Navn: _____ Dato: _____ Poeng: _____

WireGuard mot OpenVPN Arbeidsark

Sammenligning av protokollene WireGuard og OpenVPN, kodebasestørrelser, hastighet og kryptografiske standarder

OPPLÆRINGSOVERSIKT FOR VPN

ELEV
STUDENTSTATUS
Spor for nettverksforsvarere

SIKKER
TILKOBLINGSSTATUS
Beskytte datapakker

AKTIV
LEKKASJEBESKYTTELSE
DNS- og IPv6-lekkasjebeskyttelse

Velkommen! Dette aktivitetsheftet veileder deg gjennom de grunnleggende prinsippene i virtuelle private nettverk (VPN-er). Du utforsker hvordan krypterte tunneler sikrer dataene dine, hvordan nettverksprotokoller fungerer, og hvordan du identifiserer og begrenser personvernlekkasjer.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk VPN-begreper og -protokoller.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms VPN-veiledning

URL: https://www.vpn.com/no/vpn/

Din læringsveiledning for VPN

- Sammenlign kodebasekompleksitet og revisjonshastighet for protokoller.
- Analyser ytelsesgevinstene ved å kjøre i kjerneområdet.
- Sammenlign OpenSSL-chiffer med moderne kryptografi i WireGuard.
- Sett opp nøkkelpar med offentlig og privat nøkkel for håndtrykk mellom noder.
- Rut VPN-trafikk gjennom brannmurporter for TCP og UDP.

INSTRUKSJONER FOR ARBEIDSARKET OM PROTOKOLLSAMMENLIGNING

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på revisjon av moderne protokoller. Avslutt med bonusaktiviteten Tenk raskt.

WIREGUARD VS. OPENVPN (INNLEDNING)

Valg av VPN-protokoll krever en avveining mellom hastighet og konfigurasjonsmuligheter. OpenVPN har vært standarden i flere tiår og gir fleksibel TCP/UDP-konfigurasjon. WireGuard er en moderne erstatning som kjører direkte i kjerneområdet med bare 4 000 kodelinjer. Å forstå forskjellene mellom protokollene er nøkkelen til å optimalisere sikre nettverk.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. **1. Hva er omtrentlig størrelse på kodebasen til WireGuard-protokollen?**
   - A. Omtrent 70 000 linjer
   - B. Over 100 000 linjer
   - C. Færre enn 1 000 linjer
   - D. Rundt 4 000 linjer

2. **2. I hvilket område av operativsystemet kjører WireGuard?**
   - A. Brukerrom
   - B. Kjerneområde
   - C. Applikasjonsområde
   - D. Virtuelt rom

3. **3. Hvilket kryptografibibliotek er OpenVPN i hovedsak avhengig av?**
   - A. ChaCha20-Poly1305
   - B. Kryptografibiblioteket OpenSSL
   - C. Rammeverket Noise-protokollen
   - D. Klartekstkoding med DES

4. **4. Hva er en viktig ytelsesfordel ved WireGuard sammenlignet med OpenVPN?**
   - A. Raskere tilkoblingshåndtrykk og lavere forsinkelse
   - B. Å omgå behovet for offentlige IP-adresser
   - C. Innebygd støtte for eldre oppringt tilkobling
   - D. Null batteribelastning på mobile enheter

5. **5. Hvordan autentiserer WireGuard peer-tilkoblinger?**
   - A. Ved å utveksle vanlige brukerpassord
   - B. Ved å verifisere sertifikater for domeneregistrering
   - C. Ved å bruke statiske offentlige og private nøkkelpar
   - D. Ved å kontrollere maskinvarens serienumre

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. WireGuards kompakte kodebase gjør den betydelig enklere å gjennomgå.

