

Navn: _____

Dato: _____

Point: _____

Hvad er en VPN Opgaveark

Praktiske øvelser i netværksprotokoller, tunnelering og sikkerhedskontroller.

OVERBLIK OVER VPN-LÆRING

ELEV

ELEVSTATUS

Netværksforsvarer-spor

SIKKER

FORBINDELSSTATUS

Beskytter datapakker

100%

LÆKAGEFORSVAR

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.

Åbn VPN.com's VPN-guide

URL: <https://www.vpn.com/vpn/>

Din VPN-læringsplan

- Forklar begreberne datatunnelering og indkapsling.
- Identificér standardkonfigurationer af protokoller og krypteringsmetoder.
- Analysér serveres og IP-maskerings rolle i virtuelle private netværk.
- Forstå hvordan internetudbydere sporer din browsing, og hvordan en VPN forhindrer det.
- Afgræns de operationelle rammer for virtuel netværkstopologi.

VEJLEDNING TIL HVAD ER EN VPN

Besvar multiple choice- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden på virkelige scenarier i casestudieafsnittet.

HVAD ER EN VPN? (INTRODUKTION)

Et virtuelt privat netværk er mere end blot en privatlivsknap. Det er en krypteret tunnel, der leder din internettrafik gennem en fjernserver. Det skjuler din IP-adresse, forhindrer din internetudbyder i at samle logfiler over dine handlinger online og sikrer dine data på offentlige netværk. Det er afgørende at forstå terminologien for at bevare den digitale sikkerhed.

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

Kontrolpunkt 1: Multiple choice-udfordring

1. Hvad er hovedformålet med et virtuelt privat netværk (VPN)?

- ☐ A. At øge browserens gengivelseshastighed
- ☐ B. At kryptere datapakker og skjule din offentlige IP
- ☐ C. At gemme cookie-databaser lokalt
- ☐ D. At erstatte din fysiske computerhardware

2. Hvad er netværkstunnelering i forbindelse med en VPN?

- ☐ A. At slette dublerede netværkslogfiler
- ☐ B. At installere lokale databasefiler
- ☐ C. At dele filer med andre lokale computere
- ☐ D. At indkapsle én netværkspakke i en anden sikker pakke

3. Hvilken krypteringsstandard anvendes oftest af moderne VPN'er?

- ☐ A. Forældet DES-kryptering
- ☐ B. Moderne AES-256-standard
- ☐ C. Base64-kodning i klartekst
- ☐ D. Almindelig rot13-kryptering

4. Hvilken del af din netværkstrafik krypteres af en VPN?

- ☐ A. Kun lokale printjob på netværket
- ☐ B. Ethernet-kablets fysiske føringsvej
- ☐ C. Hele nyttelastdelen af netværkspakken
- ☐ D. Kun din browsers søgehistorik

5. Hvad betyder begrebet "kryptering" inden for netværk?

- ☐ A. At omdanne klartekst til ulæselig kryptotekst
- ☐ B. At slette gamle kommunikationsoptegnelser
- ☐ C. At øge dine lokale båndbreddegrænser
- ☐ D. At dele databasenøgler offentligt

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. En VPN krypterer din trafik for at forhindre lokal aflytning på offentligt Wi-Fi.

☐

Sandt

☐

Falsk

7 Spørgsmål 7

7. En VPN ændrer fysisk hardwarekonfigurationen på din router.

☐

Sandt

☐

Falsk

8 Spørgsmål 8

8. Tunneleringsprotokoller pakker datapakker ind i et krypteret transportlag.

☐

Sandt

☐

Falsk

9 Spørgsmål 9

9. Symmetrisk kryptering bruger den samme nøgle til at kryptere og dekryptere trafik.

☐

Sandt

☐

Falsk

10 Spørgsmål 10

10. Brug af en VPN gør din internetforbindelse fysisk immun over for strømafbrydelser.

☐

Sandt

☐

Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. For at sikre din trafik pakker VPN'en dine datapakker ind i en anden protokol – en proces kaldet _____ .
2. Hvis du oplever langsomme downloadhastigheder under streaming, kan det skyldes begrænset netværks- _____ .
3. En streamingtjeneste, der kun er tilgængelig i ét bestemt land, anvender en _____ til at begrænse globale brugere.
4. De forbindelsesregler, der fastlægger kryptering og forbindelsesparametre, kaldes VPN'ens _____ .
5. Din computer bruger en lokal _____ til at overvåge netværkstrafik og blokere usikre forbindelser.
6. Når du opretter forbindelse til en VPN, ledes dine data gennem en fjern _____ for at skjule din offentlige IP.

