Navn: _____ Dato: _____ Point: _____

WireGuard vs. OpenVPN Opgaveark

Sammenligning af protokollerne WireGuard og OpenVPN, størrelsen af kodebaserne, hastighed og kryptografiske standarder

OVERBLIK OVER VPN-LÆRING

ELEV
ELEVSTATUS
Netværksforsvarer-spor

SIKKER
FORBINDELSESSTATUS
Beskytter datapakker

AKTIV
LÆKAGEBESKYTTELSE
DNS- og IPv6-lækagebeskyttelse

Velkommen! Dette opgavehæfte guider dig gennem de grundlæggende principper bag virtuelle private netværk (VPN'er). Du vil udforske, hvordan krypterede tunneler sikrer dine data, hvordan netværksprotokoller fungerer, og hvordan du opdager og afhjælper lækager af personlige oplysninger.

OPGAVEARKETS KONTROLPUNKTER

- [ ] **Del 1-4: Lær VPN-begreber og protokoller.**
- [ ] **Del 5-7: Løs kryds og tværs samt ordjagt.**
- [ ] **Del 8-9: Løs casestudier og chifferudfordring.**
- [ ] **Del 10: Gennemgå grundlæggende og avanceret FAQ.**
- [ ] **Del 11: Udforsk 10 interessante fakta fra virkeligheden.**
- [ ] **Bonus: Tænk hurtigt-udfordring.**

Åbn VPN.com's VPN-guide

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

Din VPN-læringsplan

- Sammenlign protokollernes kodekompleksitet og hvor hurtigt de kan revideres.
- Analysér ydelsesgevinsten ved at køre i kernen.
- Sammenlign OpenSSL-algoritmer med WireGuards moderne kryptografi.
- Opsæt offentlige og private nøglepar til handshakes mellem parter.
- Send VPN-trafik gennem TCP- og UDP-porte i firewallen.

VEJLEDNING TIL OPGAVEARKET OM PROTOKOLSAMMENLIGNING

Besvar flervalgs- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden på revision af moderne protokoller. Slut af med bonusaktiviteten Tænk hurtigt.

WIREGUARD VS. OPENVPN (INTRODUKTION)

Valget af VPN-protokol handler om at afveje hastighed og opsætningsmuligheder. OpenVPN har været standarden i årtier og er fleksibel med både TCP og UDP. WireGuard er en moderne afløser, der kører direkte i kernen med kun 4.000 linjer kode. At forstå forskellene er nøglen til at optimere sikre netværk.

LÆS HVERT KONTROLPUNKT GRUNDIGT, OG VÆLG ELLER SKRIV DET RIGTIGE SVAR.

Kontrolpunkt 1: Flervalgsopgave

1 **1. Hvor stor er WireGuard-protokollens kodebase omtrent?**

- A. Cirka 70.000 linjer
- B. Over 100.000 linjer
- C. Under 1.000 linjer
- D. Omkring 4.000 linjer

2 **2. Hvor i styresystemet kører WireGuard?**

- A. I brugerrummet
- B. I kernen
- C. I applikationsrummet
- D. I det virtuelle rum

3 **3. Hvilket kryptografisk bibliotek bygger OpenVPN primært på?**

- A. ChaCha20-Poly1305
- B. Det kryptografiske bibliotek OpenSSL
- C. Noise-protokolrammeværket
- D. DES-kodning i klartekst

4 **4. Hvad er en vigtig ydelsesfordel ved WireGuard frem for OpenVPN?**

- A. Hurtigere handshakes og lavere latenstid
- B. Ingen behov for offentlige IP-adresser
- C. Indbygget understøttelse af gammelt modemopkald
- D. Intet batteriforbrug på mobile enheder

5 **5. Hvordan godkender WireGuard forbindelser mellem parter?**

- A. Ved at udveksle almindelige adgangskoder
- B. Ved at kontrollere domænecertifikater
- C. Ved at bruge faste offentlige og private nøglepar
- D. Ved at tjekke hardwarens serienumre

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. WireGuards kompakte kodebase gør den markant lettere at revidere.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. OpenVPN er generelt hurtigere end WireGuard, fordi den kører i kernen.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. OpenVPN kan tilpasses vidt og understøtter både UDP og TCP.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. WireGuard bruger moderne kryptografi som ChaCha20 til hurtig pakkekryptering.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. WireGuard kræver komplekse certifikatmyndigheder for at kunne godkende.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

Læs hver sætning nedenfor, og udfyld det tomme felt med det rigtige ord fra ordbanken.

