Emri: _____ Data: _____ Pikët: _____

WireGuard kundrejt OpenVPN Fletë pune

Krahasimi i protokolleve WireGuard dhe OpenVPN, madhësive të kodit, shpejtësisë dhe standardeve kriptografike

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

- Krahaso kompleksitetin e kodit dhe shpejtësinë e auditimit të protokolleve.
- Analizo përfitimet e performancës nga ekzekutimi brenda hapësirës së kernelit.
- Krahaso shifrat OpenSSL me kriptografinë moderne të WireGuard.
- Konfiguro çifte çelësash publikë dhe privatë për handshake-et mes peer-eve.
- Kalo trafikun VPN përmes porteve të firewall-it TCP dhe UDP.

UDHËZIME PËR FLETËN E PUNËS PËR KRAHASIMIN E PROTOKOLLEVE

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 auditimin e protokolleve moderne. Përfundo me aktivitetin bonus Mendo shpejt.

WIREGUARD KUNDRAS OPENVPN (HYRJE)

Zgjedhja e një protokolli VPN kërkon balancimin e shpejtësisë dhe të opsioneve të konfigurimit. OpenVPN ka qenë standardi për dekada, duke ofruar fleksibilitet konfigurimi TCP/UDP. WireGuard është një zëvendësim modern që ekzekutohet drejtpërdrejt në hapësirën e kernelit me vetëm 4,000 rreshta kodi. Të kuptuarit e dallimeve mes protokolleve është çelësi për të optimizuar rrjetet e tua të sigurta.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Sa është përafërsisht madhësia e kodit burimor të protokollit WireGuard?

- A. Rreth 70,000 rreshta
- B. Mbi 100,000 rreshta
- C. Më pak se 1,000 rreshta
- D. Rreth 4,000 rreshta

2. Në cilën hapësirë të sistemit operativ funksionon WireGuard?

- A. Hapësira e përdoruesit
- B. Hapësira e kernelit
- C. Hapësira e aplikacionit
- D. Hapësirë virtuale

3. Mbi cilën bibliotekë kriptografike mbështetet kryesisht OpenVPN?

- A. ChaCha20-Poly1305
- B. Biblioteka kriptografike OpenSSL
- C. Korniza e protokollit Noise
- D. Kodimi DES në tekst të thjeshtë

4. Cili është një përfitim kyç i performancës së WireGuard kundrejt OpenVPN?

- A. Handshake-e më të shpejta lidhjeje dhe vonesë më e ulët
- B. Duke anashkaluar nevojën për adresa IP publike
- C. Mbështetje e integruar vendase për dial-up të vjetër
- D. Zero ngarkesë shtesë baterie në pajisjet celulare

5. Si i autentikon WireGuard lidhjet e peer-ave?

- A. Duke shkëmbyer fjalëkalime standarde të përdoruesve
- B. Duke verifikuar certifikatat e regjistrimit të domenit
- C. Duke përdorur çifte statike çelësash publikë dhe privatë
- D. Duke kontrolluar numrat serialë të harduerit

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

6 Pyetja 6

6. Baza e kodit kompakte e WireGuard e bën dukshëm më të lehtë për t'u audituar.

- ○ E vërtetë
- ○ E gabuar

7 Pyetja 7

7. OpenVPN në përgjithësi është më i shpejtë se WireGuard sepse ekzekutohet në hapësirën e kernelit.

- ○ E vërtetë
- ○ E gabuar

8 Pyetja 8

8. OpenVPN është shumë i konfigurueshëm dhe mbështet protokollet UDP dhe TCP.

- ○ E vërtetë
- ○ E gabuar

9 Pyetja 9

9. WireGuard përdor kriptografi moderne si ChaCha20 për enkriptim të shpejtë të paketave.

- ○ E vërtetë
- ○ E gabuar

10 Pyetja 10

10. WireGuard kërkon konfigurime komplekse të autoritetit të certifikimit për autentikim.

- ○ 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. Protokolli modern _____ funksionon drejtpërdrejt brenda berthamës së SO-së.

