Navn: _____ Dato: _____ Point: _____

VPN.com: guide til VPN Opgaveark

Praktiske øvelser i netværksprotokoller, tunnelering og sikkerhedskontroller.

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 begreberne datatunnelering og indkapsling.
- Identificér standardkonfigurationer af protokoller og krav til båndbredde.
- Analysér firewalls og geoblokerings rolle i internettets routing.
- Forstå hvordan udbydere sporer ukrypteret surfing, og hvordan en VPN forhindrer det.
- Afgræns betydningen af serverplacering og jurisdiktion.

VEJLEDNING TIL VPN-GUIDEN

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 virkelige scenarier i casestudieafsnittet. Slut af med bonusaktiviteten Tænk hurtigt.

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: Flervalgsopgave

1. Hvad er en VPN-protokol?

- A. En enhed, der forbinder kabler.
- B. Regler for, hvordan data krypteres og sendes.
- C. Et browserplugin, der blokerer reklamer.
- D. En internetudbyder.

2. Hvad er den mest sandsynlige årsag, hvis VPN'en føles langsom?

- A. VPN-serveren er for langt væk eller overbelastet.
- B. Skærmens opløsning er for høj.
- C. Du har slået cookies fra i browseren.
- D. Tastaturet er sat forkert op.

3. Hvorfor anbefales VPN på offentligt wi-fi?

- A. Den gør forbindelsen gratis.
- B. Den øger routerens rækkevidde.
- C. Den krypterer trafikken, så hackere på samme net ikke kan læse den.
- D. Den sletter automatisk spam.

4. Hvad beskriver en geoblokering?

- A. Et værktøj, der måler afstanden til en server.
- B. En begrænsning, der spærrer adgang ud fra placering.
- C. En protokol til komprimering af filer.
- D. En metode til backup.

5. Hvad kan din internetudbyder se, når du bruger VPN?

- A. Dine søgeord og de sider, du ser.
- B. At du er koblet på en VPN, men ikke hvad trafikken indeholder.
- C. Intet, heller ikke at du er online.
- D. Filer og billeder på din harddisk.

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Skjult placering

6. En VPN skjuler enhedens offentlige IP-adresse, så websteder ikke let kan se, hvor du befinder dig.

Sandt Falsk

7 VPN og hastighed

7. Med VPN slået til bliver din internetforbindelse dobbelt så hurtig som uden.

Sandt Falsk

8 Aflytning på offentligt wi-fi

8. Bruger du usikret offentligt wi-fi uden VPN, kan andre på nettet opsnappe din ukrypterede trafik.

Sandt Falsk

9 Firewalls og blokerede forbindelser

9. Administratorer kan sætte firewalls op til at opdage og blokere udgående VPN-tunneler.

Sandt Falsk

10 Strenge politikker uden logning

10. En streng politik om ingen logning betyder, at udbyderen ved lov skal gemme dine søgninger og besøgte links i mindst 30 dage.

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 PRIVATLIV PROTOKOL SERVER TUNNELERING UDBYDER

Skriv dine svar her:

