Navn: _____ Dato: _____ Point: _____

Sådan skjuler du din IP-adresse Opgaveark

Skjul IP-adresser, maskering af placering, proxy, Tor og forebyggelse af DNS-/WebRTC-lækager

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

- Forklar hvordan IP-adresser fungerer, og hvordan de afslører placeringer.
- Sammenlign proxyer, Tor og VPN'er til maskering af netværksadresser.
- Identificér metoder til at opdage og forhindre DNS- og WebRTC-lækager.
- Forstå hvordan websteder sporer brugere via deres offentlige IP.
- Vurdér multi-hop-routing og krypterede tunneler som IP-beskyttelse.

VEJLEDNING TIL OPGAVEARKET OM IP-BESKYTTELSE

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 at skjule din IP-adresse og forhindre lækager. Slut af med bonusaktiviteten Tænk hurtigt.

SÅDAN SKJULER DU DIN IP (INTRODUKTION)

Din IP-adresse er en digital postadresse, der afslører din fysiske placering og dine netværksvaner. At skjule din IP-adresse er første forsvarslinje mod sporing på nettet, målrettet profilering og geografiske blokeringer. Når du forstår, hvordan du sikkert skjuler din adresse, hjælper det med at beskytte dit privatliv på nettet.

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

Kontrolpunkt 1: Flervalgsopgave

1 **1. Hvad afslører en enheds offentlige IP-adresse for de websteder, du besøger?**

- A. Brugerens kreditkortnummer
- B. Din omtrentlige placering og navnet på din internetudbyder
- C. Hele den lokale filmappe
- D. Tastaturets sprogindstillinger

2 **2. Hvilken metode skjuler din IP og krypterer al trafik på hele systemet?**

- A. En almindelig webproxy
- B. At rydde browserens cookies
- C. Et virtuelt privat netværk (VPN)
- D. At slå den indbyggede firewall fra

3 **3. Hvad er en væsentlig privatlivsbegrænsning ved en gratis webproxy?**

- A. Den krypterer ikke datatrafik på offentlige netværk
- B. Den kræver installation af et eksternt styresystem
- C. Den er helt ulovlig i USA
- D. Den kræver en dedikeret telefonlinje

4 **4. Hvordan giver Tor-netværket brugerne høj anonymitet?**

- A. Ved at gøre forbindelseshastigheden hurtigere
- B. Ved at route trafikken gennem tre relæer drevet af frivillige
- C. Ved at registrere dit navn i en global database
- D. Ved kun at give offentlige myndigheder adgang

5 **5. Hvad er en DNS-lækage?**

- A. En fejl, hvor en e-mail sendes til den forkerte adresse
- B. Når DNS-forespørgsler går uden om VPN-tunnelen til internetudbyderen
- C. En hardwarefejl i routerens strømforsyning
- D. En opdatering af netværkskortets driver

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. En proxyserver krypterer baggrundstrafik i styresystemet ligesom en VPN.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. Tor-routing er meget sikker, men sænker surfehastigheden.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. WebRTC-lækager kan afsløre din rigtige IP under en aktiv VPN-session.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. Med en VPN slået til og uden lækager kan din internetudbyder ikke se, hvilke websteder du besøger.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. At skjule din IP-adresse blokerer sporing via browser-fingerprinting.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. Når domæneforespørgsler går uden om den sikre tunnel, kaldes det en _____ .
2. Browserbaserede _____ kommunikations-API'er kan utilsigtet lække din egen IP-adresse.
3. En web- _____ omdirigerer browsertrafik, men krypterer ikke pakkernes indhold.
4. Den flerlagede kryptering i _____ netværket giver en høj grad af anonymitet.
5. Din offentlige _____ tildeles af din teleudbyder og afslører dit område.
6. Regionale medieblokeringer omgås ved hjælp af _____ maskering.

