Navn: _____ Dato: _____ Poeng: _____

Mullvads sikkerhet

Analyse av sikkerhetsarkitekturen til Mullvad VPN, inkludert diskløse servere med bare RAM, reviderte retningslinjer uten logging, lokal nøkkelgenerering, WireGuard-kryptering og kvantebestandige tunnelkonfigurasjoner.

LÆRINGSOVERSIKT: MULLVADS SIKKERHET

ELEV
STUDENTSTATUS
Spor for nettverksforsvarere

SIKKER
TILKOBLINGSSTATUS
Beskytte datapakker

AKTIV
LEKKASJEBESKYTTELSE
DNS- og IPv6-lekkasjebeskyttelse

Velkommen! Dette aktivitetsheftet veileder deg gjennom sikkerhetsarkitekturen til Mullvad. Du utforsker diskløse servere som bare bruker RAM, reviderte policyer om null logger, lokal nøkkelgenerering og kvanteresistente tunneler.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk VPN- og nettverkssikkerhetskonfigurasjoner.**
- [ ] **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 veiledning om de beste VPN-ene

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

Din læringsveiledning for Mullvad-sikkerhet

- Analyser den tekniske arkitekturen og konfigurasjonsreglene for Mullvad Security.
- Konfigurer klientinnstillinger for å hindre lekkasjer av IP-, DNS- og WebRTC-trafikk.
- Sammenlign egendefinerte priser, prøveperioder og ytelsesfunksjoner med standardmodeller.

INSTRUKSJONER FOR GUIDE TIL MULLVADS SIKKERHET

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på Mullvads serverkontroller med personvern i fokus. Avslutt med bonusaktiviteten Tenk raskt.

VURDERING AV INFRASTRUKTUR MED ANONYMITET FØRST OG RAM-NIVÅER (INNLEDNING)

Mullvad bruker ikke vanlige kontoer med passord, men baserer seg på tilfeldig genererte 16-sifrede koder. Infrastrukturen er bygget med diskløse noder som kun bruker RAM, WireGuard-nøkler som genereres lokalt og reviderte policyer om ingen datalagring.

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

Kontrollpunkt 1: Flervalgsutfordring

1. Hvilken tunnelprotokoll er standard i Mullvads app?

- A) OpenVPN
- B) WireGuard
- C) IKEv2
- D) PPTP

2. Hva krever Mullvad for å opprette en ny konto?

- A) Ingenting i det hele tatt
- B) E-postadresse
- C) Telefonnummer
- D) ID-dokument

3. Hvilken kryptografisk tunnel beskytter mot kvantedatamaskiner?

- A) AES-256-GCM
- B) Kvante-WireGuard
- C) RSA-4096
- D) SOCKS5-proxy

4. Hvilken sikkerhetsmekanisme blokkerer risikoen for WebRTC-lekkasjer?

- A) Nettleserutvidelse
- B) Nettverks-kill switch
- C) Ruting av WebRTC gjennom VPN-grensesnittet
- D) Split Tunneling

5. Hvilken multihop-funksjon ruter trafikk gjennom flere noder?

- A) Dobbel NAT
- B) WireGuard Multihop
- C) Chameleon-protokoll
- D) Bypasser

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Mullvad krever en e-postadresse når kontoen genereres.

○ Sant ○ Usant

7 Spørsmål 7

7. SOCKS5-proxyer kan konfigureres inne i Mullvad-tunneler.

○ Sant ○ Usant

8 Spørsmål 8

8. Mullvad eier og driver all sin servermaskinvare.

○ Sant ○ Usant

9 Spørsmål 9

9. Network Kill Switch er alltid aktiv som standard.

○ Sant ○ Usant

10 Spørsmål 10

10. Kontantbetalinger sendt i posten kan ikke refunderes i det hele tatt.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Mullvad bygger på _____ som sin viktigste raske og sikre tunnelprotokoll.
2. Å rute data gjennom to serverplasseringer kalles _____ -konfigurasjon.
3. For å hindre datalogger på disk bruker Mullvad _____ dedikerte noder.
4. Systemtrafikk blokkeres når en tunnel svikter, via den innebygde _____ -sikringen.
5. Revisjonserklæringer bekrefter at Mullvad opprettholder en streng, verifisert policy om _____ .
6. Intern applikasjonsruting kan isoleres med et tilpasset _____ -oppsett.
7. Postkvantealgoritmer for kryptering sikrer data inne i en _____ tunnel.
8. Private navneservere er utplassert globalt for å bidra til å blokkere farlige _____ .

