Navn: _____ Dato: _____ Poeng: _____

# Sikkerhet i ProtonVPN

Analyse av sikkerhetsarkitekturen til ProtonVPN, inkludert Secure Core-servere, NetShield DNS-filtrering, sveitsisk personvernjurisdiksjon, reviderte apper med åpen kildekode og Stealth-protokollen.

## LÆRINGSOVERSIKT: SIKKERHET I PROTONVPN

**ELEV**
**STUDENTSTATUS**
Spor for nettverksforsvarere

**SIKKER**
**TILKOBLINGSSTATUS**
Beskytte datapakker

**AKTIV**
**LEKKASJEBESKYTTELSE**
DNS- og IPv6-lekkasjebeskyttelse

**Velkommen!** Dette aktivitetsheftet veileder deg gjennom sikkerhetsarkitekturen til Proton VPN. Du skal utforske Secure Core-servere med dobbelt hopp, DNS-blokkering med NetShield, sveitsiske personvernlover og Stealth-tilsløring.

**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/protonvpn/sikkerhet/

# Din læringsveiledning for ProtonVPN-sikkerhet

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

## INSTRUKSJONER FOR VEILEDNINGEN OM SIKKERHET I PROTONVPN

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på Secure Core-ruting med dobbelt hopp og sveitsisk personvernstyring. Avslutt med bonusaktiviteten Tenk raskt.

## SECURE CORE-ARKITEKTUR MED DOBBELT HOPP OG SVEITSISK PERSONVERNJURISDIKSJON

Proton VPN beskytter brukertrafikken med Secure Core-servere som eies av Proton i Sveits, Island og Sverige, reviderte applikasjoner med åpen kildekode og Stealth-obfuskeringsprotokollen, som er utformet for å omgå dyp pakkeinspeksjon.

## (INTRODUKSJON)

Proton VPN beskytter brukertrafikken med Secure Core-servere som eies av Proton i Sveits, Island og Sverige, reviderte applikasjoner med åpen kildekode og Stealth-obfuskeringsprotokollen, som er utformet for å omgå dyp pakkeinspeksjon.

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

## Kontrollpunkt 1: Flervalgsutfordring

**1** **1. Hva slags anlegg huser Protons Secure Core-servere?**

- A) Virtuelle maskiner i offentlig sky
- B) Høysikkerhetsanlegg
- C) Offentlige datasentre
- D) Delte rack

**2** **2. Hvilken protokoll bidrar til å omgå streng sensur fra myndigheter?**

- A) PPTP
- B) Stealth-protokoll
- C) OpenVPN UDP
- D) IKEv2

**3** **3. Hva er funksjonen til Proton VPNs NetShield?**

- A) Speed Booster
- B) DNS-blokkering av annonser og skadevare
- C) Skylagring
- D) Portvideresending

**4** **4. Under hvilket lands personvernlover opererer Proton AG?**

- A) USA
- B) Storbritannia
- C) Sveits
- D) Panama

**5** **5. Hvordan blir klientappene til Proton VPN verifisert av eksperter?**

- A) Hemmelig kode
- B) Åpne revisjoner
- C) Proprietær lisens
- D) Myndighetsgjennomgang

## Kontrollpunkt 2: Utfordring med sant eller usant

**6 Spørsmål 6**

6. Secure Core ruter trafikken gjennom personvernvennlige land før utgangen.

○ Sant ○ Usant

**7 Spørsmål 7**

7. Sveits er medlem av 14 Eyes, alliansen for etterretningsovervåking.

○ Sant ○ Usant

**8 Spørsmål 8**

8. NetShield blokkerer annonser og ondsinnede domener direkte på DNS-nivå.

○ Sant ○ Usant

**9 Spørsmål 9**

9. Proton VPN-applikasjonene har 100 % åpen kildekode og er offentlig revidert.

○ Sant ○ Usant

**10 Spørsmål 10**

10. Stealth-protokollen bruker standard WireGuard-hoder uten tilsløring.

○ Sant ○ Usant

## Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Multi-hop-ruting gjennom Proton-eide servere i personvernvennlige land kalles _____ -arkitektur.