○ Sant ○ Usant

7 Spørsmål 7

7. OpenVPN er vanligvis raskere enn WireGuard fordi det kjører i kjerneområdet.

○ Sant ○ Usant

8 Spørsmål 8

8. OpenVPN er svært konfigurerbart og støtter både UDP- og TCP-protokoller.

○ Sant ○ Usant

9 Spørsmål 9

9. WireGuard bruker moderne kryptografi som ChaCha20 for rask kryptering av pakker.

○ Sant ○ Usant

10 Spørsmål 10

10. WireGuard krever komplekse oppsett med sertifiseringsinstans for å autentisere.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. Den moderne protokollen _____ opererer direkte inne i OS-kjernen.
2. Den eldre protokollen _____ er avhengig av kryptobiblioteket OpenSSL.
3. Å kjøre kode i _____ reduserer overhead ved kontekstbytte.
4. OpenVPN kjører i _____ og ruter pakker via virtuelle grensesnitt.
5. WireGuard bruker offentlige og private _____ for å identifisere tilkoblingspartnere.
6. En liten kodebase forbedrer programvarens sikkerhetsmessige _____ .

ORDBANK

BRUKERROM KJERNEROM KOMPAKT KODE NØKKELPAR OPENSSL OPENVPN REVIDERBARHET WIREGUARD

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble nettverksbegreper

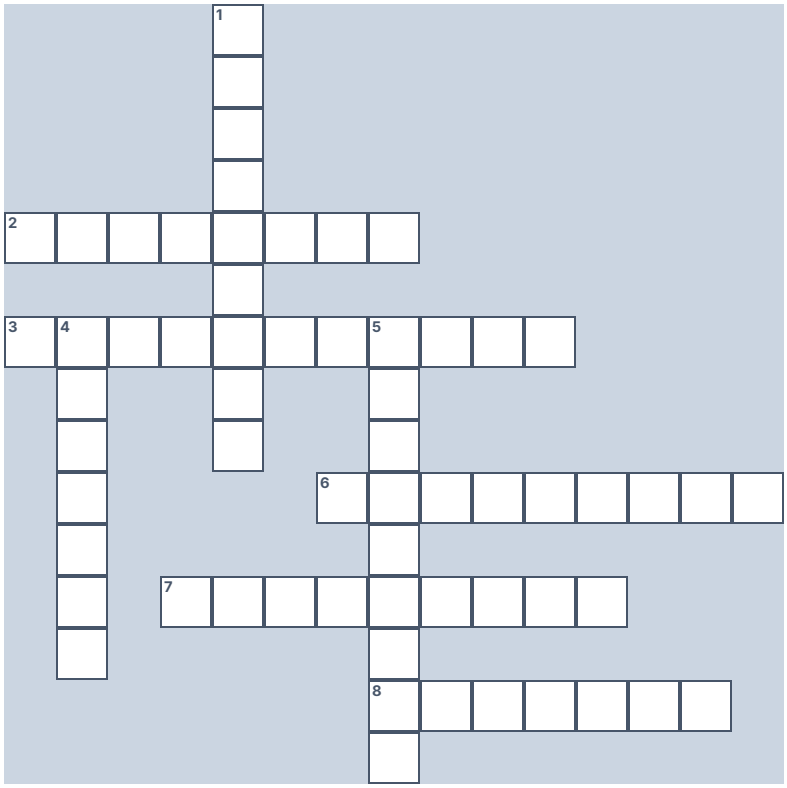
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. WireGuard	A	Kjøreområde der OpenVPN kjører, noe som skaper belastning ved kontekstbytte.
☐	2. OpenVPN	B	Den kompakte størrelsen på WireGuards kodebase, som gjør den mye enklere å revidere.
☐	3. Kjerneområde	C	Kryptografisk bibliotek som OpenVPN bruker for chifferalgoritmer.
☐	4. Brukerområde	D	Transportprotokoller som OpenVPN støtter; WireGuard selv kjører kun over UDP.
☐	5. 4 000 LINJER	E	Det området i operativsystemet der WireGuard kjører for å oppnå hastighet.
☐	6. OpenSSL	F	Asymmetriske tokens som WireGuard bruker for å verifisere tilkoblinger mellom noder.
☐	7. Nøkkelpar	G	Moderne VPN-protokoll utformet for høy hastighet og enkel kodegjennomgang.
☐	8. TCP/UDP	H	Robust eldre protokoll som bruker en stor, kompleks konfigurasjonskodebase.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