ORDBANK MED FAGUDTRYK

BÅNDBREDDE

FIREWALL

GEOBLOKERING
SERVERISP
TUNNELERING

PRIVATLIV

PROTOKOL

Skriv dine svar her:

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

Kontrolpunkt 4: Match netværksbegreber

MATCH DEFINITIONER

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

1. Tunnelering

A

Internetudbyder, som logger din trafik, medmindre den er krypteret.

2. Protokol

B

Indpakning af datapakker i en anden pakke for sikker transport.

3. Båndbredde

H

Den maksimale dataoverførselshastighed på en forbindelse.

4. Server

D

En fjerncomputer, der leder din trafik og skjuler din IP.

5. Geoblokering

E

En begrænsning, der blokerer adgang ud fra fysisk placering.

6. Firewall

F

Et sikkerhedssystem, der overvåger og blokerer uautoriseret trafik.

7. Privatliv

G

Tilstanden af at være fri for sporing eller offentlig overvågning.

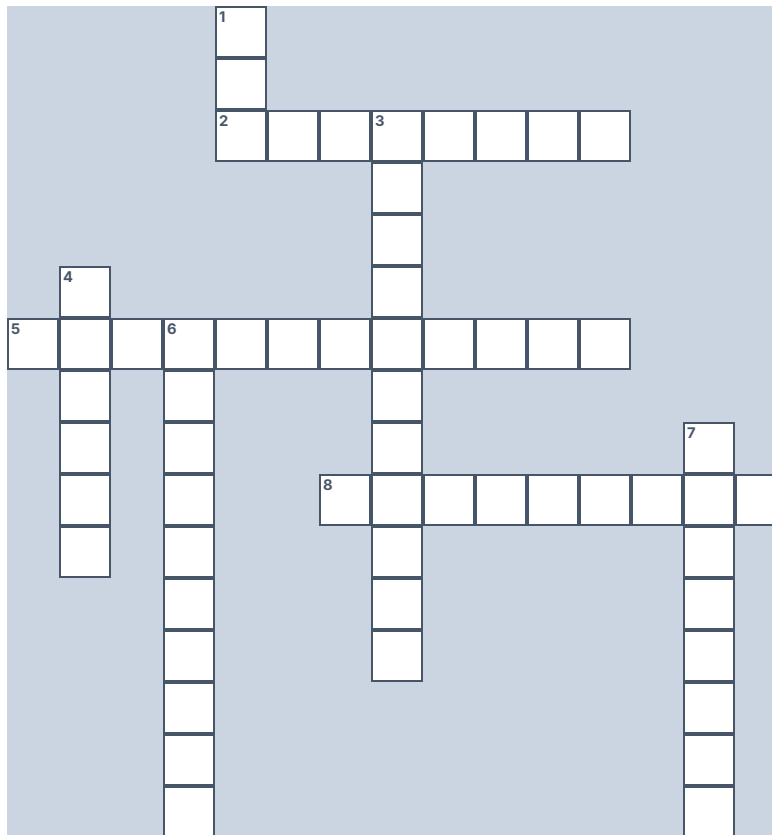
8. ISP

C

Et sæt regler, der bestemmer, hvordan data sendes over netværket.

