Navn: _____ Dato: _____ Poeng: _____

Proxy mot VPN Arbeidsark

Sammenligning av proxyservere og virtuelle private nettverk, forskjeller i kryptering og ruting per applikasjon eller for hele systemet

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 applikasjonsproxyer med VPN-kryptering for hele systemet.
- Identifiser SOCKS5-funksjoner sammenlignet med enkle HTTP-proxyer.
- Analyser hvordan nettleserbaserte proxyer lar bakgrunnsapper være eksponert.
- Forstå hvordan internettleverandører logger ukryptert trafikk på proxytunneler.
- Velg riktig rutingverktøy ut fra behovet for hastighet og sikkerhet.

INSTRUKSJONER FOR ARBEIDSARKET OM PROXY-SAMMENLIGNING

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

PROXY MOT VPN (INNLEDNING)

Proxyer og VPN-er har ulike funksjoner for digitalt personvern. En proxyserver fungerer som en omdirigering på applikasjonslaget og maskerer IP-adressen din for bestemte programmer uten å kryptere dataene. En VPN opererer på nettverksnivå og sikrer all systemtrafikk med kryptering. Hvilket verktøy som passer best, avhenger av sikkerhetsbehovene dine.

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

Kontrollpunkt 1: Flervalgsutfordring

1. På hvilket lag i OSI-modellen opererer en vanlig HTTP-proxy?

- A. Fysisk lag
- B. Nettverkslag
- C. Applikasjonslaget
- D. Datalinklaget

2. Hva er en viktig protokollfordel ved SOCKS5 sammenlignet med vanlige HTTP-proxyer?

- A. Den tvinger frem full kryptering av nyttelasten
- B. Den støtter all TCP-/UDP-trafikkruting
- C. Den er immun mot DNS-lekkasjer
- D. Den opererer direkte i kjerneområdet

3. Hvorfor er et VPN vanligvis sikrere enn en proxyserver?

- A. Den kjører på raskere ekstern maskinvare
- B. Den krypterer all nettverkstrafikk for hele systemet
- C. Den krever ikke lokale rutingtabeller
- D. Den eliminerer nettverkslatens fullstendig

4. Hvilken proxytype omdirigerer trafikk uten kryptering som standard?

- A. En enkel HTTP-proxy
- B. En kryptert HTTPS-proxy
- C. En sikker WireGuard-klient
- D. En obfuskert VPN-server

5. Hva skjer med bakgrunnstrafikk fra apper når du bruker en nettleserproxy?

- A. Den krypteres automatisk
- B. Den blokkeres av proxy-serveren
- C. Den rutes gjennom proxy-tunnelen
- D. Den omgår proxyen og eksponerer IP-adressen din

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. En SOCKS5-proxy krypterer alt pakkeinnhold som går gjennom serveren.

○ Sant ○ Usant

7 Spørsmål 7

7. En VPN opererer på nettverkslaget for å sikre all systemtrafikk.

○ Sant ○ Usant

8 Spørsmål 8

8. Proxyer er vanligvis raskere enn VPN-er fordi de utfører dyp pakkekryptering.

○ Sant ○ Usant

9 Spørsmål 9

9. Å konfigurere en proxy krever at du setter opp omdirigering av trafikk inne i bestemte apper.

○ Sant ○ Usant

10 Spørsmål 10

10. Å bruke en proxy sikrer ikke datatrafikken din mot sporing fra den lokale internettleverandøren.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. En _____ på applikasjonslaget omdirigerer bestemt nettlesertrafikk uten å sikre andre apper.

2. En robust _____ innkapsler og krypterer alle datapakker fra enheten.

3. Protokollen _____ ligger mellom applikasjons- og transportlaget.

4. HTTP-proxyer fungerer på OSI-modellens _____ .

5. Vanlige proxyservere mangler _____ av nyttelasten, noe som gjør data sårbare.

6. En VPN gir _____ beskyttelse for alle nettverkskort.

ORDBANK

APPLIKASJONSLAG KRYPTERING PROXY SOCKS5 SYNLIGHET
SYSTEMDEKKENDE UDP-STØTTE VPN-TUNNEL

Skriv svarene dine her:

1. 2.