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

Kontrolpunkt 4: Match netværksbegreber

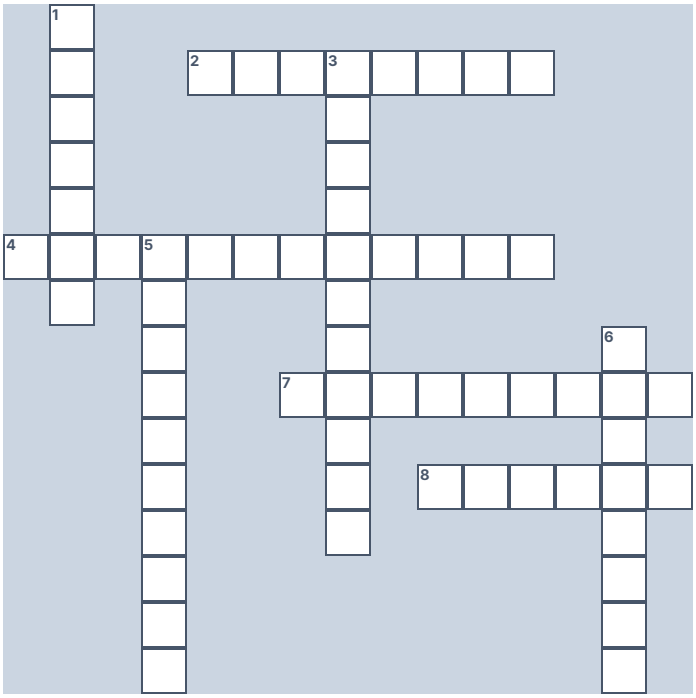
MATCH BEGREBER OG DEFINITIONER

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

	1. Tunnelering	A	Et sæt regler, der bestemmer, hvordan data sendes over netværket.
	2. Protokol	B	Den maksimale dataoverførselshastighed på en forbindelse.
	3. Båndbredde	C	En begrænsning, der blokerer adgang ud fra fysisk placering.
	4. Server	D	Et sikkerhedssystem, der overvåger og blokerer uautoriseret trafik.
	5. Geoblokering	E	En fjerncomputer, der leder din trafik og skjuler din IP.
	6. Firewall	F	Tilstanden af at være fri for sporing eller offentlig overvågning.
	7. Privatliv	G	Internetudbyder, der fører din trafik og kan se ukrypteret aktivitet.
	8. ISP	H	Indpakning af datapakker i en anden pakke for sikker transport.

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. Regelsæt, der bestemmer, hvordan data overføres over netværket (8)

4. Begrænsning, der forhindrer adgang til nettet ud fra fysisk placering (12)

7. Tilstanden at være fri for sporing og offentlig overvågning (9)

8. Fjern computer, der sender din trafik videre og skjuler din IP (6)

LODRETTE NØGLER

1. Internet..., der fører din trafik og kan se ukrypteret aktivitet (7)

3. Indpakning af datapakker i en anden pakke for sikker overførsel (11)

5. Den maksimale hastighed for dataoverførsel over en forbindelse (10)

6. Sikkerhedssystem, der overvåger og blokerer uautoriseret trafik (8)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

2 vandret: Regelsæt, der bestemmer, hvordan data overføres over netværket (8 bogstaver):

4 vandret: Begrænsning, der forhindrer adgang til nettet ud fra fysisk placering (12 bogstaver):

7 vandret: Tilstanden at være fri for sporing og offentlig overvågning (9 bogstaver):

8 vandret: Fjern computer, der sender din trafik videre og skjuler din IP (6 bogstaver):

LODRETTE NØGLER

1 lodret: Internet..., der fører din trafik og kan se ukrypteret aktivitet (7 bogstaver):

3 lodret: Indpakning af datapakker i en anden pakke for sikker overførsel (11 bogstaver):

5 lodret: Den maksimale hastighed for dataoverførsel over en forbindelse (10 bogstaver):

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

Kontrolpunkt 6: Skjult ordjagt

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

U D B Y D E R P V Ø X C Å Y G

G L L I Å D O R E S P Z R C W

N L B A Å P E I M A R E Q E F

I A H J D T S V N F O J U Å U

R W G S Y F A A A S T Q O B R

E E W Æ S L T T W U O D O Å Ø

L R B G U Z Z L K A K T Å N Ø

E I Ø M H J O I T L O N N D V

N F Q I S S H V Å A L Q X B G

N X C Ø T Ø B I N Å H K P R R

U G E O B L O K E R I N G E P

T Z C N Å Ø G Æ Q Y X M X D R

B P S E R V E R Y V N H X D D

Ø X L T B Z Å Æ N T S Æ J E Q

E A D L S Y Z Z M K I W I G B

ORDLISTE MED FAGUDTRYK

TUNNELERING BÅNDBREDDE GEOBLOKERING PROTOKOL FIREWALL SERVER UDBYDER PRIVATLIV

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. BÅNDBREDDE
C. GEOBLOKERING
D. PROTOKOL
E. FIREWALL
F. SERVER
G. UDBYDER
H. PRIVATLIV

DEFINITIONER OG MATCHFELTER
1. Internet..., der fører din trafik og kan se ukrypteret aktivitet.
2. Sikkerhedssystem, der overvåger og blokerer uautoriseret trafik.
3. Den maksimale hastighed for dataoverførsel over en forbindelse.
4. Fjern computer, der sender din trafik videre og skjuler din IP.
5. Begrænsning, der forhindrer adgang til nettet ud fra fysisk placering.
6. Regelsæt, der bestemmer, hvordan data overføres over netværket.
7. Tilstanden at være fri for sporing og offentlig overvågning.
8. Indpakning af datapakker i en anden pakke for sikker overførsel.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. EENULRTINGN
2. GELOGINOER KB
3. EIFWALLR
4. RDDYEUB
5. DREÅDEBBDN
6. OLTKPORO
7. ESVRRE
8. VAIPVRTLI