2. Protokolli i trashëguar _____ mbështetet te biblioteka kriptografike OpenSSL.

3. Ekzekutimi i kodit në: _____ ul ngarkesën shtesë të ndërrimit të kontekstit.

4. OpenVPN funksionon në: _____ , duke rrugëzuar paketat përmes ndërfaqeve virtuale.

5. WireGuard përdor një _____ publik dhe privat për të identifikuar bashkëlidhjet.

6. Madhësia e vogël e kodit përmirëson një cilësi të sigurisë së softuerit: _____ .

BANKA E FJALËVE TË LEKSIKUT

AUDITUESHMËRI ÇIFT ÇELËSASH KERNEL SPACE KOD KOMPAKT OPENSSL
OPENVPN USER SPACE WIREGUARD

Shkruaj përgjigjet e tua këtu:

1. 2.

3. 4.

5. 6.

Pika e kontrollit 4: Përputhja e koncepteve të rrjetit

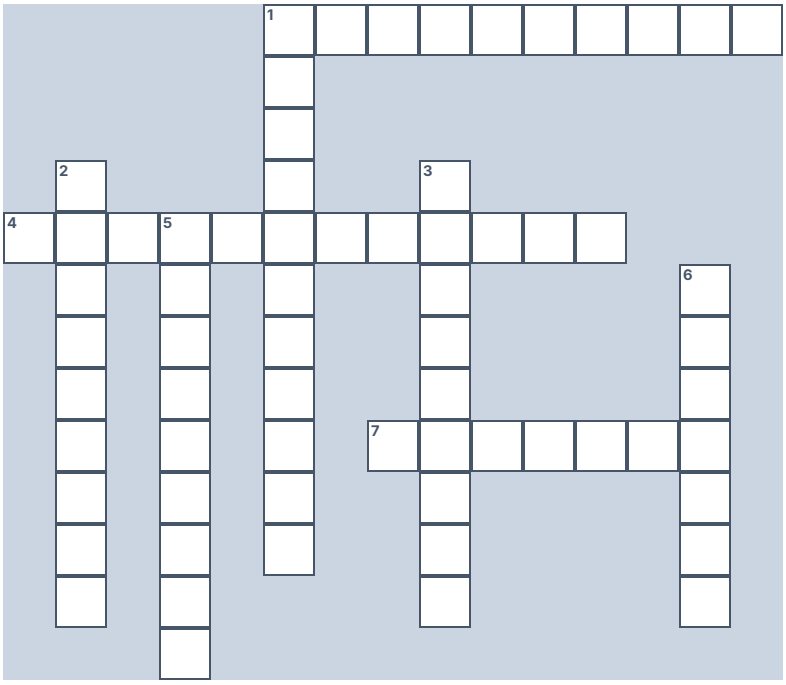
PËRPUTHJA E PËRKUFIZIMEVE

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. WireGuard	A	Zona e ekzekutimit ku funksionon OpenVPN, që krijon ngarkesë të ndërrimit të kontekstit.
☐	2. OpenVPN	B	Madhësia kompakte e bazës së kodit të WireGuard, që e bën shumë më të lehtë për t'u audituar.
☐	3. Hapësira e kernelit	C	Biblioteka kriptografike mbi të cilën mbështetet OpenVPN për algoritmet e shifrimit.
☐	4. Hapësira e përdoruesit	D	Protokollet e transportit që mbështet OpenVPN; vetë WireGuard punon vetëm mbi UDP.
☐	5. 4,000 rreshta	E	Zona e ekzekutimit të sistemit operativ ku funksionon WireGuard për shpejtësi.
☐	6. OpenSSL	F	Token asimetrikë që përdor WireGuard për të verifikuar lidhjet e peer-ave.
☐	7. Çift çelësash	G	Protokoll modern VPN, i projektuar për shpejtësi të lartë dhe auditim të thjeshtë të kodit.
☐	8. TCP/UDP	H	Protokoll i fuqishëm i trashëguar që përdor një bazë kodi konfigurimi të madhe e komplekse.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

1. Madhësia kompakte e bazës së kodit të WireGuard, që e bën shumë më të lehtë për auditim (10)

4. Tokena asimetrikë që WireGuard përdor për të verifikuar lidhjet e bashkëlidhësve (12)

7. Protokoll i fortë i trashëguar që përdor një bazë kodi të madhe dhe konfigurim kompleks (7)

VERTIKALISHT

1. Zona e ekzekutimit të sistemit operativ ku funksionon WireGuard për shpejtësi (11)

2. Protokoll modern VPN i projektuar për shpejtësi të lartë dhe auditim të thjeshtë të kodit (9)

3. Zona e ekzekutimit ku funksionon OpenVPN, duke krijuar ngarkesë shtesë të ndërrimit të kontekstit (9)

5. Protokollet e transportit që mbështet OpenVPN; vetë WireGuard funksionon vetëm mbi UDP (9)

6. Bibliotekë kriptografike nga e cila varet OpenVPN për algoritmet e shifrimit (7)

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

1 horizontalisht: Madhësia kompakte e bazës së kodit të WireGuard, që e bën shumë më të lehtë për auditim (10 shkronja):