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. Regler for hvordan data sendes og krypteres (8)
- 5. Blokering af adgang til websteder ud fra placering (12)
- 8. At være fri for sporing eller overvågning (9)

LODRETTE NØGLER

- 1. Internetudbyder, logger trafik medmindre den er krypteret (3)
- 3. Processen med at pakke datapakker ind i andre pakker (11)
- 4. Fjernserver, der leder trafik og skjuler din IP (6)
- 6. Hastighed for dataoverførsel på en forbindelse (10)
- 7. Sikkerhedssystem, der overvåger og blokerer trafik (8)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

2 vandret: Regler for hvordan data sendes og krypteres (8 bogstaver):

5 vandret: Blokering af adgang til websteder ud fra placering (12 bogstaver):

8 vandret: At være fri for sporing eller overvågning (9 bogstaver):

LODRETTE NØGLER

1 lodret: Internetudbyder, logger trafik medmindre den er krypteret (3 bogstaver):

3 lodret: Processen med at pakke datapakker ind i andre pakker (11 bogstaver):

4 lodret: Fjernserver, der leder trafik og skjuler din IP (6 bogstaver):

6 lodret: Hastighed for dataoverførsel på en forbindelse (10 bogstaver):

7 lodret: Sikkerhedssystem, der overvåger og blokerer trafik (8 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

TUNNELERING

PROTOKOL

BÅNDBREDDE
PRIVATLIVSERVER
ISP

GEOBLOKERING

FIREWALL

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. TUNNELERING
- B. PROTOKOL
- C. BÅNDBREDDE
- D. SERVER
- E. GEOBLOKERING
- F. FIREWALL
- G. PRIVATLIV
- H. ISP

DEFINITIONER OG MATCHFELTER

- ☐ 1. Et sæt regler for hvordan netværkstrafik krypteres og ledes. (B)
- ☐ 2. Indpakning af datapakker i andre pakker for sikker transport. (A)
- ☐ 3. Sikkerhedssystem, der overvåger og styrer netværkstrafik. (F)
- ☐ 4. Begrænsning af adgang til webtjenester ud fra enhedens placering. (E)
- ☐ 5. Den maksimale datamængde, der kan sendes over en forbindelse. (C)
- ☐ 6. En fjerncomputer, der leder trafik og skjuler din egen IP-adresse. (D)
- ☐ 7. Tilstanden af at være fri for uautoriseret sporing eller overvågning. (G)
- ☐ 8. Internetudbyder, som logger ukrypteret trafik. (H)

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. E E N U L R T I N G N

5. O K R L T P O O

2. D D B Å B E E D R N

6. E V S R R E

3. G E E K N R O O G L
I B

7. F L W A L I E R

4. A V I V L T P R I

8. P S I

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?"

Sidste udfordring: Afkod chifferet

En VPN krypterer din trafik for at sikre den. Brug bogstav-til-tal-nøglen nedenfor til at afkode cybersikkerhedsbeskeden ved at skrive de tilsvarende bogstaver i de tomme felter. Afkodet cybersikkerhedsbesked:

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

Afkodet cybersikkerhedsbesked:

<u>2</u>	<u>5</u>	<u>19</u>	<u>11</u>	<u>25</u>	<u>20</u>	<u>4</u>	<u>9</u>	<u>20</u>	<u>16</u>	<u>18</u>	<u>9</u>	<u>22</u>	<u>1</u>	<u>20</u>	<u>12</u>	<u>9</u>	<u>22</u>
<u>13</u>	<u>5</u>	<u>4</u>	<u>5</u>	<u>14</u>	<u>19</u>	<u>9</u>	<u>11</u>	<u>11</u>	<u>5</u>	<u>18</u>	<u>20</u>	<u>21</u>	<u>14</u>	<u>14</u>	<u>5</u>	<u>12</u>	

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z).

Kontrolpunkt 9: 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: Vil en VPN gøre min internethastighed langsommere?

Ja, en smule. Krypteringen og den fysiske afstand til VPN-serveren giver ekstra forsinkelse og overhead. Påvirkningen varierer efter udbyder, protokol, serverafstand, enhed og netværksforhold.

Q5: Er det lovligt at bruge en VPN?