2. For å omgå dyp pakkeinspeksjon og nettverksbrannmurer aktiverer brukere _____ -modus.

3. Skadevaredomener, sporere og annonseskript filtreres av _____ -DNS.

4. Proton sier at de under _____ ikke er forpliktet til å føre logger over brukeraktivitet.

5. Hvis VPN-tunnelen kobles fra uventet, blokkeres internettrafikken av _____ -sikringen.

6. Uavhengige sikkerhetsforskere verifiserer klientens integritet fordi appene har _____ .

**ORDBANK**

AES-GCM | KILL SWITCH | NETSHIELD | SECURE CORE | STEALTH | SVEITSISK LOV | WIREGUARD | ÅPEN KILDEKODE

**Skriv svarene dine her:**

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

# Kontrollpunkt 4: Koble VPN- og nettverksbegreper

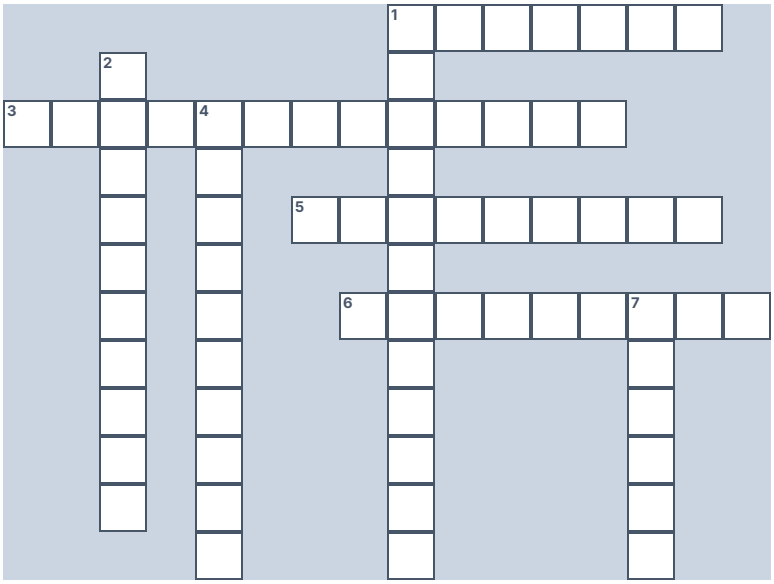
**KOBLE DEFINISJONER**

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

| | | | |
|---|---|---|---|
| ☐ | 1. SECURE CORE | A | Offentlig tilgjengelig og uavhengig revidert klientprogramvare. |
| ☐ | 2. STEALTH | B | Standard for symmetrisk chiffer som krypterer VPN-ens datapakker. |
| ☐ | 3. NETSHIELD | C | Strenge juridiske personvernlover i Sveits, utenfor jurisdiksjonene i 14 Eyes. |
| ☐ | 4. SVEITSISK LOV | D | En tilslørt tunneleringsprotokoll forkledd som vanlig HTTPS-nettrafikk. |
| ☐ | 5. KILL SWITCH | E | En moderne lett protokoll som gir robust kryptografi og høy hastighet. |
| ☐ | 6. ÅPEN KILDEKODE | F | Et DNS-basert filter som blokkerer annonser, telemetrisporere og skadevare. |
| ☐ | 7. WIREGUARD | G | Et multihopp-design som ruter trafikk gjennom Proton-eide servere i første hopp. |
| ☐ | 8. AES-GCM | H | Et sikkerhetsvern som stanser nettverksoverføring ved tilkoblingsbrudd. |