3. 4.

5. 6.

Kontrollpunkt 4: Koble nettverksbegreper

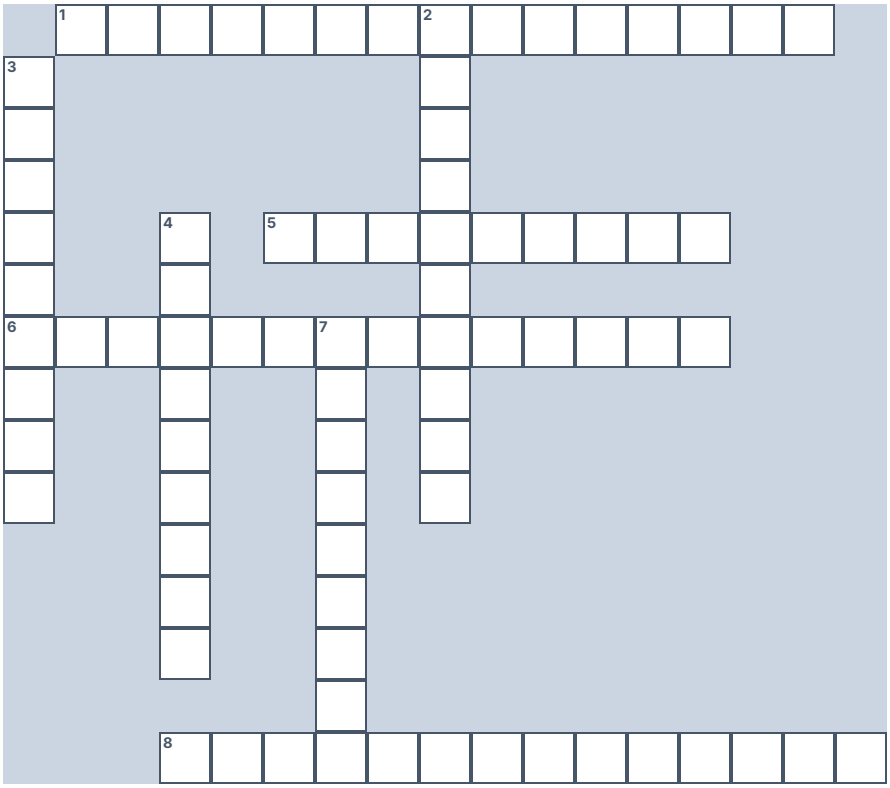
KOBLE DEFINISJONER

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

☐	1. HTTP-proxy	A	Ruting på operativsystemnivå som krypterer all applikasjonstrafikk.
☐	2. SOCKS5-proxy	B	Applikasjonslaget, der standard protokoller for webproxy fungerer.
☐	3. VPN-tunnel	C	SOCKS5s evne til å videresende UDP i tillegg til TCP, i motsetning til vanlige HTTP-proxyer.
☐	4. Systemomfattende	D	Klientutvidelse som bare skjuler trafikk inne i nettleserens sandkasse.
☐	5. OSI-lag 7	E	Kryptering og innkapsling som omslutter all bakgrunnstrafikk fra enheten.
☐	6. UDP-støtte	F	Trafikktilstand der ukrypterte proxydata forblir synlige for internettleverandører.
☐	7. Nettleserproxy	G	Proxy på applikasjonslaget som omdirigerer bestemt nettlesertrafikk.
☐	8. Innsyn for internettleverandøren	H	Proxyprotokoll mellom applikasjonslaget og transportlaget, uten kryptering.