1. Den moderne _____ protokol kører direkte i styresystemets kerne.
2. Den ældre _____ protokol bygger på kryptobiblioteket OpenSSL.
3. At afvikle kode i _____ reducerer overhead ved kontekstskift.
4. OpenVPN kører i _____ og router pakker via virtuelle grænseflader.
5. WireGuard bruger offentlige og private _____ til at identificere forbindelsens parter.
6. En lille kodebase styrker softwarens sikkerheds- _____ niveau.

ORDBANK MED FAGUDTRYK

BRUGERRUMMET KERNEN NOISE NØGLEPAR OPENSSL OPENVPN REVIDERBARHED WIREGUARD

Skriv dine svar her:

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

Kontrolpunkt 4: Match netværksbegreber

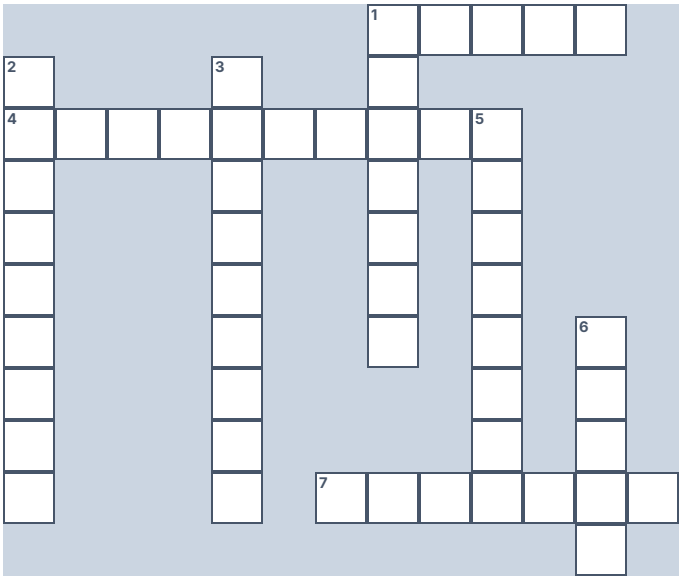
MATCH BEGREBER OG DEFINITIONER

Match hvert fagudtryk til venstre med den rigtige definition til højre ved at skrive det tilhørende bogstav (A-H) i indtastningsfeltet.

☐	1. WireGuard	A	Det område hvor OpenVPN kører, hvilket giver overhead ved kontekstskift.
☐	2. OpenVPN	B	Den kompakte størrelse af WireGuards kodebase, som gør den meget lettere at revidere.
☐	3. Kernen	C	Kryptobibliotek som OpenVPN bruger til sine algoritmer.
☐	4. Brugerrummet	D	Transportprotokoller, som OpenVPN understøtter; WireGuard selv kører kun over UDP.
☐	5. 4.000 LINJER	E	Det område i styresystemet, hvor WireGuard kører for hastighedens skyld.
☐	6. OpenSSL	F	Asymmetriske nøgler som WireGuard bruger til at bekræfte parter.
☐	7. Nøglepar	G	Moderne VPN-protokol bygget til høj hastighed og enkel koderevision.
☐	8. TCP/UDP	H	Robust ældre protokol med en stor og kompleks kodebase.

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

1. Område i styresystemet, hvor WireGuard kører for hastighedens skyld (5)

4. Krypteringsmetoder som ChaCha20 og AES (10)

7. Kryptografisk bibliotek, som OpenVPN bygger på for sine chifferalgoritmer (7)

LODRETTE NØGLER

1. Beskriver WireGuards lille kodebase, der gør den meget lettere at revidere (7)

2. Den indledende udveksling, hvor WireGuard bruger asymmetriske nøglepar til at bekræfte peers (9)

3. Område, hvor OpenVPN kører, hvilket giver overhead ved kontekstskift (9)

5. Gennemgang af kildekoden for sikkerhedsfejl, som WireGuards lille kodebase gør lettere (8)

6. Protokolrammen bag WireGuards handshake (5)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

Brugere af skærmlæser og tastatur kan skrive krydsordssvarene direkte i tekstfelterne nedenfor.