ORDBANK

DNS-LEKKASJER | INGEN LOGGER | KILL SWITCH | KVANTESIKKER | MULTI-HOP | RAM-BASERTE | SOCKS5 | WIREGUARD

Skriv svarene dine her:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Kontrollpunkt 4: Koble VPN- og nettverksbegreper

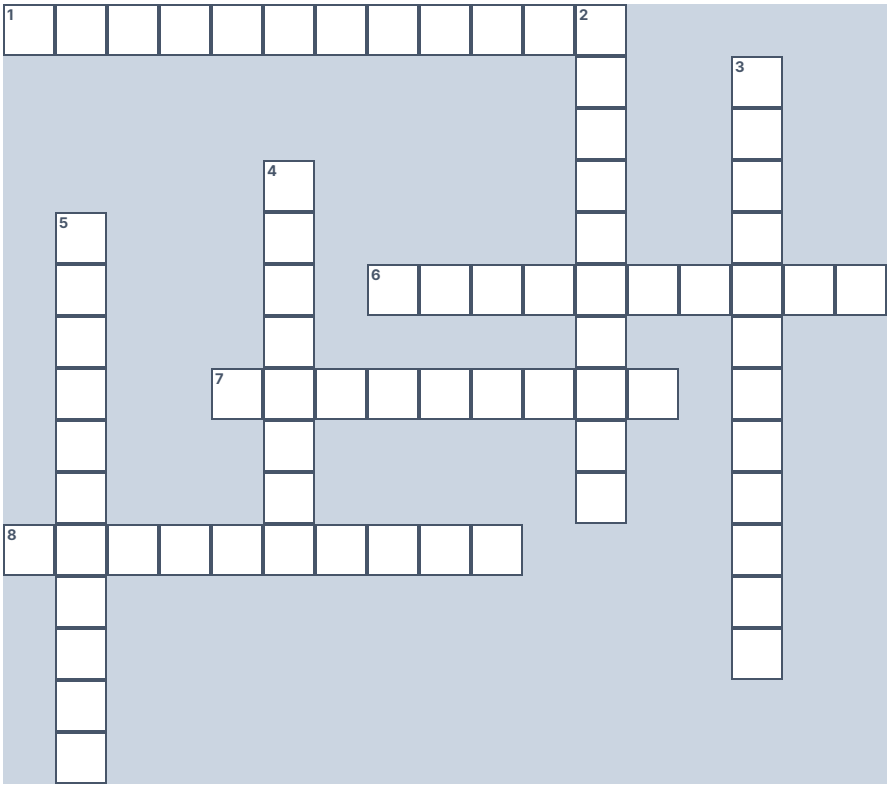
KOBLE DEFINISJONER

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	En sikkerhetsfunksjon som kutter trafikken når en VPN faller ut.
☐	2. MULTI-HOP	B	En lett og høytytende sikker tunneleringsprotokoll.
☐	3. KUN RAM	C	En intern proxyprotokoll som brukes til å isolere klientapplikasjoner.
☐	4. KILL SWITCH	D	Ruting av trafikk gjennom en inngangs- og en utgangsservernode.
☐	5. INGEN LOGGER	E	Krypteringsmekanismer utformet for å motstå kvanteangrep.
☐	6. SOCKS-PROXY	F	Eksponering av DNS-forespørslenes mål utenfor VPN-tunnelen.
☐	7. KVANTESIKKER	G	Servermaskinvare med flyktig minne som ikke beholder data ved omstart.
☐	8. DNS-LEKKASJER	H	Datastandard uten lagring, verifisert av uavhengige revisjoner.