Kontrollpunkt 5: Kryssord

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



VANNRETT

1. Lag 7, der standard webproxy-protokoller opererer (15)

5. SOCKS5s evne til å videresende UDP i tillegg til TCP, i motsetning til vanlige HTTP-proxyer (9)

6. Klientutvidelse som bare skjuler trafikk inne i nettleserens sandkasse (14)

8. Ruting på operativsystemnivå som krypterer all applikasjonstrafikk (14)

LODDRETT

2. Proxyprotokoll mellom applikasjons- og transportlaget, uten kryptering (10)

3. Kryptering og innkapsling som omslutter all bakgrunnstrafikk fra enheten (9)

4. Proxy på applikasjonslaget som omdirigerer bestemt nettlesertrafikk (9)

7. Trafikktilstand der ukryptert proxydata forblir synlig for internettleverandører (9)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

1 vannrett: Lag 7, der standard webproxy-protokoller opererer (15 bokstaver):

5 vannrett: SOCKS5s evne til å videresende UDP i tillegg til TCP, i motsetning til vanlige HTTP-proxyer (9 bokstaver):

6 vannrett: Klientutvidelse som bare skjuler trafikk inne i nettleserens sandkasse (14 bokstaver):

8 vannrett: Ruting på operativsystemnivå som krypterer all applikasjonstrafikk (14 bokstaver):

LODDRETT

2 loddrett: Proxyprotokoll mellom applikasjons- og transportlaget, uten kryptering (10 bokstaver):

3 loddrett: Kryptering og innkapsling som omslutter all bakgrunnstrafikk fra enheten (9 bokstaver):

4 loddrett: Proxy på applikasjonslaget som omdirigerer bestemt nettlesertrafikk (9 bokstaver):

7 loddrett: Trafikktilstand der ukryptert proxydata forblir synlig for internettleverandører (9 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

HTTPPROXY SOCKSPROXY VPNTUNNEL SYSTEMDEKKENDE APPLIKASJONSLAG
UDPSTØTTE NETTLESERPROXY SYNLIGHET

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. HTTPPROXY
B. SOCKSPROXY
C. VPNTUNNEL
D. SYSTEMDEKKENDE
E. APPLIKASJONSLAG
F. UDPSTØTTE
G. NETTLESERPROXY
H. SYNLIGHET

DEFINISJONER OG TILHØRENDE FELT	
	1. Lag 7, der standard webproxy-protokoller opererer.
	2. SOCKS5s evne til å videresende UDP i tillegg til TCP, i motsetning til vanlige HTTP-proxyer.
	3. Proxy på applikasjonslaget som omdirigerer bestemt nettlesertrafikk.
	4. Klientutvidelse som bare skjuler trafikk inne i nettleserens sandkasse.
	5. Kryptering og innkapsling som omslutter all bakgrunnstrafikk fra enheten.
	6. Ruting på operativsystemnivå som krypterer all applikasjonstrafikk.
	7. Trafikktilstand der ukryptert proxydata forblir synlig for internettleverandører.
	8. Proxyprotokoll mellom applikasjons- og transportlaget, uten kryptering.

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. RPPTHOXYT
2. LVETPNNUN
3. APOPAKJNSL SGALI
4. ESXPTREYEO RNTL
5. OPYOKRSSXC
6. MDEESNEDKS YKET
7. ØUTETSDTP
8. TIESLYGHN

Bonusaktivitet: Tenk raskt

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

1	Forskjeller mellom en proxy og en VPN			
2	Ting som forblir ukryptert uten en VPN			
3	Måter å gjenkjenne et falskt Wi-Fi-nettverk på			
4	Ting en mellommann gjør i hverdagen			
5	Situasjoner der en proxy er nok			
6	Enheter som kan bruke en VPN			
7	Proxytyper du kjenner til			
8	Ting en VPN kan skjule			
9	Myter om VPN-er			
10	Løfter en god VPN-leverandør gir			
11	Ting en VPN ikke kan beskytte deg mot			
12	Ord fra dette arbeidsarket du vil huske			
13	Grunner til å bruke en VPN på reise			
14	Situasjoner der du vil ha en VPN			
15	Steder der du ville brukt en VPN			

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 Coffee & Bytes på et åpent nettverk som heter «Free_Wi-Fi_No_Password». Jeg må logge inn på skole-e-posten min, og en venn sier at en gratis nettleserproxy er nok til å være trygg. Vil en proxy beskytte påloggingen og filene mine, eller trenger jeg en VPN?»