ORDBANK MED FAGUDTRYK

DNS-LÆKAGE IP-ADRESSE PLACERING PROXY ROUTING SPORING TOR WEBRTC

Skriv dine svar her:

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

Kontrolpunkt 4: Match netværksbegreber

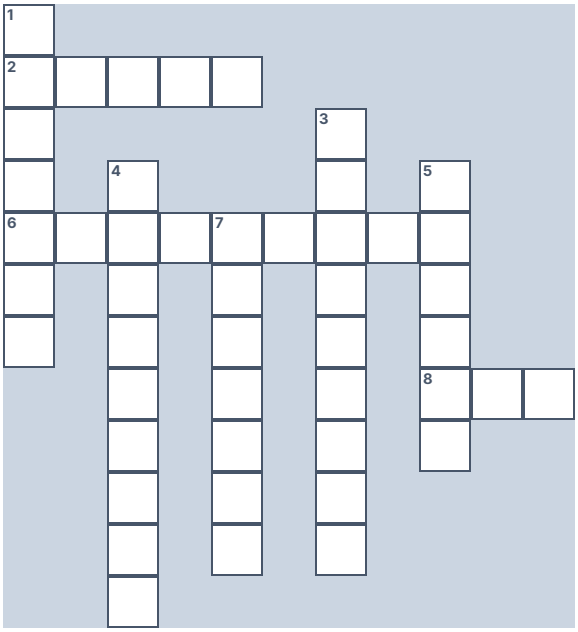
MATCH BEGREBER OG DEFINITIONER

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

☐	1. IP-adresse	A	Krypterer al en enheds trafik og router den gennem en VPN-server.
☐	2. VPN-tunnel	B	Sender data gennem tre frivillige servere og krypterer et lag ved hvert trin.
☐	3. Tor-netværket	C	Routing af forbindelsen via en server i et andet land for at omgå geoblokering.
☐	4. Webproxy	D	Unikt talmærke, der identificerer en enheds grænseflade på internettet.
☐	5. DNS-lækage	E	Omdirigerer browsertrafik på applikationslaget uden kryptering på systemniveau.
☐	6. WebRTC-API	F	Teleudbyderens logning af destinationer for ukrypteret internettrafik.
☐	7. Maskering af placering	G	Forespørgsler, der besvares uden for VPN-tunnelen og afslører besøgte domæner for udbyderen.
☐	8. Sporing hos udbyderen	H	Browserfunktion til tale og video, der kan omgå tunneler og afsløre rigtige IP-adresser.

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

2. Omdirigerer browsertrafik på applikationslaget uden kryptering på systemniveau (5)

6. Unik numerisk betegnelse, der identificerer en enheds netværksinterface på internettet (9)

8. Sender data gennem tre frivillige servere og krypterer lag for lag (3)

LODRETTE NØGLER

1. Teleselskabets registrering af, hvilke destinationer din ukrypterede trafik går til (7)

3. Forespørgsler, der besvares uden for VPN-tunnelen og afslører besøgte domæner for internetudbyderen (9)

4. At sende forbindelsen via en server i et andet land for at omgå geoblokeringer (9)

5. Browserfunktion til tale og video, der kan gå uden om tunneler og afsløre din rigtige IP-adresse (6)

7. Den vej, datapakkerne tager; en VPN sender al enhedens trafik krypteret via en VPN-server (7)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

2 vandret: Omdirigerer browsertrafik på applikationslaget uden kryptering på systemniveau (5 bogstaver):

6 vandret: Unik numerisk betegnelse, der identificerer en enheds netværksinterface på internettet (9 bogstaver):

8 vandret: Sender data gennem tre frivillige servere og krypterer lag for lag (3 bogstaver):

LODRETTE NØGLER

1 lodret: Teleselskabets registrering af, hvilke destinationer din ukrypterede trafik går til (7 bogstaver):

3 lodret: Forespørgsler, der besvares uden for VPN-tunnelen og afslører besøgte domæner for internetudbyderen (9 bogstaver):