Kontrollpunkt 5: Kryssord

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



VANNRETT

1. Eksponering av destinasjonene for DNS-forespørsler utenfor VPN-tunnelen (12)

6. En sikkerhetsfunksjon som kutter trafikken når en VPN faller ut (10)

7. En lett, høytytende og sikker tunnelprotokoll (9)

8. En intern proxyprotokoll (SOCKS5) som brukes til å isolere klientapplikasjoner (10)

LODDRETT

2. Servermaskinvare med flyktig minne som ikke beholder data ved omstart (10)

3. Krypteringsmekanismer utformet for å motstå kvanteangrep (12)

4. Ruting av trafikk gjennom en inngangs- og en utgangsservernode (8)

5. Standard for null datalagring, verifisert av uavhengige revisjoner (11)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

1 vannrett: Eksponering av destinasjonene for DNS-forespørsler utenfor VPN-tunnelen (12 bokstaver):

6 vannrett: En sikkerhetsfunksjon som kutter trafikken når en VPN faller ut (10 bokstaver):

7 vannrett: En lett, høytytende og sikker tunnelprotokoll (9 bokstaver):

8 vannrett: En intern proxyprotokoll (SOCKS5) som brukes til å isolere klientapplikasjoner (10 bokstaver):

LODDRETT

2 loddrett: Servermaskinvare med flyktig minne som ikke beholder data ved omstart (10 bokstaver):

3 loddrett: Krypteringsmekanismer utformet for å motstå kvanteangrep (12 bokstaver):

4 loddrett: Ruting av trafikk gjennom en inngangs- og en utgangsservernode (8 bokstaver):

5 loddrett: Standard for null datalagring, verifisert av uavhengige revisjoner (11 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

WIREGUARD MULTIHOP RAMBASERTE KILLSWITCH INGENLOGGER
SOCKSPROXY KVANTESIKKER DNSLEKKASJER

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. MULTIHOP**
- **C. RAMBASERTE**
- **D. KILLSWITCH**
- **E. INGENLOGGER**
- **F. SOCKSPROXY**
- **G. KVANTESIKKER**
- **H. DNSLEKKASJER**

DEFINISJONER OG TILHØRENDE FELT

_____ 1. En intern proxyprotokoll (SOCKS5) som brukes til å isolere klientapplikasjoner.

_____ 2. Krypteringsmekanismer utformet for å motstå kvanteangrep.

_____ 3. En lett, høytytende og sikker tunnelprotokoll.

_____ 4. Servermaskinvare med flyktig minne som ikke beholder data ved omstart.

_____ 5. En sikkerhetsfunksjon som kutter trafikken når en VPN faller ut.

_____ 6. Ruting av trafikk gjennom en inngangs- og en utgangsservernode.

_____ 7. Eksponering av destinasjonene for DNS-forespørsler utenfor VPN-tunnelen.

_____ 8. Standard for null datalagring, verifisert av uavhengige revisjoner.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper om virtuelle private nettverk (VPN). Skriv svarene dine i svarboksene.

1. UGEIWARDR
2. TBRAAEERSM
3. IOLGGNERNG E
4. EITASREKKKV N
5. IHUPTMOL
6. CSLITKIWHL
7. OKSRPOXYSC
8. ASEJKRDKNE SL

Bonusaktivitet: Tenk raskt

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

1	Sikkerhetsfunksjoner i Mullvad			
2	Spørsmål til kundestøtten i Mullvad			
3	Måter å lage et sterkt passord på			
4	Personer du ville anbefalt Mullvad til			
5	Ting en revisjon kan kontrollere			
6	Land kjent for sterk personvernlovgivning			
7	Ting du gjør på nettet hver dag			
8	Land der du ville hatt Mullvad-servere			
9	Innstillinger du slår på for ekstra sikkerhet			
10	Ting kryptering beskytter			
11	Typer VPN-lekkasjer			
12	Sikkerhetsord du lærte i dette arbeidsarket			
13	Trusler på offentlig Wi-Fi			
14	Apper du ville brukt sammen med Mullvad			
15	Enheter du ville installert Mullvad på			

Kontrollpunkt 8: Casestudier om VPN og nettverk

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

CASESTUDIE 1: INTEGRERING AV KVANTERESISTENS



Scenario: Et finansselskap må sikre filoverføringer mot fremtidig kvantedekryptering.