ALEX (REISENDE STUDENT)

👩‍💻 «Jeg er i utlandet, og en biologidokumentar som er vert i hjemlandet mitt, sier «Denne videoen er ikke tilgjengelig der du befinner deg nå.» En klassekamerat bruker en proxy, og jeg har en VPN. Hvorfor er jeg blokkert, og hvilket verktøy ville fungert bedre?»

Kontrollpunkt 9: Knekk chifferet

For å fullføre treningen i proxysammenligning må du dekryptere denne hemmelige meldingen om sikker tunneling.

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	13	4	9	18	9	7	5	18		20	18	1	6	9	11	11	5	14
		4	9	14		13	5	4		5	14		16	18	15	24	25	

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: Hva er en proxyserver?

En proxyserver er en mellommann som videresender forespørsler mellom applikasjonen din og målserveren. Nettstedet ser proxyens IP-adresse i stedet for din, men bare trafikk fra apper som er konfigurert til å bruke proxyen blir omdirigert, og en enkel proxy krypterer ikke denne trafikken.

Q3: Gjør en VPN meg helt anonym på nett?

Nei. Selv om en VPN skjuler IP-adressen din og krypterer trafikk, kan du fortsatt spores via informasjonskapsler i nettleseren, aktive kontoer (som Google eller Facebook), nettleserens fingeravtrykk eller hvis VPN-leverandøren din logger dataene dine.

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 en proxy en VPN?

Nei. En proxy videresender trafikk for bestemte apper, vanligvis uten kryptering. En VPN bygger en kryptert tunnel på nettverkslaget som frakter all trafikk fra enheten, inkludert apper i bakgrunnen.

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: Kan jeg bruke en gratis proxy?

Du kan, men gratis proxyer drives ofte av ukjente operatører. Fordi en enkel proxy ikke krypterer trafikken, kan operatøren se og til og med endre ukrypterte sider. Sjekk hvem som driver tjenesten før du bruker den.

Q7: Fører en proxy logger?

Det kan det. En proxy behandler hver forespørsel den videresender, så operatøren kan registrere IP-adressen din, nettstedene du besøker og når. Sjekk hvem som driver den og hva personvernerklæringen sier.

Q8: Når er en proxy nok?

En proxy kan være nok til oppgaver med lav risiko, som å endre den tilsynelatende plasseringen til én nettleser. For bank, offentlig Wi-Fi eller beskyttelse av alle apper på en enhet er en VPN det tryggere valget, fordi den krypterer all trafikk.

Q9: Kan en proxy beskytte alle appene på telefonen min?

Nei. Bare apper som respekterer proxy-innstillingen bruker den; resten kobler til direkte. En VPN-app ruter i stedet alle appene på telefonen gjennom den krypterte tunnelen sin.

Q10: Hva er en SOCKS5-proxy?

SOCKS5, definert i RFC 1928, er en proxyprotokoll som ligger mellom applikasjons- og transportlaget. Den kan videresende TCP-tilkoblinger og UDP-datagrammer og støtter autentisering, men har ingen innebygd kryptering. [1]

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

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

Q1: På hvilke nettverkslag opererer proxyer og VPN-er?

En HTTP-proxy fungerer på applikasjonslaget (lag 7) og forstår nettforespørsler. SOCKS5 ligger mellom applikasjons- og transportlaget. VPN-protokoller som IPsec eller WireGuard fungerer på nettverkslaget, slik at de kan frakte all IP-trafikk fra enheten.