4 lodret: At sende forbindelsen via en server i et andet land for at omgå geoblokeringer (9 bogstaver):

5 lodret: Browserfunktion til tale og video, der kan gå uden om tunneler og afsløre din rigtige IP-adresse (6 bogstaver):

7 lodret: Den vej, datapakkerne tager; en VPN sender al enhedens trafik krypteret via en VPN-server (7 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

D T J G P T N S R Æ S Q C W U

V F Y M K B A P B C W Q Æ M L

Æ M X Æ W L E O S O E K E J O

E O O L S R H R O O B S T U W

G V R H C I U I S Q R I U M C

A Y P E V P Ø N X C T Å Y A G

K L I Å D A O G R E C S Z S R

Æ C W B A D Å P O E M A E K Q

L E F H J R D T U S N F J E U

S Å U G S E T Y T F A A S R Q

N O R W Æ S O S I L T W U I D

D O Ø B G S R U N Z Z K A N T

Å Ø Ø M H E J O G T L N N G V

Q I S S H Å A Q X G X C Ø T Ø

B I N Å H K P R P Z C N Å Ø G

ORDLISTE MED FAGUDTRYK

IPADRESSE DNSLÆKAGE WEBRTC PROXY TOR ROUTING SPORING MASKERING

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. IPADRESSE
B. DNSLÆKAGE
C. WEBRTC
D. PROXY
E. TOR
F. ROUTING
G. SPORING
H. MASKERING

DEFINITIONER OG MATCHFELTER
[ ] 1. Omdirigerer browsertrafik på applikationslaget uden kryptering på systemniveau.
[ ] 2. Teleselskabets registrering af, hvilke destinationer din ukrypterede trafik går til.
[ ] 3. Den vej, datapakkerne tager; en VPN sender al enhedens trafik krypteret via en VPN-server.
[ ] 4. Unik numerisk betegnelse, der identificerer en enheds netværksinterface på internettet.
[ ] 5. Browserfunktion til tale og video, der kan gå uden om tunneler og afsløre din rigtige IP-adresse.
[ ] 6. At sende forbindelsen via en server i et andet land for at omgå geoblokeringer.
[ ] 7. Sender data gennem tre frivillige servere og krypterer lag for lag.
[ ] 8. Forespørgsler, der besvares uden for VPN-tunnelen og afslører besøgte domæner for internetudbyderen.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. **ERDPISSEA**
2. **CWBTRE**
3. **ROT**
4. **GPIRNSO**
5. **AÆNEKLDGS**
6. **XPOYR**
7. **RNIGOTU**
8. **GENMKARIS**

Bonusaktivitet: Tænk hurtigt

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

1	Grunde til at bruge en VPN på rejsen			
2	Browsere, du kender			
3	Ting, en VPN kan skjule			
4	Ord, der har med privatliv at gøre			
5	Ord fra dette opgaveark, du vil huske			
6	Ting, en hjemmeside kan gætte ud fra din IP			
7	Tal eller tegn i en IP-adresse			
8	Myter om VPN			
9	VPN-tjenester, du kender			
10	Ting, din internetudbyder kan se			
11	Ting, en god VPN-udbyder lover			
12	Ting, der kan lække din rigtige IP			
13	Grunde til at skjule din placering			
14	Måder at skjule din IP-adresse			
15	Enheder, der kan bruge en VPN			

Kontrolpunkt 8: VPN-casestudier

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

SARAH (STUDERENDE PÅ CAFÉ)

👩‍💻 "Hej! Jeg sidder på Coffee & Bytes. Der er et usikret offentligt netværk, der hedder 'Free_Wi-Fi_No_Password'. Jeg vil logge ind på min skolemail og uploade min opgave, men jeg er bekymret for hackere. Hvilke risici er der ved at bruge dette netværk uden en VPN, og hvordan sikrer en VPN mine data?"