2. Transportprotokoller som OpenVPN støtter; WireGuard selv kjører bare over UDP (8)

3. Den kompakte størrelsen på WireGuards kodebase, som gjør den mye enklere å revidere (11)

6. Utførelsesområde der OpenVPN kjører, noe som skaper overhead ved kontekstbytte (9)

7. Asymmetriske nøkler som WireGuard bruker til å verifisere peer-tilkoblinger (9)

8. Kryptografibibliotek som OpenVPN er avhengig av for chifferalgoritmer (7)

LODDRETT

1. Moderne VPN-protokoll utformet for høy hastighet og enkel kodegjennomgang (9)

4. Robust eldre protokoll med en stor, kompleks konfigurasjonskodebase (7)

5. Utførelsesområde i operativsystemet der WireGuard kjører for hastighet (9)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

2 vannrett: Transportprotokoller som OpenVPN støtter; WireGuard selv kjører bare over UDP (8 bokstaver):

3 vannrett: Den kompakte størrelsen på WireGuards kodebase, som gjør den mye enklere å revidere (11 bokstaver):

6 vannrett: Utførelsesområde der OpenVPN kjører, noe som skaper overhead ved kontekstbytte (9 bokstaver):

7 vannrett: Asymmetriske nøkler som WireGuard bruker til å verifisere peer-tilkoblinger (9 bokstaver):

8 vannrett: Kryptografibibliotek som OpenVPN er avhengig av for chifferalgoritmer (7 bokstaver):

LODDRETT

1 loddrett: Moderne VPN-protokoll utformet for høy hastighet og enkel kodegjennomgang (9 bokstaver):

4 loddrett: Robust eldre protokoll med en stor, kompleks konfigurasjonskodebase (7 bokstaver):

5 loddrett: Utførelsesområde i operativsystemet der WireGuard kjører for hastighet (9 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

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

ORDLISTE

WIREGUARD OPENVPN KJERNEROM BRUKERROM KOMPAKTKODE OPENSSL NØKKELPAR TCPOGUDP

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. WIREGUARD
B. OPENVPN
C. KJERNEROM
D. BRUKERROM
E. KOMPAKTKODE
F. OPENSSL
G. NØKKELPAR
H. TCPOGUDP

DEFINISJONER OG TILHØRENDE FELT	
	1. Kryptografibibliotek som OpenVPN er avhengig av for chifferalgoritmer.
	2. Utførelsesområde i operativsystemet der WireGuard kjører for hastighet.
	3. Robust eldre protokoll med en stor, kompleks konfigurasjonskodebase.
	4. Asymmetriske nøkler som WireGuard bruker til å verifisere peer-tilkoblinger.
	5. Transportprotokoller som OpenVPN støtter; WireGuard selv kjører bare over UDP.
	6. Den kompakte størrelsen på WireGuards kodebase, som gjør den mye enklere å revidere.
	7. Moderne VPN-protokoll utformet for høy hastighet og enkel kodegjennomgang.
	8. Utførelsesområde der OpenVPN kjører, noe som skaper overhead ved kontekstbytte.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale VPN-begreper. Skriv svarene dine i de utfyllbare svarboksene.