# Kontrollpunkt 5: Kryssord

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




## VANNRETT

**1. En tilsløret tunnelprotokoll forkledd som vanlig HTTPS-nettrafikk (7)**

**3. Offentlig tilgjengelig og uavhengig revidert klientprogramvare (13)**

**5. Et DNS-basert filter som blokkerer annonser, telemetrisporere og skadevare (9)**

**6. En moderne lett protokoll som gir robust kryptografi og høy hastighet (9)**

## LODDRETT

**1. Strenge juridiske personvernlover i Sveits, utenfor 14 Eyes-jurisdiksjonen (12)**

**2. En multi-hop-utforming som ruter trafikk gjennom Proton-eide servere som første hopp (10)**

**4. En sikkerhetsmekanisme som stanser nettverksoverføring ved tilkoblingsfall (10)**

**7. Symmetrisk chiffer av militær klasse som sikrer alle innkapslede VPN-datapakker (6)**

# Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

## VANNRETT

**1 vannrett: En tilsløret tunnelprotokoll forkledd som vanlig HTTPS-nettrafikk (7 bokstaver):**

**3 vannrett: Offentlig tilgjengelig og uavhengig revidert klientprogramvare (13 bokstaver):**

**5 vannrett: Et DNS-basert filter som blokkerer annonser, telemetrisporere og skadevare (9 bokstaver):**

**6 vannrett: En moderne lett protokoll som gir robust kryptografi og høy hastighet (9 bokstaver):**

## LODDRETT

**1 loddrett: Strenge juridiske personvernlover i Sveits, utenfor 14 Eyes-jurisdiksjonen (12 bokstaver):**

**2 loddrett: En multi-hop-utforming som ruter trafikk gjennom Proton-eide servere som første hopp (10 bokstaver):**

**4 loddrett: En sikkerhetsmekanisme som stanser nettverksoverføring ved tilkoblingsfall (10 bokstaver):**

**7 loddrett: Symmetrisk chiffer av militær klasse som sikrer alle innkapslede VPN-datapakker (6 bokstaver):**

## Kontrollpunkt 6: Skjult ordsøk

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

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

**ORDLISTE**

SECURECORE STEALTH NETSHIELD SVEITSISKLOV KILLSWITCH
ÅPENKILDEKODE WIREGUARD AESGCM

## 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. SECURECORE**
- **B. STEALTH**
- **C. NETSHIELD**
- **D. SVEITSISKLOV**
- **E. KILLSWITCH**
- **F. ÅPENKILDEKODE**
- **G. WIREGUARD**
- **H. AESGCM**

**DEFINISJONER OG TILHØRENDE FELT**

_____ 1. En tilsløret tunnelprotokoll forkledd som vanlig HTTPS-nettrafikk.

_____ 2. En moderne lett protokoll som gir robust kryptografi og høy hastighet.

_____ 3. Strenge juridiske personvernlover i Sveits, utenfor 14 Eyes-jurisdiksjonen.

_____ 4. En multi-hop-utforming som ruter trafikk gjennom Proton-eide servere som første hopp.

_____ 5. Symmetrisk chiffer av militær klasse som sikrer alle innkapslede VPN-datapakker.

_____ 6. En sikkerhetsmekanisme som stanser nettverksoverføring ved tilkoblingsfall.

_____ 7. Et DNS-basert filter som blokkerer annonser, telemetrisporere og skadevare.

_____ 8. Offentlig tilgjengelig og uavhengig revidert klientprogramvare.

## 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. **RCERESOEUC** _____
2. **DNLSEIEHT** _____
3. **KWCIISHLTL** _____
4. **GDREAUWIR** _____
5. **LHAESTT** _____
6. **VTKLSOSSVIEI** _____
7. **KODIÅPEKEDELN** _____
8. **SMACGE** _____

# Bonusaktivitet: Tenk raskt

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

| | | | | |
|---|---|---|---|---|
| 1 | Ting du gjør på nettet hver dag | | | |
| 2 | Land kjent for sterk personvernlovgivning | | | |
| 3 | Sikkerhetsfunksjoner i Proton VPN | | | |
| 4 | Typer VPN-lekkasjer | | | |
| 5 | Situasjoner der en kill switch hjelper | | | |
| 6 | Ting en revisjon kan kontrollere | | | |
| 7 | Innstillinger du slår på for ekstra sikkerhet | | | |
| 8 | Ting kryptering beskytter | | | |
| 9 | Ord som beskriver en god VPN-app | | | |
| 10 | Grunner til å velge Proton VPN | | | |
| 11 | Knapper eller menyer i en VPN-app | | | |
| 12 | Strømmetjenester du ser på | | | |
| 13 | Trusler på offentlig Wi-Fi | | | |
| 14 | Måter å lage et sterkt passord på | | | |
| 15 | Land der du ville hatt Proton VPN-servere | | | |