Diskusjonsspørsmål: Hvilken tunnelkonfigurasjon bør de ta i bruk i Mullvads app?

CASESTUDIE 2: DISKRET UNDERSØKENDE RUTING



Scenario: En etterforsker vil dobbeltrute nettverket sitt for å maskere inngangspunktet.

Diskusjonsspørsmål: Hvilken Mullvad-funksjon bør aktiveres for å oppnå ruting via flere servere?

Kontrollpunkt 9: Knekk chifferet

En nettverksingeniør sikrer rutingkanaler og klienttunneler. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

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

13	21	12	12	22	1	4		2	18	21	11	5	18		22	5	18	11	5	14
	16	1	19	19	15	18	4		5	12	12	5	18		5	16	15	19	20	

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 om virtuelle private nettverk (VPN-er) og tunnelering.

Q1: Hvordan sikrer Mullvad kontoer?

Mullvad bruker et generert 16-sifret kontonummer uten krav om passord eller e-post. [1]

Q2: Hvilken protokoll prioriterer Mullvad?

Mullvad prioriterer WireGuard på grunn av hastigheten, enkelheten og den moderne kryptografien. [9]

Q3: Blir Mullvad-serverne revidert?

Ja, sikkerhetsfirmaer fra tredjepart gjennomfører jevnlige revisjoner av infrastruktur og kode.

Q4: Støtter Mullvad OpenVPN?

Nei, Mullvad fjernet OpenVPN 15. januar 2026; det er kun WireGuard. [7]

Q5: Hva er Mullvads kill switch?

Det er en integrert brannmurregel som hindrer internettrafikk hvis VPN-en svikter.

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

Gå gjennom de vanligste spørsmålene og svarene om virtuelle private nettverk (VPN-er) og tunnelering.

Q6: Støttes IPv6 av Mullvad?

Ja, Mullvad støtter innebygd IPv6-ruting og lekkasjebeskyttelse.

Q7: Tilbyr Mullvad multihop?

Ja, WireGuard multihop gjør det mulig å lenke flere serverlokasjoner.

Q8: Kan jeg bruke egendefinerte DNS-resolvere?

Ja, egendefinerte DNS-adresser kan konfigureres i innstillingene til Mullvad-klienten.

Q9: Hvordan forhindres logger?

Systemkonfigurasjoner slår av logging og rydder hurtigbuffere på alle serverdaemoner.

Q10: Hvor er Mullvad registrert?

Mullvad er registrert i Göteborg i Sverige, under svensk jurisdiksjon.

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

Utforsk avanserte tekniske sider ved VPN-tunnelprotokoller, integrering av mobilklienter og utrulling i bedrifter.

Q1: Hvordan fungerer nøkkelrotasjon?

Appen roterer WireGuard-nøkler automatisk; standardintervallet i kommandolinjen er 30 dager. [3]

Q2: Hva er kvantemotstandsdyktige tunneler?

De legger til nøkkelutveksling med ML-KEM og Classic McEliece i WireGuard for å motstå fremtidige kvanteangrep. [2]

Q3: Hvordan er servere som kun bruker RAM sikre?

Disse nodene skriver ingen data til harddisker, slik at tyveri av fysiske servere blir nytteløst.

Q4: Hva er SOCKS5-proxyfunksjonen?

Den hjelper til med å rute trafikk fra bestemte apper innenfor tunnelen og hindrer lekkasjer til eksterne nettverk.

Q5: Beskytter Mullvad mot WebRTC-lekkasjer?