Q2: Forblir et HTTPS-nettsted kryptert via en proxy?

Ja. Når du åpner et HTTPS-nettsted via en proxy, kjører TLS-kryptering ende-til-ende mellom nettleseren din og nettstedet, slik at proxyen ser domenet, men ikke sideinnholdet. Vanlige HTTP-sider er fortsatt lesbare.

Q3: Hva er WebRTC-lekkasje, og hvordan forhindrer en VPN den?

WebRTC er en nettleserprotokoll som kan avsløre dine ekte lokale og offentlige IP-adresser selv når et VPN er aktivt. Premium VPN-er blokkerer eller forfalsker WebRTC-forespørsler i appene for skrivebord og mobil og i nettleserutvidelsene sine.

Q4: Hva er en transparent proxy, og hvem bruker den?

En transparent proxy avskjærer trafikk uten noe oppsett på brukerens enhet. Skoler, bedrifter og internettleverandører bruker dem til mellomlagring eller innholdsfiltrering. Brukere vet ofte ikke at en er på plass, og den gir dem ikke noe personvern.

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 er split tunneling, og når bør jeg bruke det?

Split tunneling lar deg velge hvilke apper som rutes gjennom den krypterte VPN-tunnelen, og hvilke som kobler seg direkte til internett. Bruk det til å rute sensitive bankapper gjennom VPN-en mens lokale spill kobler seg direkte, slik at du unngår forsinkelsen VPN-en legger til.

Q7: Hvorfor kan en proxy føles raskere enn en VPN-tilkobling?

En enkel proxy hopper over kryptering og håndterer bare trafikk fra én app, så den gir mindre prosessering. En VPN krypterer hver pakke fra enheten. Med moderne protokoller er forskjellen ofte liten, og proxyen gir langt mindre beskyttelse.

Q8: Kan nettsteder se at jeg bruker en proxy eller en VPN?

Ofte, ja. Mange nettsteder sjekker IP-adresser mot lister over kjente proxy- og VPN-servere, og HTTP-proxyer kan legge til hoder som Via eller X-Forwarded-For. Strømmetjenester blokkerer ofte begge deler.

Q9: Hva er beskyttelse mot DNS-lekkasjer?

DNS-lekkasjebeskyttelse tvinger enheten din til å sende oppslagsforespørsler for nettsteder (DNS-forespørsler) gjennom VPN-ens private, krypterte DNS-servere i stedet for internettleverandørens servere. Dette hindrer internettleverandøren din i å spore hvilke nettsteder du besøker.

Q10: Kan en proxy stoppe struping fra internettleverandøren?

Sjelden. En enkel proxy krypterer ikke trafikk, så internettleverandøren kan fortsatt se hva slags aktivitet det er. En VPN skjuler trafikktyper, men ingen av verktøyene løser overbelastning eller databegrensninger.

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. SOCKS-STANDARD

SOCKS Protocol Version 5 ble publisert av IETF som RFC 1928 i mars 1996 og er fortsatt referansespesifikasjonen for SOCKS5-proxyer som brukes av nettlesere og apper i dag. [1]

2. SHIM-LAG

RFC 1928 beskriver SOCKS som et mellomlag mellom applikasjonslaget og transportlaget, så det kan ikke videresende trafikk på nettverkslaget, for eksempel ICMP. [1]

3. UDP-RELÉ

SOCKS5 la til kommandoen UDP ASSOCIATE, som lar en proxy videresende UDP-datagrammer i tillegg til TCP-tilkoblinger, noe vanlige HTTP-proxyer ikke håndterer. [1]

4. STANDARD SOCKS-PORT

SOCKS5-klienter kobler til proxyserveren på TCP-port 1080 som standard, slik det er definert i RFC 1928; mange proxytjenester lar brukerne velge andre porter. [1]

5. HTTP-MELLOMLEDD

HTTP-standarden (RFC 9110) definerer en proxy som en meldingsvideresendende agent valgt av klienten, som videresender forespørsler mot opprinnelsesserveren.