# Kontrollpunkt 8: Casestudier om VPN og nettverk

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

### CASESTUDIE 1: OMGÅ RESTRIKTIVE BRANNMURER

👷

**Scenario:** En bruker reiser til et land der vanlig VPN-trafikk som OpenVPN og WireGuard blokkeres av DPI.

**Diskusjonsspørsmål:** Hvilken protokollkonfigurasjon i Proton VPN gjør at brukeren kan omgå inspeksjon på statlig nivå?

### CASESTUDIE 2: AVANSERT BESKYTTELSE MOT MOTSTANDERE

👷

**Scenario:** En finansrevisor mistenker at den lokale internettleverandørens utgangsnode kan være kompromittert av avanserte vedvarende trusler.

**Diskusjonsspørsmål:** Hvordan beskytter Secure Core revisorens identitet mot at en utgangsnode blir kompromittert?

## 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

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 19 | 5 | 3 | 21 | 18 | 5 | | 3 | 15 | 18 | 5 | | 8 | 5 | 18 | 4 | 5 | 4 | 5 |
| | | | | | | | | | | | | | | | | | | |
| 19 | 5 | 18 | 22 | 5 | 18 | 5 | | 2 | 5 | 19 | 11 | 25 | 20 | 20 | 5 | 18 | | |
| | | | | | | | | | | | | | | | | | | |
| | | 2 | 18 | 21 | 11 | 5 | 18 | 4 | 1 | 20 | 1 | | | | | | | |
| | | | | | | | | | | | | | | | | | | |

**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: Hva er Proton VPN Secure Core?

Secure Core ruter trafikken gjennom flere servere i personvernvennlige land før utgangen.

### Q2: Hva er Stealth-protokollen?

Stealth er en obfuskert protokoll som skjuler VPN-tilkoblinger som vanlig TLS/HTTPS-trafikk.

### Q3: Hvordan beskytter NetShield brukerne?

NetShield er et DNS-basert verktøy som automatisk blokkerer annonser, sporere og skadevaredomener.

### Q4: Er Proton VPN juridisk beskyttet i Sveits?

Ja, Sveits har strenge personvernlover og ligger utenfor jurisdiksjonen til USA og EU/14-Eyes. [4]

### Q5: Er Proton VPN-appene åpen kildekode?

Ja. Proton VPNs apper er åpen kildekode og har gjennomgått publiserte sikkerhetsrevisjoner.

# 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: Hvilke krypteringschiffer brukes?

Proton VPN bruker AES-256-GCM eller ChaCha20-Poly1305 med HMAC-SHA384 og RSA-4096-håndtrykk.

### Q7: Har Proton VPN en Kill Switch?

Ja, Proton VPN har en standard og en permanent kill switch for å hindre ukrypterte lekkasjer.

### Q8: Kan Proton VPN lekke DNS-spørringer?

Nei, alle DNS-forespørsler rutes gjennom krypterte private DNS-servere som eies av Proton.

### Q9: Fører Proton VPN tilkoblingslogger?

Nei, Proton VPN har en streng policy om ingen logging, bekreftet av årlige revisjoner fra Securitum. [3]

### Q10: Er Proton VPN sårbar for WebRTC-lekkasjer?

Nei, Proton-klientene har innebygde brannmurregler og rutingpolicyer som blokkerer WebRTC-lekkasjer.

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

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

### Q1: Hvor er datasentrene for Secure Core fysisk plassert?

De ligger i Sveits, på en tidligere militærbase på Island og på et underjordisk sted i Sverige. [1]

### Q2: Hvordan fungerer Perfect Forward Secrecy i Proton VPN?

En unik, kortvarig krypteringsnøkkel genereres for hver økt, slik at dekryptering i ettertid forhindres.

### Q3: Hva er Permanent Kill Switch på Windows/Linux?

Permanent Kill Switch blokkerer all nettverkstrafikk selv om VPN-appen er helt lukket eller krasjer.

