Navn: _____ Dato: _____ Poeng: _____

Hva er et VPN Arbeidsark

Praktiske øvelser i nettverksprotokoller, tunnelering og sikkerhetskontroller.

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

- Forklar begrepene datatunnelering og innkapsling.
- Identifiser standard protokollkonfigurasjoner og krypteringsmetoder.
- Analyser rollene til servere og IP-maskering i virtuelle private nettverk.
- Forstå hvordan internettleverandører sporer nettlesing, og hvordan en VPN hindrer det.
- Skill mellom de operative grensene for virtuell nettverkstopologi.

INSTRUKSJONER FOR GUIDEN «HVA ER ET VPN?»

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på virkelige scenarioer i casestudie-delen. Avslutt med bonusaktiviteten Tenk raskt.

HVA ER ET VPN? (INNLEDNING)

Et virtuelt privat nettverk er mer enn bare en personvernbryter. Det er en kryptert tunnel som ruter internettrafikken din gjennom en ekstern server. Dette skjuler IP-adressen din, hindrer internettleverandøren din i å samle logger over nettaktiviteten din og sikrer dataene dine på offentlige nettverk. Å forstå terminologien er avgjørende for å opprettholde digital sikkerhet.

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

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er hovedfunksjonen til et virtuelt privat nettverk (VPN)?

- A. Å øke gjengivelseshastigheten i nettleseren
- B. Å kryptere datapakker og skjule den offentlige IP-adressen din
- C. For å lagre databaser med nettstedets informasjonskapsler lokalt
- D. For å erstatte den fysiske maskinvaren i datamaskinen din

2. Hva er nettverkstunnelering i sammenheng med et VPN?

- A. Å slette dupliserte nettverkslogger
- B. Å installere lokale databaselagringsfiler
- C. Å dele filer med andre lokale datamaskiner
- D. Å kapsle inn én nettverkspakke i en annen sikker pakke

3. Hvilken krypteringsstandard brukes mye til å beskytte VPN-trafikk?

- A. Utdatert DES-kryptering
- B. Moderne AES-256-standard
- C. Klartekstkoding med base64
- D. Vanlig rot13-chiffer

4. Hvilken del av nettverkstrafikken din krypteres av et VPN?

- A. Bare utskriftsjobber på det lokale enhetsnettverket
- B. Den fysiske ruten for Ethernet-kabelen
- C. Hele datanyttelasten i nettverkspakken
- D. Bare nettleserens søkehistorikk

5. Hva betyr begrepet «kryptering» i nettverk?

- A. Å gjøre klartekstdata om til uleselig chiffertekst
- B. Å slette gamle kommunikasjonsregistre
- C. Å øke grensene for din lokale båndbreddehastighet
- D. Å dele tilgangsnøkler til databasen offentlig

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. En VPN krypterer trafikken din for å hindre lokal avlytting på offentlig Wi-Fi.

○ Sant ○ Usant

7 Spørsmål 7

7. En VPN endrer fysisk maskinvarekonfigurasjonen til routeren din.

○ Sant ○ Usant

8 Spørsmål 8

8. Tunnelprotokoller pakker datapakker inn i et kryptert transportlag.

○ Sant ○ Usant

9 Spørsmål 9

9. Symmetrisk kryptering bruker samme nøkkel til å kryptere og dekryptere trafikk.

○ Sant ○ Usant

10 Spørsmål 10

10. Å bruke en VPN gjør internettforbindelsen din fysisk immun mot alle strømbrudd uten nett.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. For å sikre trafikken din pakker VPN-en datapakkene dine inn i en annen protokoll, en prosess som kalles _____ .