1. **UGEIWARDR** _____
2. **MKORJERNE** _____
3. **KTKKMODEAOP** _____
4. **ERAKPLNØK** _____
5. **VNNEOPP** _____
6. **OKRRRBEMU** _____
7. **OSSLPNE** _____
8. **OCGPTDUP** _____

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Grunner til å velge WireGuard			
2	Løfter en god VPN-leverandør gir			
3	Grunner til å velge OpenVPN			
4	Grunner til å bruke en VPN på reise			
5	Ting internettleverandøren din kan se			
6	Måter å gjenkjenne et falskt Wi-Fi-nettverk på			
7	Myter om VPN-er			
8	Steder der du ville brukt en VPN			
9	Raske ting i hverdagen			
10	Ting en VPN ikke kan beskytte deg mot			
11	Ting som gjør kode lettere å kontrollere			
12	Ting en VPN kan skjule			
13	Forskjeller mellom WireGuard og OpenVPN			
14	Ord knyttet til personvern			
15	Krypteringsnavn du kjenner til			

Kontrollpunkt 8: Casestudier om VPN

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

SARAH (STUDENT PÅ KAFÉ)

👩‍💻 «Hei! Jeg sitter på kafeens Wi-Fi, og VPN-appen min lar meg velge WireGuard eller OpenVPN. Videosamtalene mine faller stadig ut når jeg går mellom kafénettverket og hotspotten på telefonen min. Hvilken protokoll bør jeg velge, og hvorfor vil den håndtere byttet bedre?»

ALEX (REISENDE STUDENT)

👩‍💻 «Jeg er i utlandet på et hotellnettverk som ser ut til å blokkere det meste av VPN-trafikk. WireGuard vil ikke koble til i det hele tatt, men jeg må få tilgang til skolens ressurser hjemme. Hva er sannsynligvis det som blokkeres, og hvordan kan OpenVPN hjelpe meg å komme gjennom?»

Kontrollpunkt 9: Knekk chifferet

For å fullføre treningen i protokollrevisjon må du dekryptere denne skjulte meldingen om kjøring i kjerneområdet.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

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

15	16	16	7	18	1	4	5	18		15	16	5	14	22	16	14		13	5	4
		5	14		18	1	19	11	5	18	5		20	21	14	14	5	12		

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del A)

Gå gjennom de vanligste spørsmålene og svarene potensielle kunder har om bruk av virtuelle private nettverk.

Q1: Hva er en VPN, og hvordan fungerer den?

Et virtuelt privat nettverk (VPN) krypterer internettforbindelsen din og ruter trafikken gjennom en sikker ekstern server. Dette maskerer den offentlige IP-adressen din og begrenser hva observatører på lokale nettverk og internettleverandøren din kan se om trafikk som rutes gjennom VPN-tunnelen.

Q2: Hvorfor er protokoller viktige?

Protokollen bestemmer hvordan VPN-en din bygger tunnelen, hvilken kryptografi som beskytter dataene dine, og hvor raskt den kobler til og kobler til på nytt. WireGuard og OpenVPN er de to protokollene med åpen kildekode som de fleste VPN-apper tilbyr, og de gjør ulike avveininger mellom enkelhet, hastighet og konfigurerbarhet.

Q3: Er en av dem mer privat enn den andre?

Ingen av protokollene gjør deg anonym. Begge krypterer tunneltrafikken med sterke chiffer; personvernet ditt avhenger hovedsakelig av hva VPN-leverandøren logger og hvordan den håndterer nøkler, kontoer og servere.

Q4: Vil en VPN gjøre internetthastigheten min tregere?

Ja, litt. Krypteringsprosessen og den fysiske avstanden til VPN-serveren gir ekstra ventetid og belastning. Effekten varierer med leverandør, protokoll, serveravstand, enhet og nettverksforhold.

Q5: Er begge åpen kildekode?

Ja. WireGuard og OpenVPN-fellesskapsutgaven publiserer begge kildekoden sin, slik at uavhengige forskere kan gjennomgå dem. WireGuards lille kodebase gjør en full gjennomgang mye raskere.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del B)

Gå gjennom de vanligste spørsmålene og svarene potensielle kunder har om bruk av virtuelle private nettverk.

Q6: Hvilken er raskest?

WireGuard er vanligvis raskere: det kjører i kjernen, bruker slank ChaCha20-Poly1305-kryptering og fullfører handshakes raskt. OpenVPN har mer overhead, men reelle hastigheter avhenger også av serverbelastning og avstand.

Q7: Kan begge kjøre over både TCP og UDP?