Ja, appen tvinger WebRTC-forespørsler gjennom VPN-grensesnittet for å skjerme lokale IP-adresser.

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

Utforsk avanserte tekniske sider ved VPN-tunnelprotokoller, integrering av mobilklienter og utrulling i bedrifter.

Q6: Hvordan håndterer Mullvad politirazziaer?

Mullvad har ingen brukerdatabaselogger, noe som betyr at ingen brukeropplysninger kan hentes ut.

Q7: Hva er risikoen ved svensk jurisdiksjon?

Sverige er medlem av 14 Eyes, men Mullvads arkitektur med null logging fjerner datarisikoen.

Q8: Er revisjonene av klientappene åpen kildekode?

Ja, appene er åpen kildekode (GPL-3) og revidert av firmaer som X41 D-Sec. [6]

Q9: Hvordan fungerer split tunneling?

Den bruker operativsystemets rutingtabeller til å utelukke bestemte apper fra VPN-overhead.

Q10: Hvordan håndterer Mullvad kontantbetalinger?

Kontanter sendes med en tokenkode, godskrives manuelt, og konvoluttene makuleres.

Del 11: 10 fakta om VPN fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om VPN-krypteringshastigheter, protokollrevisjoner, mobiltilkobling og fjernarbeid i bedrifter.

1. VPN-INNSIKT

Mullvad ble grunnlagt i 2009 av Amagicom AB i Göteborg i Sverige.

2. VPN-INNSIKT

Kontonumre er den eneste identifikatoren som brukes til å godskrive og få tilgang til kontoer.

3. VPN-INNSIKT

Ingen navn, e-postadresser, passord eller telefonnumre lagres i brukerdatabasen.

4. VPN-INNSIKT

WireGuard-nøkler genereres lokalt på klientenheter for å hindre kompromittering på serversiden.

5. VPN-INNSIKT

Cure53s infrastrukturrevisjon fra 2024 fant ingen feil som bryter anonymiteten til VPN-trafikken. [5]

6. VPN-INNSIKT

Hver Mullvad WireGuard-server kjører en SOCKS5-proxy som bare er tilgjengelig i tunnelen. [8]

7. VPN-INNSIKT

WireGuard-trafikk kan obfuskeres med Shadowsocks, QUIC eller LWO for å passere brannmurer. [10]

8. VPN-INNSIKT

Mullvad fullførte overgangen til VPN-servere som kun bruker RAM i september 2023. [4]

9. VPN-INNSIKT

ML-KEM og Classic McEliece forhandler fram en post-kvantum forhåndsdelt nøkkel for WireGuard. [2]

10. VPN-INNSIKT

Kontantkonvolutter og innhold som ikke er penger makuleres etter at tiden er godskrevet.

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale tekniske standarder, spesifikasjoner og regelverk.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] Mullvad VPN. (n.d.). Why Mullvad VPN?
https://mullvad.net/en/why-mullvad-vpn

[2] Mullvad VPN. (n.d.). Quantum-resistant tunnels with WireGuard.
https://mullvad.net/en/help/quantum-resistant-tunnels-with-wireguard

[3] Mullvad VPN. (n.d.). CLI commands for using WireGuard.
https://mullvad.net/en/help/cli-command-wg

[4] Mullvad VPN. (2023). We have successfully completed our migration to RAM-only VPN infrastructure.
https://mullvad.net/en/blog/we-have-successfully-completed-our-migration-to-ram-only-vpn-infrastructure

[5] Mullvad VPN. (2024). Fourth Infrastructure audit completed by Cure53.
https://mullvad.net/en/blog/fourth-infrastructure-audit-completed-by-cure53

[6] Mullvad VPN. (2024). The report for the 2024 security audit of the app is now available.
https://mullvad.net/en/blog/the-report-for-the-2024-security-audit-of-the-app-is-now-available

[7] Mullvad VPN. (2024). Removing OpenVPN 15th January 2026.
https://mullvad.net/en/blog/removing-openvpn-15th-january-2026

