Navn: _____ Dato: _____ Poeng: _____

Guide til den mest sikre VPN-en

Teknisk analyse av VPN-design med høy sikkerhet, servere med flyktig minne som bare bruker RAM, Zero Trust-tilgangssikkerhet, forsvar mot DNS-lekkasjer med privat kryptert DNS og reviderte WireGuard-konfigurasjoner.

LÆRINGSOVERSIKT: GUIDE TIL DEN MEST SIKRE VPN-EN

ELEV
STUDENTSTATUS
Spor for nettverksforsvarere

SIKKER
TILKOBLINGSSTATUS
Beskytte datapakker

AKTIV
LEKKASJEBESKYTTELSE
DNS- og IPv6-lekkasjebeskyttelse

Velkommen! Dette aktivitetsheftet veileder deg gjennom de tekniske standardene for svært sikre VPN-er. Du utforsker serverutstyr som bare bruker RAM, Zero Trust-tilgangssikkerhet, private krypterte DNS-resolvere og reviderte WireGuard-konfigurasjoner.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk VPN- og nettverkssikkerhetskonfigurasjoner.**
- [ ] **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 veiledning om de beste VPN-ene

URL: https://www.vpn.com/no/vpn/mest-sikre-vpn/

Din læringsveiledning for den sikreste VPN-en

- Analyser den tekniske arkitekturen og krypteringsstandardene for Most Secure VPN Guide.
- Konfigurer klientinnstillinger for å hindre lekkasjer av IP-, DNS- og WebRTC-trafikk.
- Sammenlign proprietære tunnelprotokoller med standardimplementeringer.

INSTRUKSJONER FOR GUIDE TIL DEN MEST SIKRE VPN-EN

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på servermaskinvare som kun bruker RAM, og Zero Trust-systemer. Avslutt med bonusaktiviteten Tenk raskt.

INFRASTRUKTURER SOM KUN BRUKER RAM OG ZERO TRUST-NETTVERK (INNLEDNING)

En virkelig sikker VPN bygger på et Zero Trust-rammeverk, servere med bare RAM for å hindre at beslagleggelse av disker avslører logger, private krypterte DNS-oppløsere og reviderte protokoller som WireGuard. Disse kontrollene i kombinasjon beskytter digitale verdier av høy verdi mot trusler om avlytting.

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

Kontrollpunkt 1: Flervalgsutfordring

1. **1. Hvilken arkitektur er avgjørende for å sikre høyest mulig sikkerhet i moderne VPN-servere?**
   - A) Serverinfrastruktur med bare RAM
   - B) Diskbasert lagring
   - C) Dynamisk DNS-ruting
   - D) Aktivering av portvideresending

2. **2. Hvilken protokoll anbefales bredt for de sikreste og mest moderne VPN-konfigurasjonene?**
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. **3. Hvilket sikkerhetsrammeverk krever at hver eneste tilkobling kontrolleres kontinuerlig uten unntak?**
   - A) Zero Trust-arkitektur
   - B) Perimeterbrannmurer
   - C) Dynamisk ruting
   - D) Delte hemmelige nøkler

4. **4. Hva er hovedrollen til DNS-lekkasjebeskyttelse i en VPN-klient?**
   - A) Rute alle DNS-forespørsler gjennom private krypterte oppløsere
   - B) Obfuskere IP-pakker
   - C) Hurtigbufre DNS-spørringer lokalt
   - D) Deaktiver navneservere

5. **5. Hvordan øker multi-hop-ruting den samlede sikkerheten i en VPN-tunnel?**
   - A) Ruter data gjennom to separate servere i serie
   - B) Øker komprimeringshastigheten
   - C) Krypterer data med chiffer med lav sikkerhet
   - D) Omgår brannmurer

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Servere som kun bruker RAM lagrer loggfiler i flyktig minne, som tømmes ved omstart.