4 horizontalisht: Tokena asimetrikë që WireGuard përdor për të verifikuar lidhjet e bashkëlidhësve (12 shkronja):

7 horizontalisht: Protokoll i fortë i trashëguar që përdor një bazë kodi të madhe dhe konfigurim kompleks (7 shkronja):

VERTIKALISHT

1 vertikalisht: Zona e ekzekutimit të sistemit operativ ku funksionon WireGuard për shpejtësi (11 shkronja):

2 vertikalisht: Protokoll modern VPN i projektuar për shpejtësi të lartë dhe auditim të thjeshtë të kodit (9 shkronja):

3 vertikalisht: Zona e ekzekutimit ku funksionon OpenVPN, duke krijuar ngarkesë shtesë të ndërrimit të kontekstit (9 shkronja):

5 vertikalisht: Protokollet e transportit që mbështet OpenVPN; vetë WireGuard funksionon vetëm mbi UDP (9 shkronja):

6 vertikalisht: Bibliotekë kriptografike nga e cila varet OpenVPN për algoritmet e shifrimit (7 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.

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

LISTA E FJALËVE TË LEKSIKUT

WIREGUARD, OPENVPN, KERNELSPACE, USERSPACE, KODKOMPAKT, OPENSSL, ÇIFTÇELËSASH, TCPDHEUDP

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. WIREGUARD**
- **B. OPENVPN**
- **C. KERNELSPACE**
- **D. USERSPACE**
- **E. KODKOMPAKT**
- **F. OPENSSL**
- **G. ÇIFTÇELËSASH**
- **H. TCPDHEUDP**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Bibliotekë kriptografike nga e cila varet OpenVPN për algoritmet e shifrimit.
2. Zona e ekzekutimit të sistemit operativ ku funksionon WireGuard për shpejtësi.
3. Protokoll i fortë i trashëguar që përdor një bazë kodi të madhe dhe konfigurim kompleks.
4. Tokena asimetrikë që WireGuard përdor për të verifikuar lidhjet e bashkëlidhësve.
5. Protokollet e transportit që mbështet OpenVPN; vetë WireGuard funksionon vetëm mbi UDP.
6. Madhësia kompakte e bazës së kodit të WireGuard, që e bën shumë më të lehtë për auditim.
7. Protokoll modern VPN i projektuar për shpejtësi të lartë dhe auditim të thjeshtë të kodit.
8. Zona e ekzekutimit ku funksionon OpenVPN, duke krijuar ngarkesë shtesë të ndërrimit të kontekstit.

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. **UGEIWARDR** _____
2. **EEEKCLRAPSN** _____
3. **KMKPOOTKAD** _____
4. **SËÇFLHEASÇIT** _____
5. **VNNEOPP** _____
6. **CRSAPUSEE** _____
7. **OSSLPNE** _____
8. **PHDTDCEUP** _____

Aktivitet bonus: Mendo shpejt

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

1	Arsye për të zgjedhur WireGuard			
2	Premtime që jep një ofrues i mirë VPN			
3	Arsye për të zgjedhur OpenVPN			
4	Arsye për të përdorur një VPN gjatë udhëtimit			
5	Gjëra që mund të shohë ofruesi yt i internetit			
6	Mënyra për të dalluar një rrjet Wi-Fi të rremë			
7	Mite për VPN-të			
8	Vende ku do të përdorje një VPN			
9	Gjëra të shpejta në jetën e përditshme			
10	Gjëra nga të cilat një VPN nuk mund të të mbrojë			
11	Gjëra që e bëjnë kodin më të lehtë për t'u kontrolluar			
12	Gjëra që mund t'i fshehë një VPN			
13	Dallime mes WireGuard dhe OpenVPN			
14	Fjalë që lidhen me privatësinë			
15	Emra enkriptimi që njeh			

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 në Wi-Fi-n e kafenesë dhe aplikacioni im VPN më lejon të zgjedh WireGuard ose OpenVPN. Thirrjet e mia video ndërpriten kur lëviz mes rrjetit të kafenesë dhe hotspot-it të telefonit tim. Cilin protokoll duhet të zgjedh, dhe pse do ta përballonte më mirë këtë ndërrim?"