Nei. OpenVPN kan kjøre over UDP eller TCP, og TCP-modus hjelper på nettverk som blokkerer UDP. WireGuard sender pakkene sine bare over UDP, så det kan svikte på nettverk som bare tillater TCP. [4]

Q8: Hvordan velger jeg den beste VPN-en?

Se etter revisjonsgodkjente policyer om ingen logging, sterke protokoller (WireGuard, OpenVPN), sikre serverplasseringer, høy hastighet, servere som kun bruker RAM, en kill switch-funksjon og jurisdiksjon utenfor etterretningsallianser (som 5/9/14 Eyes).

Q9: Kan jeg bruke WireGuard og OpenVPN på telefonen min?

Ja. WireGuard er på tvers av plattformer, med apper for Windows, macOS, Linux, iOS og Android, og OpenVPN-klienter finnes for de samme systemene. De fleste VPN-apper lar deg velge den ene eller den andre. [1]

Q10: Hvorfor er WireGuard så lite?

WireGuard støtter ett fast sett med moderne chiffer i stedet for mange valg. Linux-implementeringen trenger under 4000 kodelinjer, noe som gjør den enklere å gjennomgå enn større VPN-kodebaser. [3]

Kontrollpunkt 10: Avanserte vanlige spørsmål om VPN (Del C)

Utforsk tekniske og strukturelle sider ved virtuelle private nettverk og sikre tunnelprotokoller.

Q1: Hva er forskjellen mellom WireGuard, OpenVPN og IKEv2?

WireGuard er en moderne, lettvekts protokoll (bare ca. 4000 kodelinjer) som gir høy hastighet og raske tilkoblingstider. OpenVPN er en svært sikker, velprøvd protokoll med åpen kildekode. IKEv2 er utmerket for mobile enheter fordi den kan koble til igjen raskt når du bytter nettverk.

Q2: Hvilke chiffer bruker WireGuard?

WireGuard bruker ChaCha20 med Poly1305 til kryptering, Curve25519 til nøkkelutveksling, BLAKE2s til hashing og Noise-rammeverket til handshake. Det finnes ingen forhandling om chiffer, så brukerne kan ikke velge et svakt alternativ. [2]

Q3: Hvilke chiffer og biblioteker kan OpenVPN bruke?

OpenVPN er tett integrert med OpenSSL-biblioteket og bruker TLS til å utveksle nøkler. Administratorer kan velge chiffer for datakanalen, for eksempel AES-256-GCM, noe som gir fleksibilitet, men også rom for svake innstillinger. [4]

Q4: Hvordan autentiserer hver protokoll motparter?

WireGuard-peers identifiserer hverandre med statiske offentlige nøkler, omtrent som å utveksle SSH-nøkler, og hver nøkkel er knyttet til tillatte tunnel-IP-er. OpenVPN bruker vanligvis en sertifiseringsinstans med X.509-sertifikater, ofte kombinert med brukernavn og passord.

Q5: Hvordan omgår obfuskering VPN-blokkeringer?

Obfuskering (eller «Stealth VPN») skjuler VPN-trafikk slik at den ser ut som vanlig HTTPS-trafikk (port 443). Dette kan hjelpe den med å komme forbi dyp pakkeinspeksjon (DPI), som myndigheter eller skole- og kontornettverk bruker for å blokkere VPN.

Kontrollpunkt 10: Avanserte vanlige spørsmål om VPN (Del D)

Utforsk tekniske og strukturelle sider ved virtuelle private nettverk og sikre tunnelprotokoller.

Q6: Hva skjer når jeg bytter fra Wi-Fi til mobilnett?

WireGuard er tilkoblingsløst: det sender pakker fra den nye adressen, og tunnelen fortsetter etter et raskt handshake. OpenVPN beholder øktstatus, så et nettverksbytte kan kreve en ny tilkobling som tar litt lengre tid.

