISHT

1 vertikalisht: ZEROTRUST Kuadër sigurie që kërkon autentikim të vazhdueshëm të të gjithë përdoruesve (9 shkronja)

2 vertikalisht: MBROJTJEDNS Zbatimi i pyetjeve private DNS për të mbrojtur kërkimet e serverëve të emrave (11 shkronja)

4 vertikalisht: PROTOKOLL Bashkësi rregullash teknike që përcaktojnë si paketohen dhe dërgohen të dhënat (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.	RTOEZUSTR	ZEROTRUST	5.	IHUPTMOL	MULTIHOP
2.	EERRVASREMËMTV	SERVERVETËMRAM	6.	JSTENDMBJRO	MBROJTJEDNS
3.	KWCIISHLTL	KILLSWITCH	7.	ARTUAUID	AUDITUAR
4.	IMIRTPENK	ENKRIPTIM	8.	LOLPTRKOO	PROTOKOLL

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"VPN TË SIGURTA MBROJNË ASETE ME VLERË"

Çelësi i studimeve të rastit

A STUDIMI I RASTIT 1: FORCIMI I INFRASTRUKTURËS SË NDËRMARRJES

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një bankë korporative po ridizajnon topologjinë e qasjes në distancë. Ajo kërkon një arkitekturë zero trust që lidh të gjitha pajisjet e klientëve me serverë të sigurt.
- Strategjia dhe zgjidhja e rekomanduar: Udhëzime për vlerësimin: Shpjego se mikrosegmentimi kufizon qasjen në burime specifike, duke parandaluar lëvizjen anësore të kërcënimeve nëse një pajisje komprometohet.

B STUDIMI I RASTIT 2: MBROJTJET E SERVERËVE VETËM ME RAM

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një ofrues VPN i fokusuar te siguria po përditëson serverët e tij për të parandaluar që sekuestrimi fizik i serverëve të ekspozojë historikun e regjistrave të përdoruesve.
- Strategjia dhe zgjidhja e rekomanduar: Udhëzime për vlerësimin: Trego se serverët RAM-Only nuk kanë ruajtje në disk fizik. Humbja e energjisë fshin automatikisht të gjitha të dhënat e përkohshme në memorien e paqëndrueshme.