### Q4: Støtter Proton VPN IPv6-ruting og lekkasjebeskyttelse?

Proton VPN ruter IPv6-trafikk fullstendig gjennom tunnelene eller deaktiverer den på en trygg måte for å hindre lekkasjer.

### Q5: Hvordan håndterer NetShields DNS-filtrering HTTPS-inspeksjon?

NetShield opererer utelukkende på DNS-oppløsningslaget uten å kreve inngripende TLS-dekryptering.

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

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

### Q6: Hvem utførte Proton VPNs kodegjennomganger fra tredjepart?

SEC Consult reviderte appene, og Securitum reviderer appene og policyen om ingen logging.

### Q7: Hvordan er Stealth-protokollen sammenlignet med OpenVPN XOR eller Shadowsocks?

Stealth tunnelerer WireGuard over obfuskert TLS og yter bedre enn eldre OpenVPN-baserte obfuskeringsmetoder. [5]

### Q8: Kan sveitsiske myndigheter tvinge Proton VPN til å logge trafikk?

Proton opplyser at de etter sveitsisk lov ikke er forpliktet til å lagre logger over brukeraktivitet eller data.

### Q9: Hvordan er Proton VPN-servere beskyttet mot beslagleggelse?

Alle Proton VPN-servere er bare metal-maskiner beskyttet med full diskkryptering. [2]

### Q10: Støtter Proton VPN konfigurasjon av egne DNS-servere?

Ja, betalende abonnenter kan konfigurere egendefinerte oppstrøms DNS-servere direkte i appinnstillingene.

# 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**

1. Proton eier og installerer selv Secure Core-serverne sine, på høysikkerhetssteder i Sveits, Island og Sverige. [1]

**2. VPN-INNSIKT**

2. Proton VPNs klientapper har åpen kildekode og gjennomgår gjentakende kodeaudits fra tredjepart.

**3. VPN-INNSIKT**

3. Stealth-tilslørings-protokollen omgår dyp pakkeinspeksjon ved å simulere vanlig TLS-trafikk.

**4. VPN-INNSIKT**

4. Sveits står utenfor de internasjonale etterretningsallianser 5 Eyes, 9 Eyes og 14 Eyes. [4]

**5. VPN-INNSIKT**

5. NetShield opererer på DNS-resolvernivå og hindrer annonser og skadevare før nyttelasten lastes ned.

**6. VPN-INNSIKT**

6. Perfect Forward Secrecy sikrer at kompromitterte nøkler ikke kan dekryptere tidligere fangede trafikkøkter. [7]

**7. VPN-INNSIKT**

7. Proton VPN bruker full diskkryptering på bare metal-servere for å beskytte serverkonfigurasjoner. [2]

**8. VPN-INNSIKT**

8. Den permanente kill switch-funksjonen hindrer lekkasjer av ukryptert data selv ved omstart av operativsystemet.

**9. VPN-INNSIKT**

9. Securitum har revidert og bekreftet Proton VPNs retningslinje om ingen logging i fem påfølgende årlige revisjoner. [3]

**10. VPN-INNSIKT**

10. Proton VPN ble utviklet av forskere som møttes ved CERN (Den europeiske organisasjonen for kjernefysisk forskning). [4]

# Tekniske referanser og kilder

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

## FAGLIGE REFERANSER OG BRANSJEREFERANSER


[1] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

## Fasit: Kontrollpunkt 1 – flervalg

**1** **Spørsmål 1** **Riktig svar: B**

### MERKNAD TIL LÆREREN

Secure Core-serverne står i høysikkerhetsanlegg, blant annet en tidligere militærbase på Island og et underjordisk datasenter i Sverige.

**2** **Stealth-obfuskeringsprotokoll** FORSVAR MOT SENSUR **Riktig svar: B**

### MERKNAD TIL LÆREREN

Protons Stealth-protokoll skjuler WireGuard-tilkoblinger som vanlig TLS/HTTPS-trafikk for å omgå brannmurer med dyp pakkeinspeksjon (DPI).