ALEX (STUDERENDE PÅ REJSE)

👩‍💻 "Åh nej! Jeg er på rejse i udlandet for et projekt og prøver at se en biologidokumentar, der ligger på en server i mit hjemland. Men siden skriver 'Denne video er ikke tilgængelig på din nuværende placering.' Hvorfor bliver jeg blokeret, og hvordan kan en VPN hjælpe mig med at se den?"

Kontrolpunkt 9: Afkod chifferet

Afslut din træning i IP-maskering ved at afkode denne hemmelige besked om at skjule dine digitale spor.

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

19	11	10	21	12		4	9	14		1	4	18	5	19	19	5		13	5	4
					5	20		19	11	10	21	12	20		19	25	19	20	5	13

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 bør jeg bruge en VPN?

En VPN beskytter dit digitale privatliv, sikrer din forbindelse på offentlige Wi-Fi-netværk (f.eks. caféer eller lufthavne), kan mindske aktivitetsbaseret hastighedsbegrænsning, når udbyderen ikke kan identificere den krypterede trafiktype, omgår geografiske begrænsninger og hjælper med at sikre ressourcer til fjernarbejde.

Q3: Gør en VPN mig helt anonym online?

Nej. Selvom en VPN skjuler din IP-adresse og krypterer trafikken, kan du stadig spores via browsercookies, aktive konti (f.eks. Google eller Facebook), browser-fingerprinting, eller hvis din VPN-udbyder logger dine data.

Q4: Skjuler en webproxy min IP-adresse?

Ja, men kun for den trafik, der sendes gennem den, som regel din browser. De fleste webproxyer krypterer ikke dine data, så din internetudbyder eller netværksoperatøren kan stadig se, hvad du sender og modtager.

Q5: Er det lovligt at skjule min IP?

I mange lande, ja, men nogle begrænser eller forbyder VPN'er og andre værktøjer, der bruges til at skjule en IP-adresse. At skjule din IP gør aldrig en ulovlig handling lovlig, så tjek de lokale love, før du bruger et.

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del B)

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

Q6: Skjuler Tor min IP?

Ja. Tor sender din trafik gennem tre frivillige relæer (guard, middle og exit), så websteder ser exit-relæets adresse, og intet enkelt relæ kender både hvem du er, og hvor du går hen. [1]

Q7: Hvad afslører min IP?

Din offentlige IP afslører som regel din internetudbyder og en omtrentlig placering, fx dit land eller din by. Websteder kan også bruge den til at koble dine besøg sammen og til at anvende geoblokeringer.

Q8: Hvordan tjekker jeg, at den er skjult?

Forbind til din VPN, besøg derefter et websted, der viser din IP, og kør lækagetest for DNS og WebRTC. De viste IP- og DNS-servere bør tilhøre VPN'en, ikke din internetudbyder. Hvis din rigtige IP vises, så slå lækagebeskyttelse til.

Q9: Kan jeg bruge en VPN på min telefon og mit smart-tv?

Ja. Moderne VPN-udbydere tilbyder dedikerede apps til iOS, Android, macOS, Windows, Linux og smart-tv samt routeropsætninger, der beskytter alle enheder på dit hjemmenetværk.

Q10: Hvad er en kill switch?

En kill switch er en sikkerhedsfunktion, der automatisk afbryder din enhed fra internettet, hvis VPN-forbindelsen falder ud. Det forhindrer, at ukrypterede data eller din rigtige IP-adresse lækkes.

Kontrolpunkt 10: Avanceret VPN-FAQ (del C)

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

Q1: Hvorfor kan websteder stadig spore mig, når jeg har skjult min IP-adresse?

At skjule din IP stopper ikke browser-fingerprinting. Trackere kan kombinere detaljer som din skærmopløsning, installerede skrifttyper og browserindstillinger til et id, og cookies eller konti, du er logget ind på, kan også identificere dig, så brug også en privatlivsfokuseret browser. [3]

Q2: Hvad er dobbelt VPN eller Multi-Hop-routing?