2. Hvis du opplever lav nedlastingshastighet under streaming, kan det skyldes begrenset _____ i nettverket.

3. En strømmetjeneste som bare er tilgjengelig i ett bestemt land, bruker _____ for å begrense brukere globalt.

4. Tilkoblingsreglene som definerer kryptering og tilkoblingsparametere, kalles VPN-ens _____ .

5. Datamaskinen din bruker en lokal _____ for å overvåke nettverkstrafikk og blokkere usikre tilkoblinger.

6. Når du kobler til en VPN, rutes dataene dine gjennom en ekstern _____ for å skjule din offentlige IP.

ORDBANK

BRANNMUR BÅNDBREDDE GEOBLOKKERING NETTLEVERANDØR PERSONVERN PROTOKOLL SERVER TUNNELERING

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble nettverksbegreper

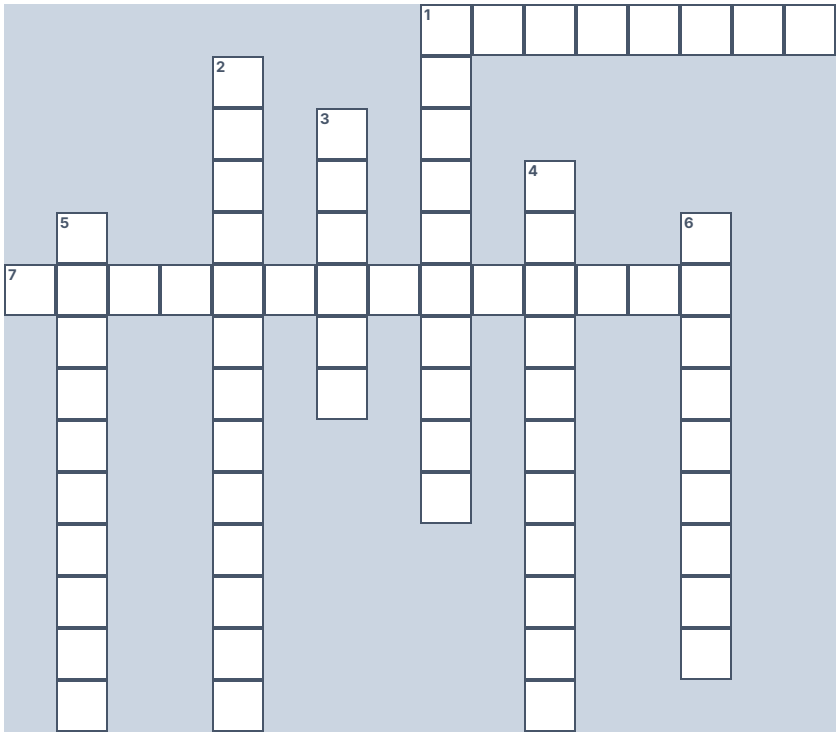
KOBLE DEFINISJONER

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

☐	1. Tunnelering	A	En ekstern datamaskin som ruter trafikken din og maskerer IP-adressen din.
☐	2. Protokoll	B	Internettleverandør som bærer trafikken din og kan se ukryptert aktivitet.
☐	3. Båndbredde	C	En begrensning som hindrer nettilgang basert på fysisk plassering.
☐	4. Server	D	Et sikkerhetssystem som overvåker og blokkerer uautorisert trafikk.
☐	5. Geoblokkering	E	Et sett med regler som bestemmer hvordan data overføres over nettverket.
☐	6. Brannmur	F	Tilstanden å være fri for sporing eller offentlig overvåking.
☐	7. Personvern	G	Den maksimale dataoverføringshastigheten over en tilkobling.
☐	8. Internettleverandør	H	Å pakke datapakker inn i en annen pakke for sikker overføring.

Kontrollpunkt 5: Kryssord

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



VANNRETT

1. Et sikkerhetssystem som overvåker og blokkerer uautorisert trafikk (8)

7. Internettleverandør, som logger trafikken din med mindre den er kryptert (14)

LODDRETT

1. Den maksimale datahastigheten for overføring over en tilkobling (10)

2. En begrensning som hindrer nettilgang basert på fysisk plassering (13)

3. En ekstern datamaskin som ruter trafikken din og skjuler IP-adressen din (6)

4. Innkapsling av datapakker i en annen pakke for sikker overføring (11)

5. Tilstanden av å være fri for sporing eller offentlig overvåking (10)

6. Et sett regler som bestemmer hvordan data overføres over nettverket (9)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

1 vannrett: Et sikkerhetssystem som overvåker og blokkerer uautorisert trafikk (8 bokstaver):

7 vannrett: Internettleverandør, som logger trafikken din med mindre den er kryptert (14 bokstaver):

LODDRETT

1 loddrett: Den maksimale datahastigheten for overføring over en tilkobling (10 bokstaver):

2 loddrett: En begrensning som hindrer nettilgang basert på fysisk plassering (13 bokstaver):