6. DYP PAKKEINSPEKSJON

Deep Packet Inspection (DPI) undersøker pakkeinnhold og trafikkmønstre; ukryptert proxy-trafikk er fullt synlig for den, mens VPN-trafikk avslører langt mindre.

7. VPN-ER PÅ NETTVERKSLAGET

IPsec, beskrevet i NIST SP 800-77, beskytter trafikk på nettverkslaget, slik at IP-pakkene til alle applikasjoner kan sikres uten oppsett for hver enkelt app. [2]

8. KUN NETTLESER

En proxy som er satt opp i én nettleser, påvirker bare den nettleseren; e-postklienter, spill og systemoppdateringer fortsetter å bruke enhetens vanlige tilkobling.

9. TOR MOT PROXYER

Tor sender trafikk gjennom tre frivillige reléer (guard, midtre og exit) og nås vanligvis via en lokal SOCKS-proxy, noe som legger til lag en enkelt proxy ikke kan gi.

10. AVVEINING MOT HASTIGHET

Proxyer kan virke raskere fordi de hopper over kryptering, men moderne VPN-protokoller som WireGuard gir lite overhead samtidig som de beskytter all trafikk på enheten.

Tekniske referanser og kilder

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

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

[2] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

Fasit: Sammenligning av proxy-servere og virtuelle private nettverk, krypteringsforskjeller og ruting på appnivå kontra systemnivå

1 **Proxyens OSI-lag** PROTOKOLLER — **Riktig svar: C**

MERKNAD TIL LÆREREN

Standard HTTP/HTTPS-proxyer opererer på applikasjonslaget (lag 7) og omdirigerer bestemt nettlesertrafikk. De mangler systemomfattende nettverksruting.

2 **Spørsmål 2** — **Riktig svar: B**

MERKNAD TIL LÆREREN

SOCKS5 videresender TCP- og UDP-trafikk mellom applikasjonslaget og transportlaget, men krypterer ikke som standard, mens HTTP-proxyer håndterer nettforespørsler.

3 **VPN-systemkryptering** WI-FI-SIKKERHET — **Riktig svar: B**

MERKNAD TIL LÆREREN

En VPN kapsler inn og krypterer all operativsystemtrafikk i hele systemet, mens en proxy bare omdirigerer trafikk for bestemte konfigurerte applikasjoner.

4 **Manglende kryptering i proxyer** RUTINGKONTROLLER — **Riktig svar: A**

MERKNAD TIL LÆREREN

HTTP-proxyer videresender nettlesertrafikk på applikasjonslaget uten å kryptere pakkenes nyttelast, noe som betyr at nettverksoperatøren eller internettleverandøren din fortsatt kan spore innholdstrafikken din.

5 **Sårbarhet ved omgåelse** PERSONVERN — **Riktig svar: D**

MERKNAD TIL LÆREREN

Nettleserproxyer bruker bare regler i selve nettleseren. Bakgrunnsapper, oppdateringer av operativsystemet og e-postklienter omgår proxyen og avslører din opprinnelige IP-adresse.

Fasit: Kontrollpunkt 2 – sant eller usant

6 Spørsmål 6

Riktig svar: Usant

MERKNAD TIL LÆREREN

SOCKS5 videresender trafikk mellom applikasjonslaget og transportlaget, men utfører ingen kryptering som standard, så innholdet i pakkene er lesbart under overføring.

7 Tunneler på nettverkslaget HASTIGHETER

Riktig svar: Sant

MERKNAD TIL LÆREREN

Ved å kjøre på nettverkslaget ruter og krypterer en VPN utgående trafikk fra enheten din, noe som bidrar til å beskytte trafikk i hele systemet.