Multi-Hop sender din trafik gennem to eller flere VPN-servere efter hinanden. Det tilføjer et ekstra lag kryptering og hjælper med at holde din rigtige IP-adresse skjult for det andet hop, hvis én server kompromitteres.

Q3: Hvad er WebRTC-lækage, og hvordan forhindrer en VPN det?

WebRTC er en browserprotokol, der kan afsløre dine rigtige lokale og offentlige IP-adresser, selv når en VPN er aktiv. Premium-VPN'er blokerer eller forfalsker WebRTC-forespørgsler i deres desktop- og mobilapps samt browserudvidelser.

Q4: Kan IPv6-trafik lække min rigtige IP-adresse?

Ja, hvis din VPN kun tunnelerer IPv4. Din enhed kan så sende IPv6-trafik uden om tunnelen og afsløre en adresse, som din internetudbyder har tildelt. Brug en VPN, der tunnelerer eller blokerer IPv6, og bekræft det med en IPv6-lækagetest.

Q5: Hvordan omgår obfuskering VPN-blokeringer?

Obfuskering (eller "Stealth VPN") forklæder VPN-trafikpakker, så de ligner almindelig HTTPS-webtrafik (port 443). Det hjælper 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: Afslører split tunneling min rigtige IP-adresse?

Ja, for de apps, du udelukker. Trafik, der sendes uden om tunnelen, bruger din rigtige IP, og RFC 8828 bemærker, at WebRTC kan afsløre internetudbyderens adresse under en VPN med split tunneling, medmindre browseren begrænser det. [2]

Q7: Hvad er en delt IP-adresse, og hvordan hjælper den privatlivet?

Med en delt IP optræder mange VPN-brugere online med den samme adresse på samme tid. Det gør det meget sværere for et websted at knytte et enkelt besøg til dig end med en dedikeret IP, som kun du bruger.

Q8: Kan min internetudbyder se, at jeg bruger en VPN til at skjule min IP?

Som regel, ja. Din internetudbyder kan se, at du forbinder til en VPN-servers IP-adresse, hvornår du forbinder, og hvor meget data du sender, men ikke de websteder, du besøger, eller indholdet i den krypterede tunnel.

Q9: Hvad er DNS-lækagebeskyttelse?

DNS-lækagebeskyttelse tvinger din enhed til at sende opslagsforespørgsler (DNS-forespørgsler) gennem VPN'ens private, krypterede DNS-servere i stedet for udbyderens servere. Det forhindrer din internetudbyder i at spore, hvilke sider du besøger.

Q10: Er en proxy eller en VPN bedst til at skjule min IP?

En VPN er som regel bedre. Den skjuler din IP for alle apps på enheden og krypterer trafikken, mens en webproxy typisk kun dækker browseren og ofte ikke tilføjer kryptering.

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), en tidlig VPN-protokol fra en Microsoft-ledet gruppe i 1990'erne, anses i dag for usikker, så moderne VPN'er bruger WireGuard eller OpenVPN.

2. FINGERPRINTING

At skjule din IP stopper ikke browser-fingerprinting, som kan identificere dig ud fra detaljer som skærmopløsning og installerede skrifttyper. [3]

3. WIREGUARD-REVOLUTIONEN

WireGuard har en meget strømlinet kodebase designet til effektivitet, hvilket gør den lettere at gennemgå for sikkerhedssårbarheder end traditionelle protokoller.

4. ADRESSEEKSPONERING VIA WEBRTC

RFC 8828 advarer om, at WebRTC kan finde både en VPN's offentlige adresse og den adresse fra internetudbyderen, som VPN'en kører over, medmindre browseren begrænser det. [2]

5. 5-EYES-ALLIANCENS OPRINDELSE

Five Eyes-efterretningssamarbejdet mellem USA, Storbritannien, Canada, Australien og New Zealand udsprang af de allieredes samarbejde om signalefterretning under Anden Verdenskrig.