3 loddrett: En ekstern datamaskin som ruter trafikken din og skjuler IP-adressen din (6 bokstaver):

4 loddrett: Innkapsling av datapakker i en annen pakke for sikker overføring (11 bokstaver):

5 loddrett: Tilstanden av å være fri for sporing eller offentlig overvåking (10 bokstaver):

6 loddrett: Et sett regler som bestemmer hvordan data overføres over nettverket (9 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

TUNNELERING PROTOKOLL BÅNDBREDDE SERVER GEOBLOKKERING
BRANNMUR PERSONVERN NETTLEVERANDØR

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. TUNNELERING
B. PROTOKOLL
C. BÅNDBREDDE
D. SERVER
E. GEOBLOKKERING
F. BRANNMUR
G. PERSONVERN
H. NETTLEVERANDØR

DEFINISJONER OG TILHØRENDE FELT
_____ 1. Et sett regler som bestemmer hvordan data overføres over nettverket.
_____ 2. En begrensning som hindrer nettilgang basert på fysisk plassering.
_____ 3. Et sikkerhetssystem som overvåker og blokkerer uautorisert trafikk.
_____ 4. Tilstanden av å være fri for sporing eller offentlig overvåking.
_____ 5. Internettleverandør, som logger trafikken din med mindre den er kryptert.
_____ 6. Innkapsling av datapakker i en annen pakke for sikker overføring.
_____ 7. En ekstern datamaskin som ruter trafikken din og skjuler IP-adressen din.
_____ 8. Den maksimale datahastigheten for overføring over en tilkobling.

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. EENULRTINGN
2. DDBÅBEEDRN
3. EGKRENGOKL OIB
4. NRONSEVPER
5. OORLKTPLO
6. EVSRRE
7. BRNMURNA
8. TEDERAERNV TØNL

Bonusaktivitet: Tenk raskt

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

1	Ting en IP-adresse kan avsløre			
2	Myter om VPN-er			
3	Ting som reiser over internett			
4	Løfter en god VPN-leverandør gir			
5	Hemmeligheter du ville kryptert			
6	Ting en VPN ikke kan beskytte deg mot			
7	Måter å gjenkjenne et falskt Wi-Fi-nettverk på			
8	Ord knyttet til personvern			
9	Enheter som kan bruke en VPN			
10	Ting som skjer når du trykker «Koble til»			
11	Steder der du ville brukt en VPN			
12	Grunner til å bruke en VPN på reise			
13	Ting i virkeligheten som ligner på en tunnel			
14	Ord fra dette arbeidsarket du vil huske			
15	Ord for å forklare en VPN for et barn			

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. Der er det et usikret offentlig nettverk som heter «Free_Wi-Fi_No_Password». Jeg vil logge inn på skole-e-posten min og levere oppgaven min, men jeg er bekymret for hackere. Hva er risikoen ved å bruke dette nettverket uten en VPN, og hvordan sikrer en VPN dataene mine?»

ALEX (REISENDE STUDENT)

👩‍💻 «Å nei! Jeg reiser i utlandet i forbindelse med et prosjekt og prøver å se en biologidokumentar som ligger på en server i hjemlandet mitt. Men nettstedet sier «Denne videoen er ikke tilgjengelig der du befinner deg nå.» Hvorfor er jeg blokkert, og hvordan kan en VPN hjelpe meg å se den?»

Kontrollpunkt 9: Knekk chifferet

En VPN krypterer trafikken din for å sikre den. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen om cybersikkerhet ved å skrive de tilhørende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Æ=27 Ø=28 Å=29

2	5	19	11	25	20	20		16	5	18	19	15	14	22	5	18	14	5	20
4	9	20	20		13	5	4		5	14		19	9	11	11	5	18		
					20	21	14	14	5	12									

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: Hvorfor bør jeg bruke en VPN?

En VPN beskytter ditt digitale personvern, sikrer tilkoblingen din på offentlige Wi-Fi-nettverk (som kafeer eller flyplasser), kan redusere aktivitetsbasert struping når internettleverandøren ikke kan identifisere typen kryptert trafikk, omgår geografiske begrensninger for å få tilgang til globalt innhold og bidrar til å sikre ressurser for fjernarbeid.

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 det lovlig å bruke en VPN?