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

PFS sørger for at det genereres en unik, midlertidig krypteringsnøkkel for hver eneste økt. Selv om en privat nøkkel skulle bli kompromittert i fremtiden, kan den ikke brukes til å dekryptere tidligere eller fremtidige økter, fordi de brukte uavhengige nøkler.

Q8: Er OpenVPN fortsatt et godt valg hvis WireGuard er raskere?

Ja. OpenVPN er moden og mye brukt, kjører over TCP når UDP er blokkert, og støtter sertifikatbaserte bedriftsoppsett. Mange leverandører tilbyr begge protokollene, slik at brukere kan bytte hvis den ene er blokkert eller treg.

Q9: Hvilke porter bruker de?

OpenVPNs standardport er 1194, men den kan flyttes til en hvilken som helst UDP- eller TCP-port, inkludert 443. WireGuard lytter på en UDP-port som angis i konfigurasjonen; 51820 er porten som brukes i de offisielle eksemplene.

Q10: Hvilken protokoll er enklest å sette opp for hånd?

WireGuard er vanligvis enklere: generer et nøkkelpar, utveksle offentlige nøkler og list opp tillatte IP-er. OpenVPN trenger sertifikater, en CA og flere alternativer, selv om .ovpn-profiler samler dem i én fil.

Del 11: 10 interessante fakta om VPN og innsikt fra virkeligheten

Gå gjennom disse verdifulle, virkelighetsnære fakta og innsiktene om historien, markedet og teknologien bak VPN-er.

1. FØRSTE VPN-PROTOKOLL

PPTP (Point-to-Point Tunneling Protocol) ble utviklet av en leverandørgruppe som blant annet omfattet Microsoft, og ble publisert som RFC 2637 i juli 1999 for å støtte VPN-er for ekstern tilgang. [6]

2. TO TRANSPORTER

OpenVPN kan føre tunnelen over UDP eller TCP, og i TLS-modus deler kontroll- og datakanalene én enkelt port. [4]

3. WIREGUARD-REVOLUSJONEN

WireGuard har en svært strømlinjeformet kodebase som er utformet for effektivitet, noe som gjør det enklere å gjennomgå for sikkerhetssårbarheter enn tradisjonelle protokoller. [3]

4. MODERNE KRYPTOGRAFI

WireGuard kombinerer ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 og HKDF i Noise-protokollrammeverket, uten krypteringsvalg som brukerne kan ta feil på. [2]

5. OPENSSL I OPENVPN

OpenVPN er tett integrert med OpenSSL-biblioteket og henter mange av sine kryptografiske egenskaper fra det, blant annet TLS som brukes til å utveksle nøkler. [4]

6. DYP PAKKEINSPEKSJON

Deep Packet Inspection (DPI) undersøker pakkeinnhold og trafikkmønstre, ikke bare overskrifter, og noen brannmurer bruker det til å oppdage og blokkere vanlige VPN-protokoller.

7. SSH-LIGNENDE NØKLER

WireGuard-tilkoblinger settes opp ved å utveksle enkle offentlige nøkler, omtrent som å utveksle SSH-nøkler, uten at det trengs en sertifiseringsinstans. [1]

8. PÅ TVERS AV PLATTFORMER

WireGuard ble først utgitt for Linux-kjernen og er nå tilgjengelig for Windows, macOS, BSD, iOS og Android, så den samme protokollen fungerer på de fleste enheter. [1]

9. FRAMOVERHEMMELIGHOLD

WireGuard gjentar Noise_IK-handshaket sitt med noen minutters mellomrom for å rotere de symmetriske øktnøklene, noe som gir perfect forward secrecy selv om en langtidsnøkkel senere lekker ut. [2]

10. TUN/TAP-GRENSESNITT

OpenVPN er utformet for å fungere med det virtuelle nettverksgrensesnittet TUN/TAP, som er tilgjengelig på de fleste plattformer og bærer tunnelens pakker. [4]

Tekniske referanser og kilder

Siterte publikasjoner, kryptografiske spesifikasjoner og offisielle dokumentstandarder som er brukt i dette arbeidsarket.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[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

Fasit: Sammenligning av WireGuard- og OpenVPN-protokoller, kodebasestørrelser, hastighet og kryptografiske standarder

1 **WireGuards kodestørrelse** PROTOKOLLER — **Riktig svar: D**

MERKNAD TIL LÆREREN

WireGuard er ekstremt kompakt og kjører på omtrent 4000 kodelinjer. Dette holder angrepsflaten liten og gjør gjennomgang enklere.