VANDRETTE NØGLER

1 vandret: Område i styresystemet, hvor WireGuard kører for hastighedens skyld (5 bogstaver):

4 vandret: Krypteringsmetoder som ChaCha20 og AES (10 bogstaver):

7 vandret: Kryptografisk bibliotek, som OpenVPN bygger på for sine chifferalgoritmer (7 bogstaver):

LODRETTE NØGLER

1 lodret: Beskriver WireGuards lille kodebase, der gør den meget lettere at revidere (7 bogstaver):

2 lodret: Den indledende udveksling, hvor WireGuard bruger asymmetriske nøglepar til at bekræfte peers (9 bogstaver):

3 lodret: Område, hvor OpenVPN kører, hvilket giver overhead ved kontekstskift (9 bogstaver):

5 lodret: Gennemgang af kildekoden for sikkerhedsfejl, som WireGuards lille kodebase gør lettere (8 bogstaver):

6 lodret: Protokolrammen bag WireGuards handshake (5 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

Find de 8 vigtige fagudtryk, der er skjult i gitteret nedenfor. Ordene kan stå vandret, lodret eller diagonalt.

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

ORDLISTE MED FAGUDTRYK

KERNE BRUGERRUM OPENSSL NOISE REVISION KOMPAKT ALGORITMER HANDSHAKE

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK
A. KERNE
B. BRUGERRUM
C. OPENSSL
D. NOISE
E. REVISION
F. KOMPAKT
G. ALGORITMER
H. HANDSHAKE

DEFINITIONER OG MATCHFELTER

1. Beskriver WireGuards lille kodebase, der gør den meget lettere at revidere.
2. Kryptografisk bibliotek, som OpenVPN bygger på for sine chifferalgoritmer.
3. Område, hvor OpenVPN kører, hvilket giver overhead ved kontekstskift.
4. Krypteringsmetoder som ChaCha20 og AES.
5. Den indledende udveksling, hvor WireGuard bruger asymmetriske nøglepar til at bekræfte peers.
6. Gennemgang af kildekoden for sikkerhedsfejl, som WireGuards lille kodebase gør lettere.
7. Område i styresystemet, hvor WireGuard kører for hastighedens skyld.
8. Protokolrammen bag WireGuards handshake.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige VPN-begreber. Skriv dine svar i indtastningsfelterne.

1. **NRKEE**
2. **OELSSNP**
3. **IERSINOV**
4. **IERROMTALG**
5. **RERMRGBUU**
6. **SNIEO**
7. **KKATOPM**
8. **ESKHDAHAN**

Bonusaktivitet: Tænk hurtigt

3 SVAR I HVER KATEGORI. DEN FØRSTE, DER UDFYLDER HELE LISTEN, VINDER.

1	Grunde til at vælge WireGuard			
2	Ting, en god VPN-udbyder lover			
3	Grunde til at vælge OpenVPN			
4	Grunde til at bruge en VPN på rejsen			
5	Ting, din internetudbyder kan se			
6	Måder at opdage et falsk wi-fi-net			
7	Myter om VPN			
8	Steder, hvor du ville bruge en VPN			
9	Ting, der er hurtige i hverdagen			
10	Ting, en VPN ikke kan beskytte mod			
11	Ting, der gør kode lettere at kontrollere			
12	Ting, en VPN kan skjule			
13	Forskelle på WireGuard og OpenVPN			
14	Ord, der har med privatliv at gøre			
15	Krypteringsnavne, du kender			

Kontrolpunkt 8: VPN-casestudier

Anvend de begreber, du har lært, til at løse de virkelige scenarier nedenfor.

SARAH (STUDERENDE PÅ CAFÉ)

👩‍💻 "Hej! Jeg er på caféens wi-fi, og min VPN-app lader mig vælge WireGuard eller OpenVPN. Mine videoopkald bliver ved med at falde ud, når jeg går mellem caféens netværk og min telefons hotspot. Hvilken protokol skal jeg vælge, og hvorfor vil den klare skiftet bedre?"

ALEX (STUDERENDE PÅ REJSE)

👩‍💻 "Jeg er i udlandet på et hotelnetværk, der ser ud til at blokere det meste VPN-trafik. WireGuard vil slet ikke forbinde, men jeg skal have adgang til min skoles ressourcer derhjemme. Hvad bliver sandsynligvis blokeret, og hvordan kan OpenVPN hjælpe mig igennem?"