Bruk av VPN er lovlig i mange land, men noen jurisdiksjoner begrenser, regulerer eller blokkerer VPN-tjenester. Brukere bør kontrollere gjeldende lokale lover før bruk. For mer informasjon, se veiledningene om lovlighet på VPN.com.

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 VPN?

Gratis VPN-er kan være basert på reklame, begrensede funksjoner, bruksanalyse, datagrenser eller andre inntektsmodeller. Brukere bør gå gjennom leverandørens personvernerklæring, eierskap, revisjoner og forretningsmodell før bruk.

Q7: Hva er en policy om ingen logging («no-logs»)?

En retningslinje om ingen logging beskriver hvilke aktivitets- og tilkoblingsdata en leverandør sier at den ikke oppbevarer. Det nøyaktige omfanget varierer, så leserne bør gjennomgå retningslinjen og funnene fra uavhengige revisjoner.

Q8: Hvordan velger jeg den beste VPN-en?

Se etter revisjonsgodkjente policyer om ingen logging, sterke protokoller (WireGuard, OpenVPN), sikre serverplasseringer, høy hastighet, servere som kun bruker RAM, en kill switch-funksjon og jurisdiksjon utenfor etterretningsallianser (som 5/9/14 Eyes).

Q9: Kan jeg bruke en VPN på telefonen og smart-TV-en min?

Ja. Moderne VPN-leverandører tilbyr egne apper for iOS, Android, macOS, Windows, Linux og smart-TV-er, i tillegg til ruteroppsett som beskytter alle enhetene i hjemmenettverket ditt.

Q10: Hva er en Kill Switch?

En kill switch er en sikkerhetsfunksjon som automatisk kobler enheten din fra internett hvis VPN-tilkoblingen faller ut. Dette hindrer at ukrypterte data eller den virkelige IP-adressen din lekker ut.

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

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

Q1: Hva er forskjellen mellom WireGuard, OpenVPN og IKEv2?

WireGuard er en moderne, lettvekts protokoll (bare ca. 4000 kodelinjer) som gir høy hastighet og raske tilkoblingstider. OpenVPN er en svært sikker, velprøvd protokoll med åpen kildekode. IKEv2 er utmerket for mobile enheter fordi den kan koble til igjen raskt når du bytter nettverk. [4]

Q2: Hva er dobbel VPN eller Multi-Hop-ruting?

Multi-hop ruter trafikken din gjennom to eller flere VPN-servere i rekkefølge. Dette gir et ekstra lag med kryptering og bidrar til å holde den virkelige IP-adressen din skjult for den andre serveren hvis én server blir kompromittert.

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 servere som kun bruker RAM, og hvorfor er de viktige?

Tradisjonelle servere skriver data til harddisker, som kan beslaglegges eller kompromitteres. Servere kun med RAM (diskløse) kjører helt i flyktig minne (RAM). Når serveren startes på nytt eller slås av, slettes data i minnet.

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: Hvordan fungerer Forward Secrecy (Perfect Forward Secrecy)?

PFS sørger for at det genereres en unik, midlertidig krypteringsnøkkel for hver eneste økt. Selv om en privat nøkkel skulle bli kompromittert i fremtiden, kan den ikke brukes til å dekryptere tidligere eller fremtidige økter, fordi de brukte uavhengige nøkler.

Q8: Hva er alliansene 5/9/14 Eyes, og hvorfor bør jeg bry meg?

Jurisdiksjon kan påvirke den juridiske prosessen en leverandør kan møte, men den praktiske personvernrisikoen avhenger også av hvilke data leverandøren beholder, den tekniske arkitekturen, eierskapet, åpenhetsrapportering og revisjonshistorikken.

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 VPN omgå struping av internett fra internettleverandøren?

Noen ganger. En VPN kan hjelpe når en internettleverandør selektivt bremser identifiserbare aktiviteter, men den løser ikke overbelastning, datagrenser, hastighetsgrenser på kontonivå eller dårlig nettverkskvalitet.

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. FØRSTE VPN-PROTOKOLL

PPTP (Point-to-Point Tunneling Protocol) ble utviklet av en leverandørgruppe som blant annet omfattet Microsoft, og ble publisert som RFC 2637 i juli 1999 for å støtte VPN-er for ekstern tilgang. [6]

2. MARKEDSVERDSETTELSE

Det globale VPN-markedet har vokst raskt, drevet av økende behov for fjernarbeid og krav til bedriftssikkerhet.