2 **Hastighet i kjerneområdet** LATENS — **Riktig svar: B**

MERKNAD TIL LÆREREN

Ved å kjøre direkte i kjerneområdet unngår WireGuard belastningen fra kontekstbytter, noe som gir høy gjennomstrømming.

3 **Spørsmål 3** — **Riktig svar: B**

MERKNAD TIL LÆREREN

OpenVPN er tett integrert med OpenSSL, som leverer chiffer som AES-GCM og gjør den svært konfigurerbar, men mer kompleks.

4 **Protokollytelse** RUTINGKONTROLLER — **Riktig svar: A**

MERKNAD TIL LÆREREN

WireGuard etablerer handshakes på millisekunder og reagerer umiddelbart på nettverksroaming (f.eks. når du bytter fra Wi-Fi til mobilnett).

5 **Asymmetrisk kryptografi** PERSONVERN — **Riktig svar: C**

MERKNAD TIL LÆREREN

WireGuard bruker Cryptokey Routing, som knytter offentlige nøkler til tillatte tunnel-IP-adresser, på lignende måte som oppsett med SSH.

Fasit: Kontrollpunkt 2 – sant eller usant

6 Spørsmål 6

Riktig svar: Sant

MERKNAD TIL LÆREREN

WireGuards Linux-implementasjon er på under 4,000 linjer, så sikkerhetsteam kan gå gjennom den langt raskere enn mye større VPN-kodebaser som OpenVPN.

7 Forsinkelse i brukerrommet HASTIGHETER

Riktig svar: Usant

MERKNAD TIL LÆREREN

OpenVPN kjører i brukerområdet og sender pakker frem og tilbake fra det virtuelle grensesnittet i kjernen, noe som gir overhead ved kontekstbytter (med mindre kjerneavlasting som OpenVPN DCO brukes).

8 OpenVPN-konfigurasjon SNIFFINGRISIKO

Riktig svar: Sant

MERKNAD TIL LÆREREN

OpenVPN støtter kjøring over TCP (for pålitelighet og for å komme forbi brannmurer) eller UDP (for hastighet), noe som gjør det kompatibelt med komplekse bedriftsbrannmurer.

9 Moderne kryptografi BRANNMURER

Riktig svar: Sant

MERKNAD TIL LÆREREN

WireGuard forkaster eldre chiffer til fordel for moderne, sikre primitiver som ChaCha20 og Poly1305, som kjører raskt på mobile CPU-er.

10 Forenkling med nøkkelpar INGEN LOGGING

Riktig svar: Usant

MERKNAD TIL LÆREREN

WireGuard bruker ikke sertifikater eller komplekse CA-hierarkier. Det bygger på enkle par av offentlige og private nøkler som utveksles mellom peers.

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

G 1. WireGuard	H 2. OpenVPN	E 3. Kjerneområde	A 4. Brukerområde
B 5. 4 000 LINJER	C 6. OpenSSL	F 7. Nøkkelpar	D 8. TCP/UDP

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 WIREGUARD	2 OPENVPN	3 KJERNEROM	4 BRUKERROM
5 NØKKELPAR	6 REVIDERBARHET		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 F – OPENSSL	2 C – KJERNEROM	3 B – OPENVPN	4 G – NØKKELPAR
5 H – TCPOGUDP	6 E – KOMPAKTKODE	7 A – WIREGUARD	8 D – BRUKERROM

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare WireGuard, OpenVPN og Kjerneområde med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