ALEX (STUDENT UDHËTAR)

👩‍💻 "Jam jashtë shtetit në një rrjet hoteli që duket se i bllokon shumicën e trafikut VPN. WireGuard nuk lidhet fare, por më duhet të arrij burimet e shkollës sime në vendin tim. Çfarë ka gjasa të bllokohet, dhe si mund të më ndihmojë OpenVPN ta kaloj?"

Pika e kontrollit 9: Deshifrimi i kodit

Për të përfunduar trajnimin tënd për auditimin e protokolleve, deshifro këtë mesazh të fshehur për ekzekutimin në hapësirën e kernelit.

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

18 7 20 15 11 20 7 21 17 17 18 6 16 24 18 16 15 6

16 12 7 22 23 16 6 14 15 7 22 7

21 10 18 6 12 22 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 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 kanë rëndësi protokollet?

Protokolli vendos se si VPN-ja jote ndërton tunelin e vet, cila kriptografi i mbron të dhënat e tua dhe sa shpejt lidhet e rilidhet. WireGuard dhe OpenVPN janë dy protokollet me burim të hapur që ofrojnë shumica e aplikacioneve të VPN-ve, dhe ato bëjnë kompromise të ndryshme mes thjeshtësisë, shpejtësisë dhe konfigurueshmërisë.

Q3: A është njëri prej tyre më privat se tjetri?

Asnjë nga protokollet nuk të bën anonim. Të dy enkriptojnë trafikun e tunelit me shifra të forta; privatësia jote varet kryesisht nga ajo që regjistron ofruesi i VPN-së dhe si i menaxhon çelësat, llogaritë dhe serverët.

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 janë të dyja me burim të hapur?

Po. Si WireGuard ashtu edhe edicioni komunitar i OpenVPN publikojnë kodin e tyre burimor, kështu që studiues të pavarur mund t'i shqyrtojnë. Kodi i vogël bazë i WireGuard e bën një shqyrtim të plotë shumë më të shpejtë.

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: Cili prej tyre është më i shpejtë?

WireGuard është zakonisht më i shpejtë: ekzekutohet në kernel, përdor enkriptimin e lehtë ChaCha20-Poly1305 dhe i përfundon shpejt shtrëngimet e duarve. OpenVPN ka më shumë ngarkesë shtesë, por shpejtësitë reale varen edhe nga ngarkesa e serverit dhe distanca.

Q7: A mund të ekzekutohen të dyja mbi TCP dhe UDP?

Jo. OpenVPN mund të punojë mbi UDP ose TCP, dhe modaliteti TCP ndihmon në rrjete që bllokojnë UDP. WireGuard i dërgon paketat e tij vetëm mbi UDP, ndaj mund të dështojë në rrjete që lejojnë vetëm TCP. [4]

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 t'i përdor WireGuard dhe OpenVPN në telefonin tim?

Po. WireGuard është ndër-platformë, me aplikacione për Windows, macOS, Linux, iOS dhe Android, dhe klientë OpenVPN ekzistojnë për të njëjtat sisteme. Shumica e aplikacioneve VPN të lejojnë të zgjedhësh cilindo prej tyre. [1]

Q10: Pse është WireGuard kaq i vogël?

WireGuard mbështet një grup të vetëm të fiksuar shifrash moderne në vend të shumë opsioneve. Implementimi i tij për Linux kërkon më pak se 4,000 rreshta kodi, gjë që e bën më të lehtë për t'u audituar se bazat më të mëdha kodi të VPN-ve. [3]

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.

Q2: Cilat shifra përdor WireGuard?

WireGuard përdor ChaCha20 me Poly1305 për enkriptim, Curve25519 për shkëmbimin e çelësave, BLAKE2s për hash-imin dhe kornizën Noise për shtrëngimin e duarve. Nuk ka negociim shifrash, ndaj përdoruesit nuk mund të zgjedhin një opsion të dobët. [2]

Q3: Cilat shifra dhe biblioteka mund të përdorë OpenVPN?