[8] Mullvad VPN. (n.d.). SOCKS5 proxy.
https://mullvad.net/en/help/socks5-proxy

[9] Mullvad VPN. (n.d.). Why WireGuard?
https://mullvad.net/en/help/why-wireguard

[10] Mullvad VPN. (n.d.). Using Mullvad VPN in restrictive locations.
https://mullvad.net/en/help/connecting-to-mullvad-vpn-from-restrictive-locations

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

[12] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1

Riktig svar: B

MERKNAD TIL LÆREREN

Hvilken tunnelprotokoll er standard i Mullvads app? → WireGuard

2 Spørsmål 2

Riktig svar: A

MERKNAD TIL LÆREREN

Når du klikker på «generate account», får du et kontonummer; det spørres ikke etter e-post eller andre personopplysninger.

3 Spørsmål 3

Riktig svar: B

MERKNAD TIL LÆREREN

Mullvads kvanteresistente WireGuard-tunneler bruker ML-KEM og Classic McEliece for å bli enige om en forhåndsdelt nøkkel.

4 Spørsmål 4

Riktig svar: C

MERKNAD TIL LÆREREN

Hvilken sikkerhetsmekanisme blokkerer risikoen for WebRTC-lekkasjer? → Ruting av WebRTC gjennom VPN-grensesnittet

5 Spørsmål 5

Riktig svar: B

MERKNAD TIL LÆREREN

Hvilken multihop-funksjon ruter trafikk gjennom flere noder? → WireGuard Multihop

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Spørsmål 6** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Usant: Mullvad ber aldri om e-postadresse; kontoer identifiseres bare med et generert nummer.

7 **Spørsmål 7** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

SOCKS5-proxyer kan konfigureres inne i Mullvad-tunneler.

8 **Spørsmål 8** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Usant: Mullvad eier noen servere, men leier også dedikerte servere fra leverandører.

9 **Spørsmål 9** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Network Kill Switch er alltid aktiv som standard.

10 **Spørsmål 10** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Kontantbetalinger sendt i posten kan ikke refunderes i det hele tatt.

Fasit for ordforråd og vurderingsmatrise

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

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

B 1. WIREGUARD	D 2. MULTI-HOP	G 3. KUN RAM	A 4. KILL SWITCH
H 5. INGEN LOGGER	C 6. SOCKS-PROXY	E 7. KVANTESIKKER	F 8. DNS-LEKKASJER

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 WIREGUARD	2 MULTI-HOP	3 RAM-BASERTE	4 KILL SWITCH
5 INGEN LOGGER	6 SOCKS5	7 KVANTESIKKER	8 DNS-LEKKASJER

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 F – SOCKSPROXY	2 G – KVANTESIKKER	3 A – WIREGUARD	4 C – RAMBASERTE
5 D – KILLSWITCH	6 B – MULTIHOP	7 H – DNSLEKKASJER	8 E – INGENLOGGER

DISKUSJONSNOTATER TIL LÆRERE

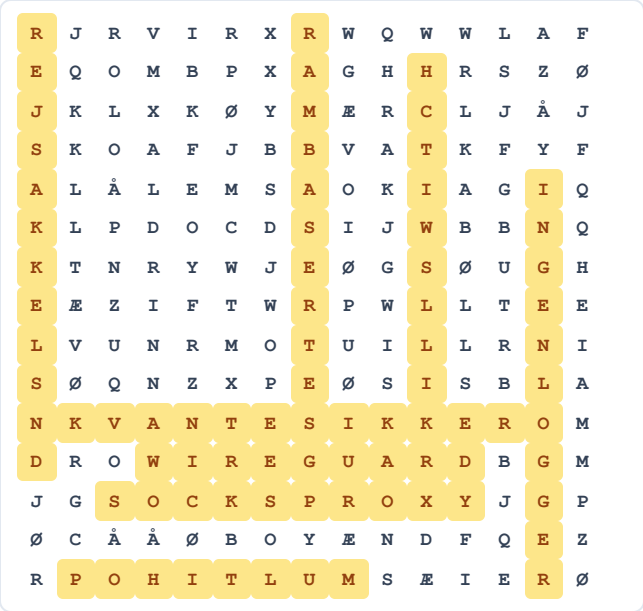
Nøkkelbegreper:
Kontroller at elevene kan forklare WIREGUARD, MULTI-HOP og KUN RAM med egne ord og gi et eksempel på hvert.