Bonusaktivitet: Tænk hurtigt

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

1	Ting, du forbinder med ordet 'tunnel'			
2	Ting, du vil lære din familie om VPN			
3	Ting på en hjemmeside, der kan spore dig			
4	Myter om VPN			
5	Ord fra dette opgaveark, du vil huske			
6	Enheder, der kan bruge en VPN			
7	Ting, en VPN ikke kan beskytte mod			
8	Lande, du ville ønske at 'besøge' online			
9	Ting, en god VPN-udbyder lover			
10	Måder at opdage et falsk wi-fi-net			
11	Spørgsmål, du har om VPN			
12	VPN-tjenester, du kender			
13	Ord, der har med privatliv at gøre			
14	Ting, en VPN kan skjule			
15	Grunde til at bruge VPN på en café			

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

En VPN krypterer din trafik for at beskytte den. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter.

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

5	14		22	16	14		11	18	25	16	20	5	18	5	18		4	9	14

20	18	1	6	9	11

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: 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 10: 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 C)

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. [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: Hvad er RAM-only-servere, og hvorfor er de vigtige?

Traditionelle servere skriver data til harddiske, som kan beslaglægges eller kompromitteres. RAM-only-servere (diskløse) kører udelukkende i flygtig hukommelse (RAM). Når serveren genstartes eller slukkes, slettes data i hukommelsen.

Q5: Hvordan omgår obfuskering VPN-blokeringer?

Obfuskering (eller "Stealth VPN") forklæder VPN-trafik, så den ligner almindelig HTTPS-trafik (port 443). Det kan hjælpe 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: Hvad er split tunneling, og hvornår bør jeg bruge det?

Split tunneling lader dig vælge, hvilke apps der går gennem den krypterede VPN-tunnel, og hvilke der forbinder direkte til internettet. Brug det til at sende følsomme bankapps gennem VPN'en, mens lokale spil forbinder direkte og undgår den ekstra forsinkelse fra VPN'en.

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 af en gruppe leverandører, herunder Microsoft, og offentliggjort som RFC 2637 i juli 1999 til understøttelse af VPN'er til fjernadgang. [6]

2. MARKEDSVÆRDI

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

3. WIREGUARD-REVOLUTIONEN

WireGuard har en meget slank kodebase, der er lettere at gennemgå for sårbarheder end traditionelle protokoller. [3]

4. STRENGE REVISIONSSTANDARDER

De største VPN-udbydere hyrer eksterne revisorer (som Cure53 eller PwC) til at gennemgå koden og bekræfte, at de ikke logger aktivitet.

5. 5-EYES-ALLIANCENS OPRINDELSE

Five Eyes-alliancen udsprang af UKUSA-aftalen om signalefterretning fra 1946 mellem USA og Storbritannien, som Canada, Australien og New Zealand senere tilsluttede sig.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) undersøger pakkernes indhold og trafikmønstre, ikke kun headere, og nogle firewalls bruger det til at opdage og blokere almindelige VPN-protokoller.

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.

8. DECENTRALISEREDE VPN'ER

Decentrale VPN'er (dVPN) fordeler trafikken på noder drevet af brugerne og gør én central udbyder mindre vigtig.

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 og exit), så intet enkelt relæ kender begge ender.

10. PRISEN FOR DATABRUD

En zero trust-model for sikker adgang sammen med VPN hjælper organisationer med at beskytte deres viden og begrænse de økonomiske følger af brud.

Tekniske referencer og kilder

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

FAGLITTERATUR OG SIKKERHEDSSTANDARDER

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.

https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.

https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

OVERSIGT OVER TEKNISKE STANDARDER

- Indpakning: RFC 4301 fastlægger sikker routing af pakker med IPsec/L2TP.
- Sporing hos udbyderen: Når DNS-opslag går gennem den krypterede tunnel, kan den lokale udbyder se mindre.
- Firewalls: Slørede pakker slipper forbi dyb pakkeinspektion.

Facitliste: Kontrolpunkt 1 – Flervalg

1 Spørgsmål 1

Rigtigt svar: B

UNDERVISNINGSNOTE

En VPN-protokol fastlægger reglerne for, hvordan tunnelen bygges, og data krypteres; de andre muligheder beskriver kabler, annonceblokkere og internetudbydere.

2 Spørgsmål 2

Rigtigt svar: A

UNDERVISNINGSNOTE

Afstand øger svartiden, og en overbelastet server har mindre kapacitet at dele ud af; skærmopløsning, cookies og tastaturlayout påvirker ikke forbindelseshastigheden.