6. DEEP PACKET INSPECTION

Avancerede firewalls bruger Deep Packet Inspection (DPI) til at analysere metadata i netværkspakker og blokere typiske kendetegn ved VPN-forbindelser.

7. GENBRUG AF TOR-KREDSLØB

Tor genbruger det samme kredsløb i cirka ti minutter og bygger derefter et nyt, hvilket gør det sværere at koble din browseraktivitet sammen. [1]

8. DECENTRALISEREDE VPN'ER

Decentraliserede VPN'er (dVPN'er) fordeler trafikken over et netværk af noder drevet af brugerne selv, hvilket mindsker afhængigheden af én central udbyder.

9. TOR KONTRA VPN-ANONYMITET

En VPN tunnelerer trafik gennem én udbyder, mens Tor (The Onion Router) sender trafik gennem tre frivillige relæer (guard, middle, exit) for at maksimere privatlivet. [1]

10. PROXYER VS. VPN-TUNNELER

En webproxy ændrer den IP-adresse, et websted ser for din browsertrafik, men i modsætning til en VPN krypterer den som regel ikke trafikken eller dækker andre apps på din enhed. [5]

Tekniske referencer og kilder

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

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[1] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

Facitliste: Skjul af IP-adresser, maskering af placering, proxy, Tor og forebyggelse af DNS/WebRTC-lækager

1 **Spørgsmål 1** — Rigtigt svar: B

UNDERVISNINGSNOTE

Hvad afslører en enheds offentlige IP-adresse for de websteder, du besøger? → Din omtrentlige placering og navnet på din internetudbyder

2 **Systemdækkende VPN-kryptering** LATENS — Rigtigt svar: C

UNDERVISNINGSNOTE

I modsætning til proxyer, der kun omdirigerer browsertrafik, opretter en VPN en krypteret tunnel for hele systemet og sikrer baggrundsprogrammer, spil og systemforespørgsler.

3 **Manglende kryptering i proxyer** WI-FI-SIKKERHED — Rigtigt svar: A

UNDERVISNINGSNOTE

Webproxyer videresender kun browsertrafik uden at kryptere pakkernes indhold, så netværksoperatøren eller udbyderen stadig kan spore din trafik.

4 **Spørgsmål 4** — Rigtigt svar: B

UNDERVISNINGSNOTE

Hvordan giver Tor-netværket brugerne høj anonymitet? → Ved at route trafikken gennem tre relæer drevet af frivillige

5 **DNS-lækager uden om tunnelen** PRIVATLIV — Rigtigt svar: B

UNDERVISNINGSNOTE

En DNS-lækage opstår, når domæneopslag går uden om VPN-tunnelen direkte til udbyderens resolvere og dermed afslører, hvilke domæner du besøger.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Proxyernes begrænsninger** IP-MASKERING — **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Proxyer fungerer på applikationslaget og mangler VPN-tunnelens integration med netværksdriveren på systemniveau.

7 **Spørgsmål 7** — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

At sende trafik gennem tre frivillige relæer med lagdelt kryptering giver ekstra forsinkelse, så Tor er som regel langsommere end en direkte forbindelse.

8 **Spørgsmål 8** — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

WebRTC kan afsløre lokale adresser og, med nogle VPN-opsætninger, den offentlige IP fra internetudbyderen under tunnelen (RFC 8828).

9 **Spørgsmål 9** — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Uden DNS- eller WebRTC-lækager ser internetudbyderen kun krypteret trafik til VPN-serveren, ikke de websteder, du besøger.

10 **Fingerprintingens grænser** INGEN LOGS — **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Fingerprinting bruger enhedens konfiguration (skærmopløsning, skrifttyper, plugins), som forbliver synlig, selv når IP'en er skjult.