3. WIREGUARD-REVOLUSJONEN

WireGuard har en svært strømlinjeformet kodebase som er utformet for effektivitet, noe som gjør det enklere å gjennomgå for sikkerhetssårbarheter enn tradisjonelle protokoller. [4]

4. STRENGE REVISJONSSTANDARDER

Ledende VPN-leverandører engasjerer eksterne revisorer (som Cure53 eller PwC) til å utføre uavhengige kodegjennomganger og verifisere at de ikke logger brukeraktivitet.

5. OPPRINNELSEN TIL 5 EYES-ALLIANSEN

Five Eyes-alliansen vokste ut av UKUSA-avtalen fra 1946 om signaletterretning mellom USA og Storbritannia, senere med Canada, Australia og New Zealand som medlemmer.

6. DYP PAKKEINSPEKSJON

Deep Packet Inspection (DPI) undersøker pakkeinnhold og trafikkmønstre, ikke bare overskrifter, og noen brannmurer bruker det til å oppdage og blokkere vanlige VPN-protokoller.

7. BEDRIFTSBRUK

En stor andel av ansatte i virksomheter globalt bruker sikre VPN-er for å logge inn på interne databaser, noe som gjør det til en sentral sikkerhetsstandard.

8. DESENTRALISERTE VPN-ER

Desentraliserte VPN-er (dVPN-er) fordeler trafikken over et nettverk av noder drevet av likemenn (peers), noe som reduserer avhengigheten av én enkelt sentralisert leverandør.

9. ANONYMITET MED TOR MOT VPN

En VPN tunnelerer trafikk gjennom én enkelt leverandør, mens Tor (The Onion Router) sender trafikk gjennom tre frivillige reléer (inngang, mellomledd og utgang), slik at ingen enkelt reléoperatør kjenner begge endene.

10. KOSTNADER VED DATABRUDD

Å bruke en sikker tilgangsmodell med nulltillit sammen med en VPN hjelper organisasjoner med å beskytte immaterielle rettigheter og redusere de økonomiske konsekvensene av datainnbrudd.

Tekniske referanser og kilder

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

FAGLIGE REFERANSER OG BRANSJEREFERANSER

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

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

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

[4] 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/

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

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Fasit: Arbeidsark om hva en VPN er

1 **Hovedfunksjon** PROTOKOLLER — **Riktig svar: B**

MERKNAD TIL LÆREREN

En VPNs hovedoppgave er å etablere en kryptert tunnel som skjermer nyttelastdata i pakker og maskerer brukerens offentlige IP-adresse.

2 **Nettverkstunnelering** LATENS — **Riktig svar: D**

MERKNAD TIL LÆREREN

Tunnelprotokoller kapsler inn opprinnelige datapakker i ytre bærerpakker slik at de kan passere trygt gjennom offentlige nettverk.

3 **Spørsmål 3** — **Riktig svar: B**

MERKNAD TIL LÆREREN

Hvilken krypteringsstandard brukes mye til å beskytte VPN-trafikk? → Moderne AES-256-standard

4 **Krypterte komponenter** RUTINGKONTROLLER — **Riktig svar: C**

MERKNAD TIL LÆREREN

En VPN krypterer hele nyttelastsegmentet i IP-datapakker og holder innholdet i overføringen konfidensielt.

5 **Spørsmål 5** — **Riktig svar: A**

MERKNAD TIL LÆREREN

Kryptering bruker en algoritme og en nøkkel for å gjøre klartekst om til uleselig chiffertekst.

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Blokkering av avlytting** IP-MASKERING — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Krypterte tunneler sørger for at pakkenyttelastene forblir uleselige for aktører som avskjærer data på lokale Wi-Fi-nettverk.

7 **Maskinvareendringer** HASTIGHETER — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

VPN-er er programvarebaserte nettverkstunneler og endrer ikke fysisk maskinvaren i gateway-ruteren din.

8 **Tunneling av pakker** SNIFFINGRISIKO — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Tunneling fungerer ved å pakke opprinnelige nettverkspakker inn i transporthoder under transport.

9 **Symmetriske nøkler** BRANNMURER — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Symmetrisk kryptografi bruker én delt nøkkel både til å kryptere og dekryptere nettverksstrømmer.