3 Spørgsmål 3

Rigtigt svar: C

UNDERVISNINGSNOTE

På åbne netværk kan andre opfange ukrypterede pakker; en VPN krypterer trafikken, så opfangede data ikke kan læses.

4 Spørgsmål 4

Rigtigt svar: B

UNDERVISNINGSNOTE

Geoblokering matcher en besøgendes offentlige IP-adresse med en placeringsdatabase og nægter adgang uden for de tilladte områder.

5 Spørgsmål 5

Rigtigt svar: B

UNDERVISNINGSNOTE

Internetudbyderen kan se, at du sender krypterede data til en VPN-server, men ikke hvilke websteder du besøger, eller hvad du søger efter.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 Spørgsmål 6

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Websteder ser VPN-serverens IP-adresse i stedet for din, hvilket skjuler din omtrentlige placering for dem.

7 Spørgsmål 7

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Kryptering og det ekstra hop til VPN-serveren sænker som regel hastigheden en smule; en VPN kan ikke fordoble din grundlæggende forbindelseshastighed.

8 Spørgsmål 8

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

På usikret wi-fi kan værktøjer til pakkesniffing opfange ukrypteret trafik, fx logins, der sendes uden HTTPS.

9 Spørgsmål 9

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Administratorer kan blokere kendte VPN-porte, fx OpenVPN's 1194, eller bruge Deep Packet Inspection til at opdage VPN-trafik.

10 Spørgsmål 10

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

En no-logs-politik er en udbyders løfte om ikke at gemme registreringer af din aktivitet; ingen lov kræver, at VPN'er gemmer søgninger i 30 dage.

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

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

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

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

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 G – UDBYDER	2 E – FIREWALL	3 B – BÅNDBREDDE	4 F – SERVER
5 C – GEOBLOKERING	6 D – PROTOKOL	7 H – PRIVATLIV	8 A – TUNNELERING

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare Tunnelering, Protokol og Båndbredde med egne ord og give et eksempel på hvert begreb.

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

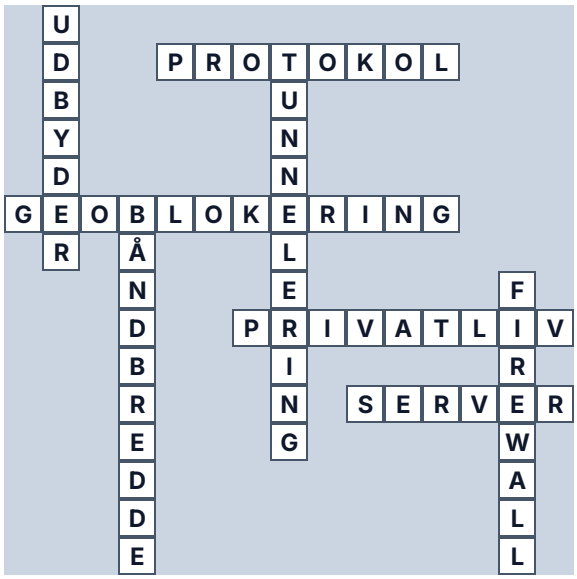
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



VANDRETTE NØGLER

2 vandret: PROTOKOL Regelsæt, der bestemmer, hvordan data overføres over netværket (8 bogstaver)

4 vandret: GEOBLOKERING Begrænsning, der forhindrer adgang til nettet ud fra fysisk placering (12 bogstaver)

7 vandret: PRIVATLIV Tilstanden at være fri for sporing og offentlig overvågning (9 bogstaver)

8 vandret: SERVER Fjern computer, der sender din trafik videre og skjuler din IP (6 bogstaver)

LODRETTE NØGLER

1 lodret: UDBYDER Internet..., der fører din trafik og kan se ukrypteret aktivitet (7 bogstaver)

3 lodret: TUNNELERING Indpakning af datapakker i en anden pakke for sikker overførsel (11 bogstaver)

5 lodret: BÅNDBREDDE Den maksimale hastighed for dataoverførsel over en forbindelse (10 bogstaver)

6 lodret: FIREWALL Sikkerhedssystem, der overvåger og blokerer uautoriseret trafik (8 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. E E N U L R T I N G N — **TUNNELERING**
2. G E L O G I N O E R K B — **GEOBLOKERING**
3. E I F W A L L R — **FIREWALL**
4. R D D Y E U B — **UDBYDER**
5. D R E Å D E B B D N — **BÅNDBREDDE**
6. O L T K P O R O — **PROTOKOL**
7. E S V R R E — **SERVER**
8. V A I P V R T L I — **PRIVATLIV**

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"EN VPN KRYPTERER DIN TRAFIK"

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.