8 Krypteringsbegrensning i proxyer SNIFFINGRISIKO

Riktig svar: Usant

MERKNAD TIL LÆREREN

Proxyer kan noen ganger være raskere, men det er fordi de IKKE utfører kryptering. Mangelen på kryptering gjør dataene sårbare for inspeksjon.

9 Omdirigering på appnivå BRANNMURER

Riktig svar: Sant

MERKNAD TIL LÆREREN

I motsetning til VPN-er for hele systemet krever proxyservere manuelt oppsett i nettleserinnstillinger eller programspesifikke proxyfelt.

10 Risiko for sporing fra internettleverandør INGEN LOGGING

Riktig svar: Sant

MERKNAD TIL LÆREREN

Fordi vanlige HTTP-/SOCKS5-proxyer ikke krypterer nyttelastdata, beholder din lokale internettleverandør full innsikt i det du gjør på nettet.

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. HTTP-proxy	H 2. SOCKS5-proxy	E 3. VPN-tunnel	A 4. Systemomfattende
B 5. OSI-lag 7	C 6. UDP-støtte	D 7. Nettleserproxy	F 8. Innsyn for internettleverandøren

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 PROXY	2 VPN-TUNNEL	3 SOCKS5	4 APPLIKASJONSLAG
5 KRYPTERING	6 SYSTEMDEKKENDE		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 E – APPLIKASJONSLAG	2 F – UDPSTØTTE	3 A – HTTPPROXY	4 G – NETTLESERPROXY
5 C – VPNTUNNEL	6 D – SYSTEMDEKKENDE	7 H – SYNLIGHET	8 B – SOCKSPROXY

DISKUSJONSNOTATER TIL LÆRERE

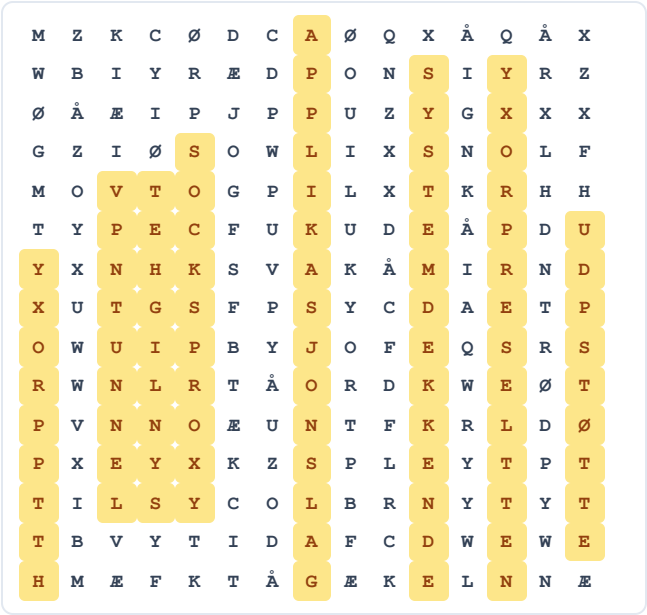
Nøkkelbegreper:
Kontroller at elevene kan forklare HTTP-proxy, SOCKS5-proxy og VPN-tunnel med egne ord og gi et eksempel på hvert.

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.

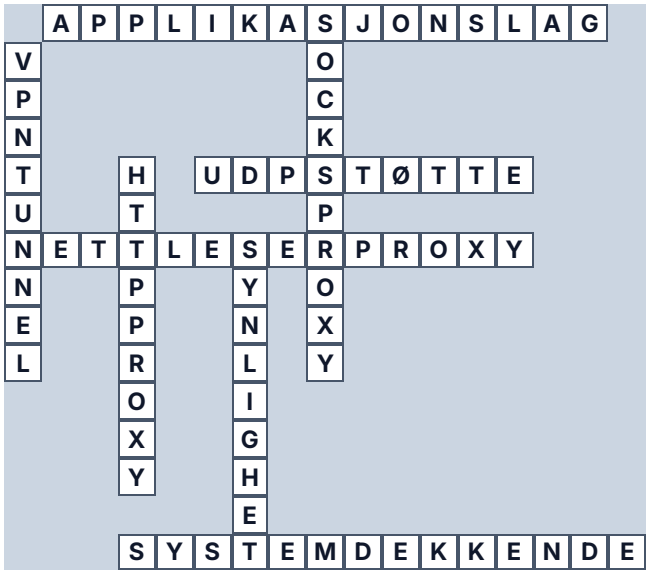
Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET



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

KRYSSORDLØSNING



	A	P	P	L	I	K	A	S	J	O	N	S	L	A	G
V								O							
P								C							
N								K							
T			H		U	D	P	S	T	Ø	T	T	E		
U			T					P							
N	E	T	T	L	E	S	E	R	P	R	O	X	Y		
N			P			Y		O							
E			P			N		X							
L			R			L		Y							
			O			I									
			X			G									
			Y			H									
						E									
			S	Y	S	T	E	M	D	E	K	K	E	N	D	E

LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

1 vannrett: APPLIKASJONSLAG Lag 7, der standard webproxy-protokoller opererer (15 bokstaver)

5 vannrett: UDPSTØTTE SOCKS5s evne til å videresende UDP i tillegg til TCP, i motsetning til vanlige HTTP-proxyer (9 bokstaver)

6 vannrett: NETTLESERPROXY Klientutvidelse som bare skjuler trafikk inne i nettleserens sandkasse (14 bokstaver)

8 vannrett: SYSTEMDEKKENDE Ruting på operativsystemnivå som krypterer all applikasjonstrafikk (14 bokstaver)

LODDRETT

2 loddrett: SOCKSPROXY Proxyprotokoll mellom applikasjons- og transportlaget, uten kryptering (10 bokstaver)

3 loddrett: VPNTUNNEL Kryptering og innkapsling som omslutter all bakgrunnstrafikk fra enheten (9 bokstaver)

4 loddrett: HTTPPROXY Proxy på applikasjonslaget som omdirigerer bestemt nettlesertrafikk (9 bokstaver)

7 loddrett: SYNLIGHET Trafikktilstand der ukryptert proxydata forblir synlig for internettleverandører (9 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. R P P T H O X Y T — **HTTPPROXY**
2. L V E T P N N U N — **VPNTUNNEL**
3. A P O P A K J N S L S G A L I — **APPLIKASJONSLAG**
4. E S X P T R E Y E O R N T L — **NETTLESERPROXY**
5. O P Y O K R S S X C — **SOCKSPROXY**
6. M D E E S N E D K S Y K E T — **SYSTEMDEKKENDE**
7. Ø U T E T S D T P — **UDPSTØTTE**
8. T I E S L Y G H N — **SYNLIGHET**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"OMDIRIGER TRAFIKKEN DIN MED EN PROXY"

Fasit til casestudiene

A Scenario A: Sikkerhet på offentlige nettverk

SNIFFING OG KRYPTERING | Sarahs dilemma

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Risikoer: Pakkesniffing, avlytting av data og man-in-the-middle-angrep. Noen på det samme nettverket på kafeen kan fange opp innloggingsopplysningene hennes eller lekse-filen hennes.
- Proxy mot VPN: En enkel nettleserproxy krypterer ikke trafikken hennes. En VPN krypterer alt på enheten, slik at avlyttede pakker blir uleselige for lokale snoker.

B Scenario B: Tilgang til blokkerte ressurser

GEOBLOKKERING OG IP-ADRESSER | Alex' dilemma

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Hvorfor blokkert: Strømmetjenesten bruker geoblokkering, som kobler reisendes lokale IP-adresse til hans fysiske land og blokkerer den basert på territoriell lisensiering.
- Hva fungerer best: Begge gir ham en IP-adresse fra hjemlandet, men en proxy dekker bare den konfigurerte appen, mens et VPN også krypterer all trafikk fra enheten hans.