OpenVPN është i integruar ngushtë me bibliotekën OpenSSL dhe përdor TLS për të shkëmbyer çelësa. Administratorët mund të zgjedhin shifra për kanalin e të dhënave si AES-256-GCM, çka shton fleksibilitetin, por edhe hapësirën për cilësime të dobëta. [4]

Q4: Si i vërteton secili protokoll palët?

Peer-at e WireGuard identifikojnë njëri-tjetrin me çelësa publikë statikë, ashtu si shkëmbimi i çelësave SSH, dhe çdo çelës lidhet me IP-të e lejuara të tunelit. OpenVPN zakonisht mbështetet në një autoritet certifikimi me certifikata X.509, shpesh të kombinuara me emër përdoruesi dhe fjalëkalim.

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 ndodh kur kaloj nga Wi-Fi në rrjetin celular?

WireGuard është pa lidhje të përhershme (connectionless): dërgon paketat nga adresa e re dhe tuneli vazhdon pas një shtrëngimi të shpejtë duarsh. OpenVPN ruan gjendjen e sesionit, ndaj një ndryshim rrjeti mund të kërkojë një rilidhje që zgjat pak më shumë.

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: A është OpenVPN ende një zgjedhje e mirë nëse WireGuard është më i shpejtë?

Po. OpenVPN është i pjekur dhe i përhapur gjerësisht, funksionon mbi TCP kur UDP bllokohet dhe mbështet konfigurime ndërmarrjesh të bazuara në certifikata. Shumë ofrues ofrojnë të dy protokollet, që përdoruesit të mund të ndërrojnë nëse njëri bllokohet ose është i ngadaltë.

Q9: Cilat porta përdorin?

Porti standard i OpenVPN është 1194, por mund të zhvendoset në çdo port UDP ose TCP, përfshirë 443. WireGuard dëgjon në një port UDP të caktuar në konfigurimin e tij; 51820 është porti i përdorur në shembujt e tij zyrtarë.

Q10: Cili protokoll është më i lehtë për t'u konfiguruar me dorë?

WireGuard është zakonisht më i thjeshtë: gjeneron një çift çelësash, shkëmben çelësat publikë dhe liston IP-të e lejuara. OpenVPN kërkon certifikata, një CA dhe më shumë opsione, megjithëse profilet .ovpn i bashkojnë në një skedar të vetëm.

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. DY TRANSPORTE

OpenVPN mund ta bartë tunelin e vet mbi UDP ose TCP, dhe në modalitetin TLS kanalet e tij të kontrollit dhe të të dhënave ndajnë një port të vetëm. [4]

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. [3]

4. KRIPTOGRAFIA MODERNE

WireGuard kombinon ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 dhe HKDF brenda kornizës së protokollit Noise, pa zgjedhje shifrash që përdoruesit të mund t'i gabojnë. [2]

5. OPENSSL BRENDA OPENVPN

OpenVPN është i integruar ngushtë me bibliotekën OpenSSL dhe nga ajo merr shumë nga aftësitë e veta kriptografike, përfshirë TLS-në që përdoret për shkëmbimin e çelësave. [4]

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. ÇELËSA NË STILIN SSH

Lidhjet WireGuard krijohen duke shkëmbyer çelësa publikë të thjeshtë, ashtu si shkëmbimi i çelësave SSH, pa nevojën për autoritet certifikimi. [1]

8. ME PLATFORMA TË NDRYSHME

WireGuard u lëshua fillimisht për kernelin e Linux dhe tani është i disponueshëm për Windows, macOS, BSD, iOS dhe Android, kështu që i njëjti protokoll funksionon në shumicën e pajisjeve. [1]

9. FSHEHTËSI E PËRPARME

WireGuard e përsërit shtrëngimin e duarve Noise_IK çdo disa minuta për të rotulluar çelësat simetrikë të sesionit, duke dhënë fshehtësi të përsosur përpara (perfect forward secrecy) edhe nëse një çelës afatgjatë rrjedh më vonë. [2]

10. NDËRFAQET TUN/TAP

OpenVPN është projektuar të punojë me ndërfaqen virtuale të rrjetit TUN/TAP, që është e disponueshme në shumicën e platformave dhe bart paketat e tunelit. [4]

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] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] 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/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Çelësi i përgjigjeve: Krahasimi i protokolleve WireGuard dhe OpenVPN, madhësia e kodit, shpejtësia dhe standardet kriptografike

1 Madhësia e kodit të WireGuard

PROTOKOLLE

Përgjigjja e saktë: D

SHËNIM PËR MËSUESIN

WireGuard është jashtëzakonisht kompakt, me rreth 4,000 rreshta kodi. Kjo e mban të vogël sipërfaqen e sulmit dhe e bën auditimin më të lehtë. Citim: WireGuard Project.