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

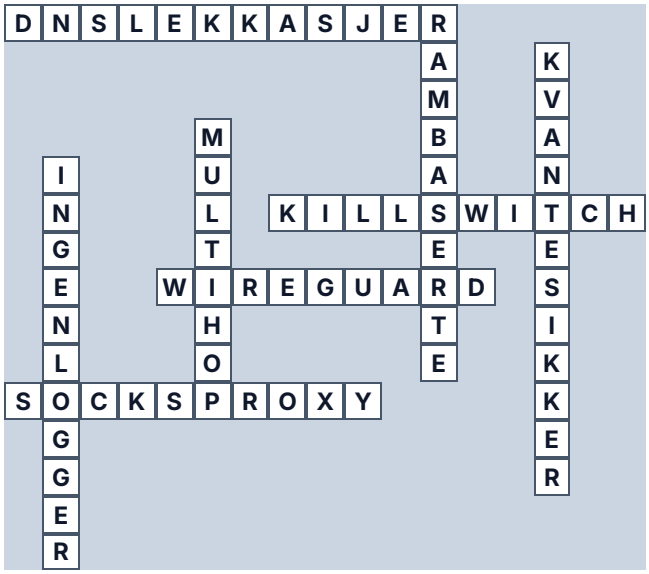
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET



KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

1 vannrett: DNSLEKKASJER Eksponering av destinasjonene for DNS-forespørsler utenfor VPN-tunnelen (12 bokstaver)

6 vannrett: KILLSWITCH En sikkerhetsfunksjon som kutter trafikken når en VPN faller ut (10 bokstaver)

7 vannrett: WIREGUARD En lett, høytytende og sikker tunnelprotokoll (9 bokstaver)

8 vannrett: SOCKSPROXY En intern proxyprotokoll (SOCKS5) som brukes til å isolere klientapplikasjoner (10 bokstaver)

LODDRETT

2 loddrett: RAMBASERTE Servermaskinvare med flyktig minne som ikke beholder data ved omstart (10 bokstaver)

3 loddrett: KVANTESIKKER Krypteringsmekanismer utformet for å motstå kvanteangrep (12 bokstaver)

4 loddrett: MULTIHOP Ruting av trafikk gjennom en inngangs- og en utgangsservernode (8 bokstaver)

5 loddrett: INGENLOGGER Standard for null datalagring, verifisert av uavhengige revisjoner (11 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.	I H U P T M O L	MULTIHOP
2.	T B R A A E E R S M	RAMBASERTE	6.	C S L I T K I W H L	KILLSWITCH
3.	I O L G G N E R N G E	INGENLOGGER	7.	O K S R P O X Y S C	SOCKSPROXY
4.	E I T A S R E K K K V N	KVANTESIKKER	8.	A S E J K R D K N E S L	DNSLEKKASJER

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"MULLVAD BRUKER VERKEN PASSORD ELLER EPOST"

Fasit til casestudiene

A CASESTUDIE 1: INTEGRERING AV KVANTERESISTENS

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Et finansselskap må sikre filoverføringer mot fremtidig kvantedekryptering.
- Anbefalt strategi og løsning: Ta i bruk kvanteresistente WireGuard-tunneler med post-kvante forhåndsdelte nøkler.

B CASESTUDIE 2: DISKRET UNDERSØKENDE RUTING

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En etterforsker vil dobbeltrute nettverket sitt for å skjule inngangspunktet.
- Anbefalt strategi og løsning: Aktiver Mullvads WireGuard Multihop-funksjon for å kaskadere inngangs- og utgangsnoder.