10 **Immunitet mot strømbrudd** INGEN LOGGING — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

En VPN krypterer bare aktive tilkoblingssignaler; den kan ikke forhindre tjenestebrudd som skyldes lokale strømbrudd.

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

H 1. Tunnelering	E 2. Protokoll	G 3. Båndbredde	A 4. Server
C 5. Geoblokkering	D 6. Brannmur	F 7. Personvern	B 8. Internettleverandør

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 TUNNELERING	2 BÅNDBREDDE	3 GEOBLOKKERING	4 PROTOKOLL
5 BRANNMUR	6 SERVER		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 B – PROTOKOLL	2 E – GEOBLOKKERING	3 F – BRANNMUR	4 G – PERSONVERN
5 H – NETTLEVERANDØR	6 A – TUNNELERING	7 D – SERVER	8 C – BÅNDBREDDE

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare Tunnelering, Protokoll og Båndbredde med egne ord og gi et eksempel på hvert.

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

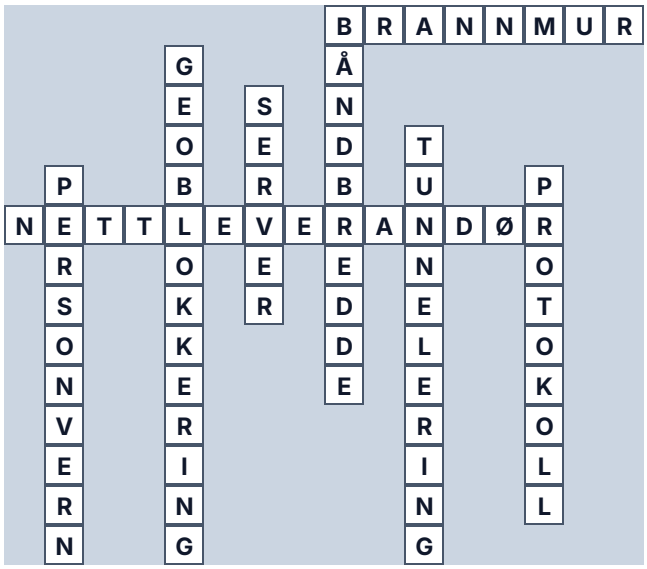
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

1 vannrett: BRANNMUR Et sikkerhetssystem som overvåker og blokkerer uautorisert trafikk (8 bokstaver)

7 vannrett: NETTLEVERANDØR Internettleverandør, som logger trafikken din med mindre den er kryptert (14 bokstaver)

LODDRETT

1 loddrett: BÅNDBREDDE Den maksimale datahastigheten for overføring over en tilkobling (10 bokstaver)

2 loddrett: GEOBLOKKERING En begrensning som hindrer nettilgang basert på fysisk plassering (13 bokstaver)

3 loddrett: SERVER En ekstern datamaskin som ruter trafikken din og skjuler IP-adressen din (6 bokstaver)

4 loddrett: TUNNELERING Innkapsling av datapakker i en annen pakke for sikker overføring (11 bokstaver)

5 loddrett: PERSONVERN Tilstanden av å være fri for sporing eller offentlig overvåking (10 bokstaver)

6 loddrett: PROTOKOLL Et sett regler som bestemmer hvordan data overføres over nettverket (9 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1.	E E N U L R T I N G N	TUNNELERING	5.	O O R L K T P L O	PROTOKOLL
2.	D D B Å B E E D R N	BÅNDBREDDE	6.	E V S R R E	SERVER
3.	E G K R E N G O K L O I B	GEOBLOKKERING	7.	B R N M U R N A	BRANNMUR
4.	N R O N S E V P E R	PERSONVERN	8.	T E D E R A E R N V T Ø N L	NETTLEVERANDØR

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"BESKYTT PERSONVERNET DITT MED EN SIKKER TUNNEL"

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.
- VPN-beskyttelse: Krypterer nyttelastene i nettverkspakkene, slik at avlyttet tunneltrafikk blir uleselig for passive snusere i det lokale nettverket når VPN-en er riktig konfigurert.

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.
- Slik hjelper VPN: Han maskerer sin virkelige posisjon ved å rute trafikken gjennom en server i hjemlandet sitt. Nettstedet ser en IP-adresse fra hjemlandet, og han får tilgang.