**3** **NetShield DNS-annonseblokkerer** DNS-FILTRERING **Riktig svar: B**

### MERKNAD TIL LÆREREN

NetShield bruker filtrering på DNS-nivå til å blokkere skadevaredomener, spionprogrammer, påtrengende annonser og telemetrisporere før nettsider lastes.

**4** **Sveitsisk juridisk jurisdiksjon** JURISDIKSJON **Riktig svar: C**

### MERKNAD TIL LÆREREN

Proton AG har hovedkontor i Genève i Sveits og drar nytte av sterke sveitsiske personvernlover utenfor de amerikanske og europeiske 14 Eyes-overvåkingsalliansene.

**5** **Spørsmål 5** **Riktig svar: B**

### MERKNAD TIL LÆREREN

Alle Proton VPN-apper har åpen kildekode; SEC Consult og senere Securitum har revidert dem.

## Fasit: Kontrollpunkt 2 – sant eller usant

**6** **Secure Core med flere jurisdiksjoner** RUTINGARKITEKTUR **Riktig svar: Sant**

### MERKNAD TIL LÆREREN

Secure Core ruter trafikken gjennom jurisdiksjoner med sterkt personvern før den går ut til bestemmelseslandet, noe som kan bidra til å beskytte mot en kompromittert utgangsserver.

**7** **Sveitsisk overvåkingsallianse** OVERVÅKINGSALLIANSER **Riktig svar: Usant**

### MERKNAD TIL LÆREREN

Sveits er ikke medlem av avtalene om deling av etterretning i 5 Eyes, 9 Eyes eller 14 Eyes, og bevarer dermed sin uavhengige juridiske suverenitet.

**8** **Spørsmål 8** **Riktig svar: Sant**

### MERKNAD TIL LÆREREN

NetShield bruker Protons DNS-servere til å sjekke domener mot lister over kjente annonse-, sporings- og skadevaredomener.

**9** **Revisjon av klienter med åpen kildekode** SIKKERHETSÅPENHET **Riktig svar: Sant**

### MERKNAD TIL LÆREREN

Proton har gjort skrivebords- og mobilappene sine åpne og publiserer revisjonsrapporter fra tredjeparter.

**10** **Spørsmål 10** **Riktig svar: Usant**

### MERKNAD TIL LÆREREN

Usant: Stealth tunnelerer WireGuard inne i obfuskert TLS over TCP slik at trafikken ser ut som vanlig HTTPS.

# 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. SECURE CORE | D 2. STEALTH | F 3. NETSHIELD | C 4. SVEITSISK LOV |
| H 5. KILL SWITCH | A 6. ÅPEN KILDEKODE | E 7. WIREGUARD | B 8. AES-GCM |

## KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

| | | | |
|---|---|---|---|
| 1 SECURE CORE | 2 STEALTH | 3 NETSHIELD | 4 SVEITSISK LOV |
| 5 KILL SWITCH | 6 ÅPEN KILDEKODE | | |

## KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

| | | | |
|---|---|---|---|
| 1 B – STEALTH | 2 G – WIREGUARD | 3 D – SVEITSISKLOV | 4 A – SECURECORE |
| 5 H – AESGCM | 6 E – KILLSWITCH | 7 C – NETSHIELD | 8 F – ÅPENKILDEKODE |

## DISKUSJONSNOTATER TIL LÆRERE

**Nøkkelbegreper:**
Kontroller at elevene kan forklare SECURE CORE, STEALTH og NETSHIELD med egne ord og gi et eksempel på hvert.