Brug af VPN er lovligt i mange lande, men nogle jurisdiktioner begrænser, regulerer eller blokerer VPN-tjenester. Brugere bør tjekke gældende lokal lovgivning før brug. Se guiderne om lovlighed på VPN.com for flere detaljer.

Kontrolpunkt 9: Grundlæggende VPN-FAQ (del B)

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

Q6: Kan jeg bruge en gratis VPN?

Gratis VPN'er kan være baseret på reklamer, begrænsede funktioner, brugsanalyse, datalofter eller andre indtjeningsmodeller. Brugere bør gennemgå udbyderens privatlivspolitik, ejerskab, revisioner og forretningsmodel før brug.

Q7: Hvad er en "no-logs"-politik?

En no-logs-politik beskriver, hvilke aktivitets- og forbindelsesdata en udbyder oplyser, at den ikke gemmer. Omfanget varierer, så læsere bør gennemgå politikken og resultaterne af uafhængige revisioner.

Q8: Hvordan vælger jeg den bedste VPN?

Se efter reviderede no-logs-politikker, stærke protokoller (WireGuard, OpenVPN), sikre serverplaceringer, høje hastigheder, RAM-only-servere, en kill switch-funktion og en jurisdiktion uden for efterretningsalliancer (som 5/9/14 Eyes).

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 A)

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

Q1: Hvad er forskellen på WireGuard, OpenVPN og IKEv2?

WireGuard er en moderne, letvægtsprotokol (kun ca. 4.000 linjer kode) med høje hastigheder og hurtig forbindelse. OpenVPN er en meget sikker og gennemtestet open source-protokol. IKEv2 er fremragende til mobile enheder, fordi den hurtigt genopretter forbindelsen ved skift mellem netværk.

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

Multi-Hop leder din trafik gennem to eller flere VPN-servere i rækkefølge. Det tilføjer et ekstra krypteringslag og sikrer, at din rigtige IP-adresse forbliver skjult for det andet led, 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: Hvad er RAM-only-servere, og hvorfor er de vigtige?

Traditionelle servere skriver data til harddiske, som kan beslaglægges eller kompromitteres. RAM-only-servere (uden disk) kører udelukkende i flygtig hukommelse (RAM). Når serveren genstartes eller slukkes, slettes alle data øjeblikkeligt og permanent.

Q5: Hvordan omgår obfuskering VPN-blokeringer?

Obfuskering (eller "Stealth VPN") omformer VPN-trafikkens pakker, så de ligner almindelig, ukrypteret HTTPS-trafik (port 443). Det omgår Deep Packet Inspection (DPI), som myndigheder eller skole- og kontornetværk bruger til at blokere VPN'er.

Kontrolpunkt 10: Avanceret VPN-FAQ (del B)

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

Q6: Hvad er split tunneling, og hvornår bør jeg bruge det?

Split tunneling lader dig vælge, hvilke apps der sendes gennem den krypterede VPN-tunnel, og hvilke der forbinder direkte til internettet. Brug det til at sikre følsomme bankapps, mens du streamer lokale spil direkte uden forsinkelse.

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

PFS sikrer, at der genereres en unik, midlertidig krypteringsnøgle til hver enkelt session. Selv hvis en privat nøgle kompromitteres senere, kan den ikke bruges til at dekryptere tidligere eller fremtidige sessioner, fordi de brugte uafhængige nøgler.

Q8: Hvad er 5/9/14 Eyes-alliancerne, og hvorfor er de relevante?

Jurisdiktionen kan påvirke den juridiske proces, en udbyder kan møde, men den reelle privatlivsrisiko afhænger også af, hvilke data udbyderen gemmer, dens tekniske arkitektur, ejerskab, gennemsigtighedsrapportering og revisionshistorik.

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: Kan en VPN omgå internetudbyderens hastighedsbegrænsning?

Nogle gange. En VPN kan hjælpe, når en udbyder selektivt sænker genkendelige aktiviteter, men den løser ikke overbelastning, datalofter, hastighedsgrænser på kontoniveau eller dårlig netværkskvalitet.