○ Sant ○ Usant

7 Spørsmål 7

7. WireGuard bruker moderne kryptografiske algoritmer som er mindre utsatt for hastighetsflaskehalser.

○ Sant ○ Usant

8 Spørsmål 8

8. En VPN-kill switch fungerer ved å blokkere all nettverkstrafikk hvis tunnelen faller ut.

○ Sant ○ Usant

9 Spørsmål 9

9. Uavhengige revisjoner fra tredjeparter er irrelevante for å verifisere sikkerhetsforpliktelser.

○ Sant ○ Usant

10 Spørsmål 10

10. Zero Trust-modeller forutsetter at alle interne nettverkstilkoblinger er sikre som standard.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Administratorer håndhever sikkerhet ved å ta i bruk et strengt _____ -rammeverk.
2. Å rute pakker gjennom flere inngangspunkter krever en sikker _____ -konfigurasjon.
3. For å hindre datalekkasjer fra stjålne disker bruker vi en arkitektur basert på _____ .
4. Kapring fra internettleverandøren motvirkes ved å konfigurere innebygde funksjoner for _____ .
5. For å blokkere trafikk ved tilkoblingsfeil aktiverer du _____ -mekanismen.
6. For å minimere lagrede databaselogger bør du velge en leverandør med et fullt _____ .

ORDBANK

DNS-BESKYTTELSE KILL SWITCH KRYPTERING MULTI-HOP NULLTILLIT PROTOKOLL RAM-SERVER REVIDERT OPPSETT

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble VPN- og nettverksbegreper

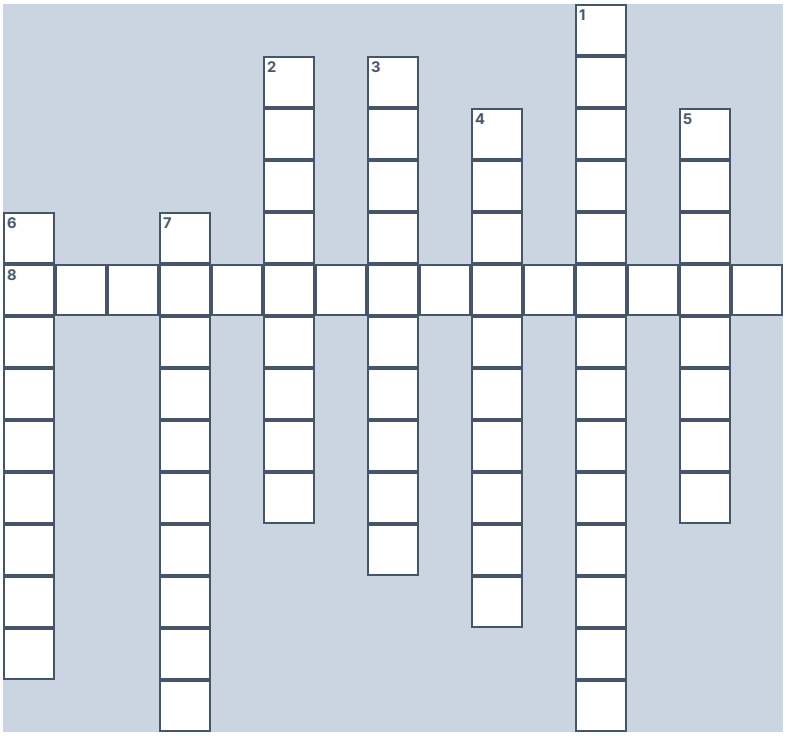
KOBLE DEFINISJONER

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

☐	1. Zero Trust	A	Uavhengig inspisert oppsett som bekrefter at ingen logger lagres.
☐	2. Multi-hop	B	Kryptografisk omblanding av datanyttelast for å sikre overføringen.
☐	3. Server som kun bruker RAM	C	Sikkerhetsrammeverk som krever kontinuerlig autentisering av alle brukere.
☐	4. DNS-beskyttelse	D	Sett med tekniske regler som bestemmer hvordan data pakkes og sendes.
☐	5. Kill Switch	E	Kaskadert VPN-ruting som kobler to servernoder i kjede.
☐	6. Revidert system	F	Serverarkitektur som bruker flyktig minne til å lagre datanyttelast.
☐	7. Kryptering	G	Håndheve private DNS-forespørsler for å beskytte oppslag hos navnetjenere.
☐	8. Protokoll	H	Feilsikker mekanisme som blokkerer trafikk hvis VPN-en feiler.