Kontrolpunkt 9: Afkod chifferet

Afslut træningen i protokolrevision ved at dekryptere denne skjulte besked om afvikling i kernen.

BOGSTAV-TIL-TAL-KRYPTERINGSNØGLE

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 Æ=27 Ø=28 Å=29

11	15	4	5		9		11	5	18	14	5	14		7	9	22	5	18

8	21	18	20	9	7	5		20	21	14	14	5	12	5	18

Afkodet besked:

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z, 27 = Æ, 28 = Ø, 29 = Å).

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del A)

Gennemgå de mest almindelige spørgsmål og svar om brugen af virtuelle private netværk.

Q1: Hvad er en VPN, og hvordan virker den?

Et virtuelt privat netværk (VPN) krypterer din internetforbindelse og leder din trafik gennem en sikker fjernserver. Det skjuler din offentlige IP-adresse og begrænser, hvad lokale observatører på netværket og din internetudbyder kan se om trafik, der går gennem VPN-tunnelen.

Q2: Hvorfor betyder protokoller noget?

Protokollen bestemmer, hvordan din VPN bygger sin tunnel, hvilken kryptografi der beskytter dine data, og hvor hurtigt den forbinder og genforbinder. WireGuard og OpenVPN er de to open source-protokoller, som de fleste VPN-apps tilbyder, og de afvejer enkelhed, hastighed og konfigurerbarhed forskelligt.

Q3: Er den ene mere privat end den anden?

Ingen af protokollerne gør dig anonym. Begge krypterer tunneltrafikken med stærke algoritmer; dit privatliv afhænger mest af, hvad VPN-udbyderen logger, og hvordan den håndterer nøgler, konti og servere.

Q4: Vil en VPN gøre min internethastighed langsommere?

Ja, en smule. Krypteringen og den fysiske afstand til VPN-serveren giver ekstra forsinkelse og overhead. Påvirkningen varierer efter udbyder, protokol, serverafstand, enhed og netværksforhold.

Q5: Er begge open source?

Ja. WireGuard og OpenVPN's community-udgave offentliggør begge deres kildekode, så uafhængige forskere kan gennemgå dem. WireGuards lille kodebase gør en fuld gennemgang meget hurtigere.

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del B)

Gennemgå de mest almindelige spørgsmål og svar om brugen af virtuelle private netværk.

Q6: Hvilken er hurtigst?

WireGuard er som regel hurtigst: Den kører i kernen, bruger den slanke ChaCha20-Poly1305-kryptering og gennemfører handshakes hurtigt. OpenVPN har mere overhead, men de reelle hastigheder afhænger også af serverbelastning og afstand.

Q7: Kan begge køre over TCP og UDP?

Nej. OpenVPN kan køre over UDP eller TCP, og TCP-tilstand hjælper på netværk, der blokerer UDP. WireGuard sender kun sine pakker over UDP, så den kan fejle på netværk, der kun tillader TCP. [4]

Q8: Hvordan vælger jeg den bedste VPN?

Se efter reviderede no-logs-politikker, stærke protokoller (WireGuard, OpenVPN), sikre serverplaceringer, høje hastigheder, RAM-only-servere, en kill switch-funktion og en jurisdiktion uden for efterretningsalliancer (som 5/9/14 Eyes).

Q9: Kan jeg bruge WireGuard og OpenVPN på min telefon?

Ja. WireGuard er platformsuafhængig med apps til Windows, macOS, Linux, iOS og Android, og der findes OpenVPN-klienter til de samme systemer. De fleste VPN-apps lader dig vælge begge. [1]

Q10: Hvorfor er WireGuard så lille?

WireGuard understøtter ét fast sæt moderne krypteringsalgoritmer i stedet for mange valgmuligheder. Dens Linux-implementering kræver under 4.000 linjer kode, hvilket gør den lettere at revidere end større VPN-kodebaser. [3]

Kontrolpunkt 10: Avanceret VPN-FAQ (del C)

Udforsk tekniske og strukturelle aspekter af virtuelle private netværk og sikre tunneleringsprotokoller.

Q1: Hvad er forskellen på WireGuard, OpenVPN og IKEv2?