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) blev udviklet i 1996 af Gurdeep Singh-Pall, en Microsoft-ingeniør, for at give virksomhedsmedarbejdere sikker fjernadgang [Ref 8].

2. MARKEDSVÆRDI

Det globale VPN-marked har oplevet hurtig vækst, drevet af stigende krav om fjernarbejde og virksomhedssikkerhed [Ref 2].

3. WIREGUARD-REVOLUTIONEN

WireGuard har en meget strømlinet kodebase designet til effektivitet, hvilket gør den lettere at revidere for sikkerhedshuller end traditionelle protokoller [Ref 9].

4. STRENGE REVISIONSSTANDARDER

Førende VPN-udbydere hyrer eksterne revisorer (som Cure53 eller PwC) til at foretage uafhængige kodegennemgange og bekræfte, at de ikke logger brugeraktivitet [Ref 10].

5. 5-EYES-ALLIANCENS OPRINDELSE

5-Eyes-netværket til deling af overvågning går tilbage til kryptografiske aftaler under 2. verdenskrig (UKUSA) om samarbejde om signalefterretning mellem de allierede lande [Ref 11].

6. DEEP PACKET INSPECTION

Avancerede firewalls bruger Deep Packet Inspection (DPI) til at analysere metadata i netværkspakker og blokere typiske kendetegn ved VPN-forbindelser [Ref 13].

7. ANVENDELSE I VIRKSOMHEDER

En stor del af virksomhedsmedarbejdere globalt bruger sikre VPN'er til at logge ind på interne databaser, hvilket gør det til en central sikkerhedsstandard [Ref 3].

8. DECENTRALISEREDE VPN'ER

Decentraliserede VPN'er (dVPN'er) fordeler trafik over et netværk af brugerdrevne knudepunkter og mindsker afhængigheden af én central udbyder [Ref 13].

9. TOR KONTRA VPN-ANONYMITET

En VPN sender trafik gennem én udbyder, mens Tor (The Onion Router) sender trafik via tre frivillige knudepunkter (Guard, Relay, Exit) for at maksimere privatlivet [Ref 13].

10. PRISEN FOR DATABRUD

Brug af en zero-trust-adgangsmodel sammen med en VPN hjælper organisationer med at beskytte immaterielle rettigheder og begrænse de økonomiske konsekvenser af databrud [Ref 12, Ref 14].

Tekniske referencer og kilder

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

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[1] Deloitte Advisory. (2025). Uafhængig privatlivsrevision af zero-knowledge-proxyarkitekturer.

<https://www.deloitte.com>

[3] WireGuard-projektet. (2021). Verifikation af moderne krypteringsmotorer i kernerummet.

<https://www.wireguard.com/papers/wireguard.pdf>

[5] Privacy Rights Clearinghouse. (2024). Ressourcer om forbrugerbeskyttelse og informationssikkerhed.

<https://privacyrights.org/>

[7] Open Web Application Security Project (OWASP). (2025). Application Security Verification Standard (ASVS): Sikker konfiguration.

<https://owasp.org/www-project-application-security-verification-standard/>

[9] NIST. (2023). Special Publication 800-77 Rev. 1: Vejledning til IPsec-VPN'er.

<https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final>

[2] IETF. (2020). RFC 8825: Evaluering af moderne kryptografiske tunneleringsprotokoller.

<https://datatracker.ietf.org/doc/rfc8825/>

[4] Cure53 Security Consulting. (2025). Arkiv over offentlige penetrationstest- og sikkerhedsvurderingsrapporter.

<https://github.com/cure53/Publications>

[6] European Digital Rights (EDRI). (2025). Verifikation af zero-logs og overholdelse af regler om datalagring.

<https://edri.org/>

[8] Center for Internet Security (CIS). (2024). Sikkerhedsretningslinjer for hjemme- og fjernarbejde.

<https://www.cisecurity.org/controls/cis-controls-list>

[10] ACM Queue. (2022). Udviklingen af virtuelle private netværk og tunneleringsarkitekturer.