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

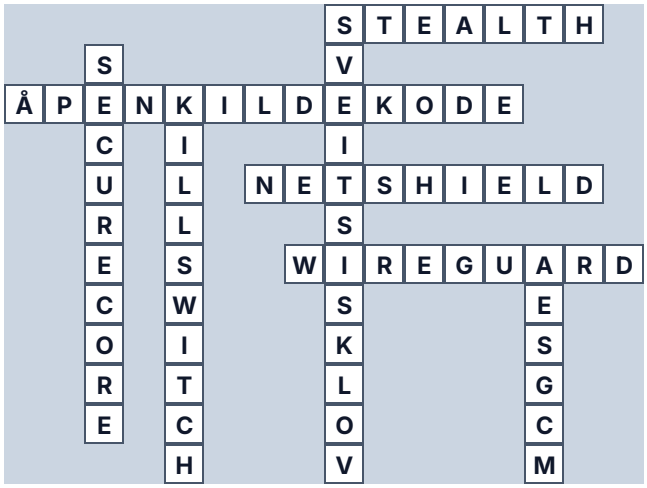
**Kildevurdering:**
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

# Fasit for oppgavene og merknader til læreren

## LØSNING PÅ ORDSØKET

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

## KRYSSORDLØSNING




## LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

### VANNRETT

**1 vannrett: STEALTH** En tilsløret tunnelprotokoll forkledd som vanlig HTTPS-nettrafikk (7 bokstaver)

**3 vannrett: ÅPENKILDEKODE** Offentlig tilgjengelig og uavhengig revidert klientprogramvare (13 bokstaver)

**5 vannrett: NETSHIELD** Et DNS-basert filter som blokkerer annonser, telemetrisporere og skadevare (9 bokstaver)

**6 vannrett: WIREGUARD** En moderne lett protokoll som gir robust kryptografi og høy hastighet (9 bokstaver)

### LODDRETT

**1 loddrett: SVEITSISKLOV** Strenge juridiske personvernlover i Sveits, utenfor 14 Eyes-jurisdiksjonen (12 bokstaver)

**2 loddrett: SECURECORE** En multi-hop-utforming som ruter trafikk gjennom Proton-eide servere som første hopp (10 bokstaver)

**4 loddrett: KILLSWITCH** En sikkerhetsmekanisme som stanser nettverksoverføring ved tilkoblingsfall (10 bokstaver)

**7 loddrett: AESGCM** Symmetrisk chiffer av militær klasse som sikrer alle innkapslede VPN-datapakker (6 bokstaver)

# Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

### FASIT: BOKSTAVBLANDING

| | | | | | |
|---|---|---|---|---|---|
| 1. | RCERESOEUC | SECURECORE | 5. | LHAESTT | STEALTH |
| 2. | DNLSEIEHT | NETSHIELD | 6. | VTKLSOSSVIEI | SVEITSISKLOV |
| 3. | KWCIISHLTL | KILLSWITCH | 7. | KODIÅPEKEDELN | ÅPENKILDEKODE |
| 4. | GDREAUWIR | WIREGUARD | 8. | SMACGE | AESGCM |

### FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

**"SECURE CORE HERDEDE SERVERE BESKYTTER BRUKERDATA"**

# Fasit til casestudiene

## A CASESTUDIE 1: OMGÅ RESTRIKTIVE BRANNMURER

Løsning for læreren

### RETTEMAL OG VEILEDNING FOR LØSNINGER

- Scenarioanalyse: En bruker reiser til et land der vanlig VPN-trafikk som OpenVPN og WireGuard blokkeres av DPI.
- Fokusspørsmål: Hvilken protokollkonfigurasjon i Proton VPN lar brukeren omgå inspeksjon på statlig nivå?
- Anbefalt strategi og løsning: Brukeren bør aktivere Stealth-protokollen, som tilslører VPN-pakkenes headere som vanlig TLS/HTTPS-nettrafikk og slipper forbi DPI-filtre.

## B CASESTUDIE 2: AVANSERT BESKYTTELSE MOT MOTSTANDERE

Løsning for læreren

### RETTEMAL OG VEILEDNING FOR LØSNINGER

- Scenarioanalyse: En finansrevisor mistenker at utgangsnoden til den lokale internettleverandøren kan være kompromittert av avanserte vedvarende trusler (APT).
- Fokusspørsmål: Hvordan beskytter Secure Core revisorens identitet mot en kompromittert utgangsnode?
- Anbefalt strategi og løsning: Secure Core sender trafikken først gjennom Proton-eide servere i Sveits, Island eller Sverige, slik at en kompromittert utgangsserver ikke kan spore brukerens IP-adresse.