WireGuard er en moderne, letvægtsprotokol (kun ca. 4.000 linjer kode) med høje hastigheder og hurtig forbindelse. OpenVPN er en meget sikker og gennemtestet open source-protokol. IKEv2 er fremragende til mobile enheder, fordi den hurtigt genopretter forbindelsen ved skift mellem netværk.

Q2: Hvilke krypteringsalgoritmer bruger WireGuard?

WireGuard bruger ChaCha20 med Poly1305 til kryptering, Curve25519 til nøgleudveksling, BLAKE2s til hashing og Noise-rammeværket til sit handshake. Der forhandles ikke om algoritmer, så brugerne kan ikke vælge en svag mulighed. [2]

Q3: Hvilke krypteringsalgoritmer og biblioteker kan OpenVPN bruge?

OpenVPN er tæt integreret med OpenSSL-biblioteket og bruger TLS til at udveksle nøgler. Administratorer kan vælge krypteringsalgoritmer til datakanalen som AES-256-GCM, hvilket giver fleksibilitet, men også plads til svage indstillinger. [4]

Q4: Hvordan godkender hver protokol peers?

WireGuard-peers identificerer hinanden ved statiske offentlige nøgler, ligesom når man udveksler SSH-nøgler, og hver nøgle er knyttet til tilladte tunnel-IP'er. OpenVPN bruger som regel en certifikatmyndighed med X.509-certifikater, ofte kombineret med brugernavn og adgangskode.

Q5: Hvordan omgår obfuskering VPN-blokeringer?

Obfuskering (eller "Stealth VPN") forklæder VPN-trafik, så den ligner almindelig HTTPS-trafik (port 443). Det kan hjælpe med at komme forbi Deep Packet Inspection (DPI), som regeringer eller skole-/arbejdsnetværk bruger til at blokere VPN'er.

Kontrolpunkt 10: Avanceret VPN-FAQ (del D)

Udforsk tekniske og strukturelle aspekter af virtuelle private netværk og sikre tunneleringsprotokoller.

Q6: Hvad sker der, når jeg skifter fra wi-fi til mobildata?

WireGuard er forbindelsesløs: Den sender pakker fra den nye adresse, og tunnelen fortsætter efter et hurtigt handshake. OpenVPN holder styr på sessionstilstanden, så et netværksskift kan kræve en genforbindelse, der tager lidt længere tid.

Q7: Hvordan virker Forward Secrecy (Perfect Forward Secrecy)?

PFS sikrer, at der genereres en unik, midlertidig krypteringsnøgle til hver enkelt session. Selv hvis en privat nøgle kompromitteres senere, kan den ikke bruges til at dekryptere tidligere eller fremtidige sessioner, fordi de brugte uafhængige nøgler.

Q8: Er OpenVPN stadig et godt valg, hvis WireGuard er hurtigere?

Ja. OpenVPN er moden og udbredt, kører over TCP, når UDP er blokeret, og understøtter certifikatbaserede virksomhedsopsætninger. Mange udbydere tilbyder begge protokoller, så brugerne kan skifte, hvis den ene er blokeret eller langsom.

Q9: Hvilke porte bruger de?

OpenVPN's standardport er 1194, men den kan flyttes til enhver UDP- eller TCP-port, herunder 443. WireGuard lytter på en UDP-port, der angives i konfigurationen; 51820 er den port, der bruges i de officielle eksempler.

Q10: Hvilken protokol er lettest at opsætte manuelt?

WireGuard er som regel enklere: Generér et nøglepar, udveksl offentlige nøgler, og angiv tilladte IP'er. OpenVPN kræver certifikater, en CA og flere indstillinger, selvom .ovpn-profiler samler dem i én fil.

Del 11: 10 interessante VPN-fakta og indsigter fra virkeligheden

Gennemgå disse værdifulde fakta og indsigter om VPN'ers historie, marked og teknologi.