<https://queue.acm.org/detail.cfm?id=3546931>

Facitliste: Hvad er en VPN – Opgaveark

1 Hovedfunktion PROTOKOLLER

Rigtigt svar: B

UNDERVISNINGSNOTE

En VPN's hovedopgave er at etablere en krypteret tunnel, der beskytter datapakkernes indhold og skjuler brugerens offentlige IP-adresse. Kilde: IETF Tunnel RFC [Ref 2].

En VPN's hovedopgave er at etablere en krypteret tunnel, der beskytter datapakkernes indhold og skjuler brugerens offentlige IP-adresse.

2 Netværkstunnelering LATENS

Rigtigt svar: D

UNDERVISNINGSNOTE

Tunneleringsprotokoller indkapsler de oprindelige datapakker i ydre bærepakker, så de sikkert kan passere offentlige netværk. Kilde: IETF Tunnel RFC [Ref 2].

Tunneleringsprotokoller indkapsler de oprindelige datapakker i ydre bærepakker, så de sikkert kan passere offentlige netværk.

3 Moderne kryptering WI-FI-SIKKERHED

Rigtigt svar: B

UNDERVISNINGSNOTE

AES-256 er den symmetriske krypteringsstandard, som sikre klienter og offentlige myndigheder verden over har tillid til. Kilde: WireGuard-projektet [Ref 3].

AES-256 er den symmetriske krypteringsstandard, som sikre klienter og offentlige myndigheder verden over har tillid til.

4 Krypterede komponenter ROUTINGKONTROL

Rigtigt svar: C

UNDERVISNINGSNOTE

En VPN krypterer hele nyttelastdelen af IP-datapakker, så indholdet af transmissionen forbliver fortroligt. Kilde: IETF Tunnel RFC [Ref 2].

En VPN krypterer hele nyttelastdelen af IP-datapakker, så indholdet af transmissionen forbliver fortroligt.

5 Definition af kryptering PRIVATLIV

Rigtigt svar: A

UNDERVISNINGSNOTE

Kryptering bruger algoritmer til at omdanne klartekst til ulæselige krypterede datastrømme. Kilde: Deloitte Advisory [Ref 1].

Kryptering bruger algoritmer til at omdanne klartekst til ulæselige krypterede datastrømme.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 Aflytning IP-MASKERING

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Krypterede tunneler sikrer, at pakkernes indhold forbliver ulæseligt for aktører, der opfanger data på lokale Wi-Fi-netværk. Kilde: Deloitte Advisory [Ref 1].

Krypterede tunneler sikrer, at pakkernes indhold forbliver ulæseligt for aktører, der opfanger data på lokale Wi-Fi-netværk.

7 Hardwareændringer HASTIGHEDER

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

VPN'er er softwarebaserede netværkstunneler og ændrer ikke fysisk hardwaren i din gateway-router. Kilde: Cure53-revision [Ref 4].

VPN'er er softwarebaserede netværkstunneler og ændrer ikke fysisk hardwaren i din gateway-router.

8 Tunneleringspakker AFLYTNINGSRISIKO

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Tunnelering fungerer ved at pakke de oprindelige netværkspakker ind i transportheadere under transporten. Kilde: IETF Tunnel RFC [Ref 2].

Tunnelering fungerer ved at pakke de oprindelige netværkspakker ind i transportheadere under transporten.

9 Symmetriske nøgler FIREWALLS

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Symmetrisk kryptografi bruger en fælles nøgle til både at kryptere og dekryptere netværksstrømme. Kilde: WireGuard-projektet [Ref 3].

Symmetrisk kryptografi bruger en fælles nøgle til både at kryptere og dekryptere netværksstrømme.

10 Strømmimmunitet INGEN LOGS

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

En VPN krypterer kun aktive forbindelsessignaler; den kan ikke forhindre afbrydelser forårsaget af lokale strømafbrydelser. Kilde: EDRI's retningslinjer for datalagring [Ref 6].

En VPN krypterer kun aktive forbindelsessignaler; den kan ikke forhindre afbrydelser forårsaget af lokale strømafbrydelser.