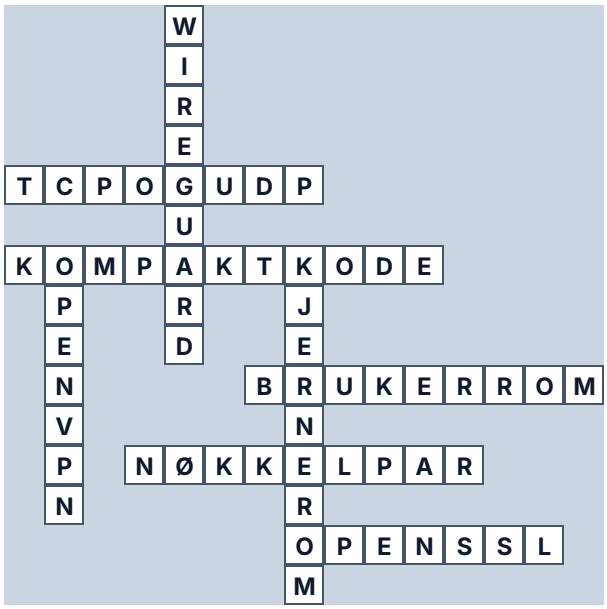
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

2 vannrett: TCPOGUDP Transportprotokoller som OpenVPN støtter; WireGuard selv kjører bare over UDP (8 bokstaver)

3 vannrett: KOMPAKTKODE Den kompakte størrelsen på WireGuards kodebase, som gjør den mye enklere å revidere (11 bokstaver)

6 vannrett: BRUKERROM Utførelsesområde der OpenVPN kjører, noe som skaper overhead ved kontekstbytte (9 bokstaver)

7 vannrett: NØKKELPAR Asymmetriske nøkler som WireGuard bruker til å verifisere peer-tilkoblinger (9 bokstaver)

8 vannrett: OPENSSL Kryptografibibliotek som OpenVPN er avhengig av for chifferalgoritmer (7 bokstaver)

LODDRETT

1 loddrett: WIREGUARD Moderne VPN-protokoll utformet for høy hastighet og enkel kodegjennomgang (9 bokstaver)

4 loddrett: OPENVPN Robust eldre protokoll med en stor, kompleks konfigurasjonskodebase (7 bokstaver)

5 loddrett: KJERNEROM Utførelsesområde i operativsystemet der WireGuard kjører for hastighet (9 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1.	U G E I W A R D R	WIREGUARD	5.	V N N E O P P	OPENVPN
2.	M K O R J E R N E	KJERNEROM	6.	O K R R R B E M U	BRUKERROM
3.	K T K K M O D E A O P	KOMPAKTKODE	7.	O S S L P N E	OPENSSL
4.	E R A K P L N Ø K	NØKKELPAR	8.	O C G P T D U P	TCPOGUDP

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"OPPGRADER OPENVPN MED EN RASKERE TUNNEL"

Fasit til casestudiene

A Scenario A: Valg av protokoll

SNIFFING OG KRYPTERING | Sarahs dilemma

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Anbefaling: WireGuard. Den lette, tilkoblingsløse utformingen gjør at tunnelen raskt kommer seg når nettverket hennes endres, og ChaCha20-Poly1305 holder krypteringen rask.
- Sikkerhet: Begge protokollene krypterer trafikken hennes på kafeens Wi-Fi, så begge beskytter påloggingene hennes når de er riktig konfigurert. Valget påvirker hovedsakelig hastighet og stabilitet.

B Scenario B: Komme forbi VPN-blokkeringer

GEOBLOKKERING OG IP-ADRESSER | Alex' dilemma

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Hvorfor blokkert: WireGuard bruker bare UDP, og hotellets brannmur blokkerer sannsynligvis UDP eller gjenkjenner WireGuard-pakker gjennom filtrering eller dyp pakkeinspeksjon.
- Slik hjelper OpenVPN: Den kan kjøre over TCP, inkludert port 443 som brukes av HTTPS, og hotellbrannmurer blokkerer sjelden denne helt, fordi nettsurfing er avhengig av den.