1. DEN FØRSTE VPN-PROTOKOL

PPTP (Point-to-Point Tunneling Protocol) blev udviklet af en gruppe leverandører, herunder Microsoft, og udgivet som RFC 2637 i juli 1999 for at understøtte VPN'er til fjernadgang. [6]

2. TO TRANSPORTPROTOKOLLER

OpenVPN kan føre sin tunnel over UDP eller TCP, og i TLS-tilstand deler kontrol- og datakanalen én port. [4]

3. WIREGUARD-REVOLUTIONEN

WireGuard har en meget strømlinet kodebase designet til effektivitet, hvilket gør den lettere at revidere for sikkerhedshuller end traditionelle protokoller. [3]

4. MODERNE KRYPTOGRAFI

WireGuard kombinerer ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 og HKDF inden for Noise-protokolrammeværket, uden valg af algoritmer, som brugerne kan tage fejl af. [2]

5. OPENSSL I OPENVPN

OpenVPN er tæt integreret med OpenSSL-biblioteket og henter mange af sine kryptografiske funktioner derfra, herunder den TLS, der bruges til at udveksle nøgler. [4]

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) undersøger pakkers indhold og trafikmønstre, ikke kun headere, og nogle firewalls bruger det til at opdage og blokere almindelige VPN-protokoller.

7. NØGLER I SSH-STIL

WireGuard-forbindelser opsættes ved at udveksle simple offentlige nøgler, ligesom når man udveksler SSH-nøgler, uden behov for en certifikatmyndighed. [1]

8. PLATFORMSUAFHÆNGIG

WireGuard blev først udgivet til Linux-kernen og findes nu til Windows, macOS, BSD, iOS og Android, så den samme protokol virker på de fleste enheder. [1]

9. FORWARD SECRECY

WireGuard gentager sit Noise_IK-handshake med få minutters mellemrum for at rotere de symmetriske sessionsnøgler, hvilket giver perfect forward secrecy, selv hvis en langtidsnøgle senere lækker. [2]

10. TUN/TAP-GRÆNSEFLADER

OpenVPN er designet til at arbejde med den virtuelle TUN/TAP-netværksgrænseflade, som findes på de fleste platforme og fører tunnelens pakker. [4]

Tekniske referencer og kilder

Citerede publikationer, kryptografiske specifikationer og officielle dokumentstandarder anvendt i dette opgaveark.

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[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

Facitliste: Sammenligning af protokollerne WireGuard og OpenVPN, kodebasernes størrelse, hastighed og kryptografiske standarder

1 WireGuards kodestørrelse PROTOKOLLER

Rigtigt svar: D

UNDERVISNINGSNOTE

WireGuard er ekstremt kompakt med omkring 4.000 linjer kode. Det holder angrebsfladen lille og gør revision lettere.

2 Hastighed i kernen LATENS

Rigtigt svar: B

UNDERVISNINGSNOTE

Ved at køre direkte i kernen undgår WireGuard overhead fra kontekstskift, hvilket giver højt gennemløb.

3 Spørgsmål 3

Rigtigt svar: B

UNDERVISNINGSNOTE

OpenVPN er tæt integreret med OpenSSL, som leverer krypteringsalgoritmer som AES-GCM og gør den meget konfigurerbar, men mere kompleks.

4 Protokollens ydelse ROUTINGKONTROL

Rigtigt svar: A

UNDERVISNINGSNOTE

WireGuard gennemfører handshakes på millisekunder og reagerer straks ved netværksskift (fx fra Wi-Fi til mobildata).

5 Asymmetrisk kryptografi PRIVATLIV

Rigtigt svar: C

UNDERVISNINGSNOTE

WireGuard bruger Cryptokey Routing, hvor offentlige nøgler knyttes til tilladte IP-adresser i tunnelen, ligesom ved SSH.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Spørgsmål 6** **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

WireGuards Linux-implementering er under 4.000 linjer, så sikkerhedsteams kan gennemgå den langt hurtigere end meget større VPN-kodebaser som OpenVPN.

7 **Latenstid i brugerrummet** HASTIGHEDER **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

OpenVPN kører i brugerrummet og sender pakker frem og tilbage fra kernens virtuelle grænseflade, hvilket tilføjer overhead fra kontekstskift (medmindre der bruges aflastning i kernen som OpenVPN DCO).

8 **OpenVPN-opsætning** AFLYTNINGSRISIKO **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

OpenVPN kan køre over TCP (for stabilitet og omgåelse af firewalls) eller UDP (for hastighed) og passer derfor til komplekse firewalls.

9 **Moderne kryptografi** FIREWALLS **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

WireGuard dropper ældre algoritmer til fordel for moderne, sikre primitiver som ChaCha20 og Poly1305, der kører hurtigt på mobile CPU'er.