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

- | | | | |
|--------------------------|----------------------|------------------------|--------------------|
| B 1. Tunnelering | C 2. Protokol | H 3. Båndbredde | D 4. Server |
| E 5. Geoblokering | F 6. Firewall | G 7. Privatliv | A 8. ISP |

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

- | | | | |
|----------------------|---------------------|-----------------------|-------------------|
| 1 TUNNELERING | 2 BÅNDBREDDE | 3 GEOBLOKERING | 4 PROTOKOL |
| 5 FIREWALL | 6 SERVER | | |

DISKUSSIONSNOTER TIL UNDERVISERE

Dataindkapsling:

Diskutér, hvordan tunnelering indkapsler TCP/IP-pakker i en anden nyttelast og skjuler metadata som headere.

Internetcensur:

Diskutér, hvordan geoblokering fungerer via databaseopslag på offentlige IP-adresser, og hvordan en proxy eller VPN omgår denne kontrol.

Risici ved offentlige netværk:

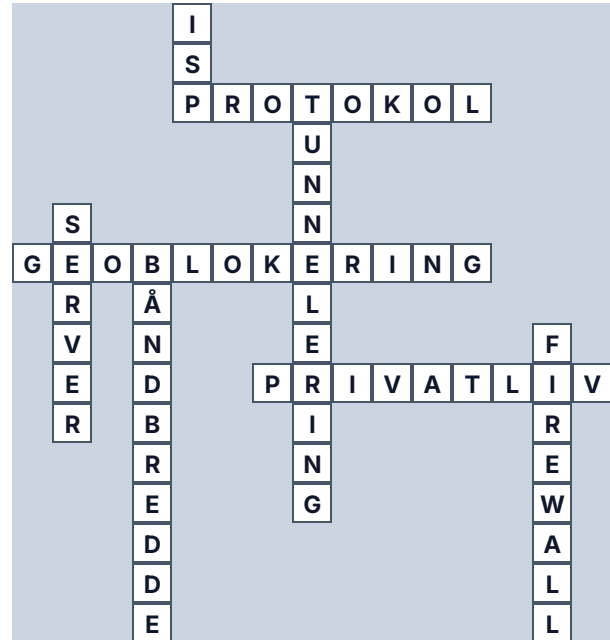
Fremhæv, at HTTPS krypterer indholdet, mens en VPN korrekt konfigureret kan beskytte DNS-forespørgsler og destinationstrafik mod det lokale netværk – men internetudbyderen kan stadig se VPN-serverens adresse, trafikmængden og tidspunkterne.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: PROTOKOL Regler for hvordan data sendes og krypteres (5,7)

5 vandret: GEOBLOKERING Blokering af adgang til websteder ud fra placering (9,3)

8 vandret: PRIVATLIV At være fri for sporing eller overvågning (12,9)

LODRETTE NØGLER

1 lodret: ISP Internetudbyder, logger trafik medmindre den er krypteret (3,7)

3 lodret: TUNNELERING Processen med at pakke datapakker ind i andre pakker (5,10)

4 lodret: SERVER Fjernserver, der leder trafik og skjuler din IP (8,4)

6 lodret: BÅNDBREDDE Hastighed for dataoverførsel på en forbindelse (9,6)

7 lodret: FIREWALL Sikkerhedssystem, der overvåger og blokerer trafik (11,16)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. EENULRTINGN	TUNNELERING	5. OKRLTPOO	PROTOKOL
2. DDBÅBEEDRN	BÅNDBREDDE	6. EVSRRE	SERVER
3. GEEKNROOGLIB	GEOBLOKERING	7. FLWALIER	FIREWALL
4. AVIVLTPRI	PRIVATLIV	8. PSI	ISP

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"BESKYT DIT PRIVATLIV MED EN SIKKER TUNNEL"

Facit til casestudier

A

Scenarie A: Sikkerhed på offentlige netværk

AFLYTNING OG
KRYPTERINGSarahs
dilemma

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Risici: Pakkeaflytning, opsnapping 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 opsnappt 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-
ADRESSERAlex'
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.