2 Shpejtësia e hapësirës së kernelit

VONESA

Përgjigjja e saktë: B

SHËNIM PËR MËSUESIN

Duke u ekzekutuar drejtpërdrejt në hapësirën e kernelit, WireGuard shmang ngarkesën shtesë të ndërrimit të kontekstit, duke mundësuar xhiro të lartë. Citim: WireGuard Project.

3 Pyetja 3

Përgjigjja e saktë: B

SHËNIM PËR MËSUESIN

OpenVPN është i integruar ngushtë me OpenSSL, që ofron shifra si AES-GCM dhe e bën shumë të konfigurueshëm, por më kompleks.

4 Performanca e protokollit

KONTROLLET E RUTERIMIT

Përgjigjja e saktë: A

SHËNIM PËR MËSUESIN

WireGuard krijon shtrëngime duarsh brenda milisekondave dhe reagon menjëherë ndaj roaming-ut të rrjetit (p.sh. kalimi nga Wi-Fi në rrjetin celular). Citim: Microsoft Native Gateway, Apple Support.

5 Kriptografia asimetrike

PRIVATËSI

Përgjigjja e saktë: C

SHËNIM PËR MËSUESIN

WireGuard përdor Cryptokey Routing, duke lidhur çelësat publikë me adresat e lejuara IP të tunelit, ngjashëm me konfigurimet e SSH. Citim: WireGuard Project.

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

6 **Pyetja 6** — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Implementimi Linux i WireGuard ka më pak se 4,000 rreshta, ndaj ekipet e sigurisë mund ta shqyrtojnë shumë më shpejt se baza kodi shumë më të mëdha të VPN-ve si OpenVPN.

7 **Vonesa në hapësirën e përdoruesit** SHPEJTËSITË — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

OpenVPN funksionon në hapësirën e përdoruesit, duke i kaluar paketat përpara e prapa nga ndërfaqja virtuale e kernelit, çka shton ngarkesë të ndërrimit të kontekstit (përveç kur përdoret çngarkim në kernel si OpenVPN DCO). Citim: DD-WRT custom firmware.

8 **Konfigurimi i OpenVPN** RREZIKU I PËRGJIMIT — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

OpenVPN mbështet ekzekutimin mbi TCP (për besueshmëri/kapërcim të firewall-it) ose UDP (për shpejtësi), duke e bërë të pajtueshëm me firewall-e komplekse të ndërmarrjeve. Citim: IETF Cryptographic Protocols.

9 **Kriptografia moderne** FIREWALL-E — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

WireGuard heq shifrat e vjetra në favor të primitivave moderne dhe të sigurta si ChaCha20 dhe Poly1305, që ekzekutohen shpejt në CPU-të e celularëve. Citim: WireGuard Project.

10 **Thjeshtimi i çiftit të çelësave** PA REGJISTRA — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

WireGuard nuk përdor certifikata ose hierarki komplekse CA; mbështetet në çifte të thjeshta çelësash publik/privat të shkëmbyer mes peer-ave. Citim: WireGuard Project.

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

G 1. WireGuard	H 2. OpenVPN	E 3. Hapësira e kernelit	A 4. Hapësira e përdoruesit
B 5. 4,000 rreshta	C 6. OpenSSL	F 7. Çift çelësash	D 8. TCP/UDP

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 WIREGUARD	2 OPENVPN	3 KERNEL SPACE	4 USER SPACE
5 ÇIFT ÇELËSASH	6 AUDITUESHMËRI		

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

1 F – OPENSSL	2 C – KERNELSPACE	3 B – OPENVPN	4 G – ÇIFTÇELËSASH
5 H – TCPDHEUDP	6 E – KODKOMPAKT	7 A – WIREGUARD	8 D – USERSPACE

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë WireGuard, OpenVPN dhe Hapësira e kernelit 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.