10 **Enkle nøglepar** INGEN LOGS **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

WireGuard bruger hverken certifikater eller komplekse CA-hierarkier, men enkle offentlige og private nøglepar udvekslet mellem parterne.

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

G 1. WireGuard	H 2. OpenVPN	E 3. Kernen	A 4. Brugerrummet
B 5. 4.000 LINJER	C 6. OpenSSL	F 7. Nøglepar	D 8. TCP/UDP

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 WIREGUARD	2 OPENVPN	3 KERNEN	4 BRUGERRUMMET
5 NØGLEPAR	6 REVIDERBARHED		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 F – KOMPAKT	2 C – OPENSSL	3 B – BRUGERRUM	4 G – ALGORITMER
5 H – HANDSHAKE	6 E – REVISION	7 A – KERNE	8 D – NOISE

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare WireGuard, OpenVPN og Kernen med egne ord og give et eksempel på hvert begreb.

Casestudier:
Bed eleverne begrunde deres anbefalinger med fakta fra opgavearket frem for antagelser.

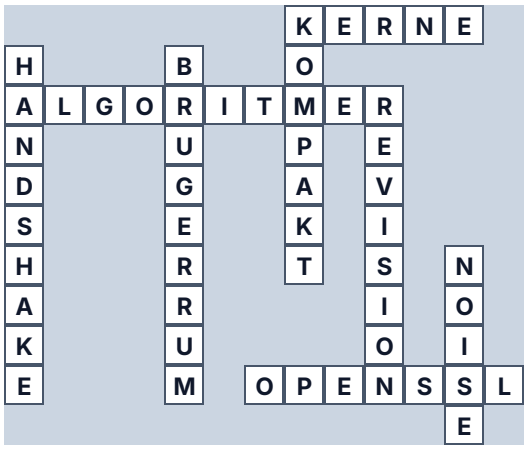
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

1 vandret: KERNE Område i styresystemet, hvor WireGuard kører for hastighedens skyld (5 bogstaver)

4 vandret: ALGORITMER Krypteringsmetoder som ChaCha20 og AES (10 bogstaver)

7 vandret: OPENSSL Kryptografisk bibliotek, som OpenVPN bygger på for sine chifferalgoritmer (7 bogstaver)

LODRETTE NØGLER

1 lodret: KOMPAKT Beskriver WireGuards lille kodebase, der gør den meget lettere at revidere (7 bogstaver)

2 lodret: HANDSHAKE Den indledende udveksling, hvor WireGuard bruger asymmetriske nøglepar til at bekræfte peers (9 bogstaver)

3 lodret: BRUGERRUM Område, hvor OpenVPN kører, hvilket giver overhead ved kontekstskift (9 bogstaver)

5 lodret: REVISION Gennemgang af kildekoden for sikkerhedsfejl, som WireGuards lille kodebase gør lettere (8 bogstaver)

6 lodret: NOISE Protokolrammen bag WireGuards handshake (5 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. NRKEE	KERNE	5. RERMRGBUU	BRUGERRUM
2. OELSSNP	OPENSSL	6. SNIEO	NOISE
3. IERSINOV	REVISION	7. KKATOPM	KOMPAKT
4. IERROMTALG	ALGORITMER	8. ESKHDAHAN	HANDSHAKE

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"KODE I KERNEN GIVER HURTIGE TUNNELER"

Facit til casestudier

A Scenarie A: Valg af protokol

AFLYTNING OG KRYPTERING | Sarahs dilemma

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Anbefaling: WireGuard. Dens lette, forbindelsesløse design lader tunnelen komme sig hurtigt, når hendes netværk skifter, og ChaCha20-Poly1305 holder krypteringen hurtig.
- Sikkerhed: Begge protokoller krypterer hendes trafik på caféens wi-fi, så begge beskytter hendes logins, når de er korrekt konfigureret; valget påvirker primært hastighed og stabilitet.

B Scenarie B: Forbi VPN-blokeringer

GEOBLOKERING OG IP-ADRESSER | Alex' dilemma

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Hvorfor blokeret: WireGuard bruger kun UDP, og hotellets firewall blokerer sandsynligvis UDP eller genkender WireGuard-pakker via filtrering eller Deep Packet Inspection.
- Sådan hjælper OpenVPN: Den kan køre over TCP, herunder port 443, som HTTPS bruger, og som hotellers firewalls sjældent blokerer helt, fordi webbrowsing afhænger af den.