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

D 1. IP-adresse	A 2. VPN-tunnel	B 3. Tor-netværket	E 4. Webproxy
G 5. DNS-lækage	H 6. WebRTC-API	C 7. Maskering af placering	F 8. Sporing hos udbyderen

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 DNS-LÆKAGE	2 WEBRTC	3 PROXY	4 TOR
5 IP-ADRESSE	6 PLACERING		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 D – PROXY	2 G – SPORING	3 F – ROUTING	4 A – IPADRESSE
5 C – WEBRTC	6 H – MASKERING	7 E – TOR	8 B – DNSLÆKAGE

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare IP-adresse, VPN-tunnel og Tor-netværket med egne ord og give et eksempel på hvert begreb.

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

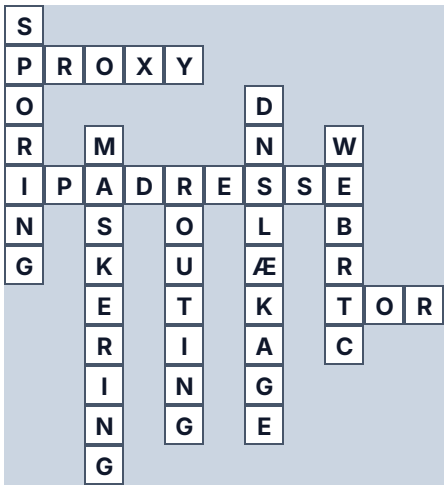
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: PROXY Omdirigerer browsertrafik på applikationslaget uden kryptering på systemniveau (5 bogstaver)

6 vandret: IPADRESSE Unik numerisk betegnelse, der identificerer en enheds netværksinterface på internettet (9 bogstaver)

8 vandret: TOR Sender data gennem tre frivillige servere og krypterer lag for lag (3 bogstaver)

LODRETTE NØGLER

1 lodret: SPORING Teleselskabets registrering af, hvilke destinationer din ukrypterede trafik går til (7 bogstaver)

3 lodret: DNSLÆKAGE Forespørgsler, der besvares uden for VPN-tunnelen og afslører besøgte domæner for internetudbyderen (9 bogstaver)

4 lodret: MASKERING At sende forbindelsen via en server i et andet land for at omgå geoblokeringer (9 bogstaver)

5 lodret: WEBRTC Browserfunktion til tale og video, der kan gå uden om tunneler og afsløre din rigtige IP-adresse (6 bogstaver)

7 lodret: ROUTING Den vej, datapakkerne tager; en VPN sender al enhedens trafik krypteret via en VPN-server (7 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1.	E R D P I S S E A	IPADRESSE	5.	A Æ N E K L D G S	DNSLÆKAGE
2.	C W B T R E	WEBRTC	6.	X P O Y R	PROXY
3.	R O T	TOR	7.	R N I G O T U	ROUTING
4.	G P I R N S O	SPORING	8.	G E N M K A R I S	MASKERING

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"SKJUL DIN ADRESSE MED ET SKJULT SYSTEM"

Facit til casestudier

A Scenarie A: Sikkerhed på offentlige netværk

AFLYTNING OG KRYPTERING | Sarahs dilemma

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Risici: Pakkeaflytning, opsnapning af data og man-in-the-middle-angreb. En anden på cafeens netværk kan opfange hendes loginoplysninger eller opgavefil.
- VPN-beskyttelse: Krypterer indholdet af netværkspakkerne, så opsnappet tunneltrafik er ulæselig for passive aflyttere på det lokale netværk, når VPN'en er korrekt konfigureret.

B Scenarie B: Adgang til blokerede ressourcer

GEOBLOKERING OG IP-ADRESSER | Alex' dilemma

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Hvorfor blokeret: Streamingtjenesten bruger geoblokering, som kobler hans lokale IP-adresse til det land, han befinder sig i, og blokerer ud fra territoriale licenser.
- Sådan hjælper en VPN: Den skjuler hans reelle placering ved at lede trafikken gennem en server i hans hjemland. Siden ser en IP fra hjemlandet og giver adgang.