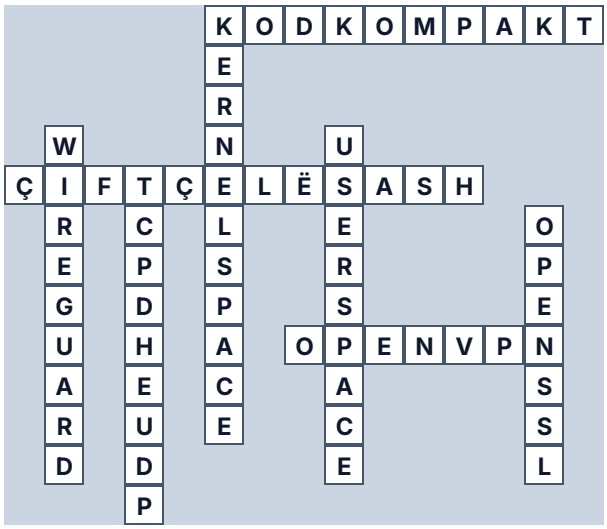
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

1 horizontalisht: KODKOMPAKT Madhësia kompakte e bazës së kodit të WireGuard, që e bën shumë më të lehtë për auditim (10 shkronja)

4 horizontalisht: ÇIFTÇELËSASH Tokena asimetrikë që WireGuard përdor për të verifikuar lidhjet e bashkëlidhësve (12 shkronja)

7 horizontalisht: OPENVPN Protokoll i fortë i trashëguar që përdor një bazë kodi të madhe dhe konfigurim kompleks (7 shkronja)

VERTIKALISHT

1 vertikalisht: KERNELSPACE Zona e ekzekutimit të sistemit operativ ku funksionon WireGuard për shpejtësi (11 shkronja)

2 vertikalisht: WIREGUARD Protokoll modern VPN i projektuar për shpejtësi të lartë dhe auditim të thjeshtë të kodit (9 shkronja)

3 vertikalisht: USERSPACE Zona e ekzekutimit ku funksionon OpenVPN, duke krijuar ngarkesë shtesë të ndërrimit të kontekstit (9 shkronja)

5 vertikalisht: TCPDHEUDP Protokollet e transportit që mbështet OpenVPN; vetë WireGuard funksionon vetëm mbi UDP (9 shkronja)

6 vertikalisht: OPENSSL Bibliotekë kriptografike nga e cila varet OpenVPN për algoritmet e shifrimit (7 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.	UGEIWARDR	WIREGUARD	5.	VNNEOPP	OPENVPN
2.	EEEKCLRAPSN	KERNELSPACE	6.	CRSAPUSEE	USERSPACE
3.	KMKPOOTKAD	KODKOMPAKT	7.	OSSLPNE	OPENSSL
4.	SËÇFLHEASÇIT	ÇIFTÇELËSASH	8.	PHDTDCEUP	TCPDHEUDP

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"PËRMIRËSO OPENVPN ME NJË TUNEL MË TË SHPEJTË"

Çelësi i studimeve të rastit

A Skenari A: Zgjedhja e një protokolli

PËRGJIMI DHE ENKRIPTIMI · Dilema e Sarës

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Rekomandim: WireGuard. Dizajni i tij i lehtë dhe pa lidhje e lejon tunelin të rikuperohet shpejt kur ndryshon rrjeti i saj, dhe ChaCha20-Poly1305 e mban enkriptimin të shpejtë.
- Siguria: Të dy protokollet e enkriptojnë trafikun e saj në Wi-Fi-n e kafenesë, ndaj secili i mbron hyrjet e saj kur është konfiguruar saktë; zgjedhja ndikon kryesisht te shpejtësia dhe qëndrueshmëria.

B Skenari B: Kapërcimi i bllokimeve të VPN-së

BLLOKIMI GJEOGRAFIK DHE IP-TË · Dilema e Alexit

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Pse u bllokua: WireGuard përdor vetëm UDP, dhe firewall-i i hotelit ose bllokon UDP-në ose i njeh paketat e WireGuard përmes filtrimit ose Deep Packet Inspection.
- Si ndihmon OpenVPN: Mund të funksionojë mbi TCP, përfshirë portën 443 të përdorur nga HTTPS, të cilën firewall-et e hoteleve e bllokojnë rrallë plotësisht, sepse shfletimi i internetit varet nga ajo.