Kontrollpunkt 5: Kryssord

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



VANNRETT

8. Uavhengig inspisert oppsett som bekrefter at ingen logger lagres (15)

LODDRETT

1. Håndheving av private DNS-forespørsler for å beskytte navneserveroppslag (14)

2. Serverarkitektur som bruker flyktig minne til å lagre datanyttelast (9)

3. Sikkerhetsrammeverk som krever kontinuerlig autentisering av alle brukere (10)

4. Kryptografisk sammenblanding av datanyttelast for å sikre dataoverføring (10)

5. Kaskadert VPN-ruting som kobler to servernoder sammen (8)

6. Sett med tekniske regler som bestemmer hvordan data pakkes og sendes (9)

7. Sikkerhetsmekanisme som blokkerer trafikk hvis VPN-en svikter (10)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

8 vannrett: Uavhengig inspisert oppsett som bekrefter at ingen logger lagres (15 bokstaver):

LODDRETT

1 loddrett: Håndheving av private DNS-forespørsler for å beskytte navneserveroppslag (14 bokstaver):

2 loddrett: Serverarkitektur som bruker flyktig minne til å lagre datanyttelast (9 bokstaver):

3 loddrett: Sikkerhetsrammeverk som krever kontinuerlig autentisering av alle brukere (10 bokstaver):

4 loddrett: Kryptografisk sammenblanding av datanyttelast for å sikre dataoverføring (10 bokstaver):

5 loddrett: Kaskadert VPN-ruting som kobler to servernoder sammen (8 bokstaver):

6 loddrett: Sett med tekniske regler som bestemmer hvordan data pakkes og sendes (9 bokstaver):

7 loddrett: Sikkerhetsmekanisme som blokkerer trafikk hvis VPN-en svikter (10 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

NULLTILLIT MULTIHOP RAMSERVER DNSBESKYTTELSE KILLSWITCH
REVIDERTOPPSETT KRYPTERING PROTOKOLL

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. NULLTILLIT
B. MULTIHOP
C. RAMSERVER
D. DNSBESKYTTELSE
E. KILLSWITCH
F. REVIDERTOPPSETT
G. KRYPTERING
H. PROTOKOLL

DEFINISJONER OG TILHØRENDE FELT
1. Sikkerhetsmekanisme som blokkerer trafikk hvis VPN-en svikter.
2. Håndheving av private DNS-forespørsler for å beskytte navneserveroppslag.
3. Kaskadert VPN-ruting som kobler to servernoder sammen.
4. Sett med tekniske regler som bestemmer hvordan data pakkes og sendes.
5. Kryptografisk sammenblanding av datanyttelast for å sikre dataoverføring.
6. Serverarkitektur som bruker flyktig minne til å lagre datanyttelast.
7. Uavhengig inspisert oppsett som bekrefter at ingen logger lagres.
8. Sikkerhetsrammeverk som krever kontinuerlig autentisering av alle brukere.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper om virtuelle private nettverk (VPN). Skriv svarene dine i svarboksene.

1. ILITUNLTLL
2. RRESARVEM
3. KWCIISHLTL
4. ENTGPIRKRY
5. IHUPTMOL
6. SKEESLYSTD NTEB
7. PPRORSEVTEE TITD
8. LOLPTRKOO

Bonusaktivitet: Tenk raskt

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

1	Låser eller nøkler du bruker hver dag			
2	Ting en VPN kan skjule			
3	Ting som gjør en VPN sikker			
4	Myter om VPN-er			
5	Grunner til å bruke en VPN på reise			
6	Trygge steder i den virkelige verden			
7	Ord som betyr «beskyttet»			
8	Løfter en god VPN-leverandør gir			
9	Ord knyttet til personvern			
10	Typer revisjon eller inspeksjon			
11	Ord fra dette arbeidsarket du vil huske			
12	Ting en hacker vil stjele			
13	Måter å gjenkjenne et falskt Wi-Fi-nettverk på			
14	Steder der du ville brukt en VPN			
15	Ting internettleverandøren din kan se			

Kontrollpunkt 8: Casestudier om VPN og nettverk

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

CASESTUDIE 1: HERDING AV BEDRIFTENS INFRASTRUKTUR



Scenario: En bedriftsbank utformer ekstern tilgangstopologi på nytt. Den krever en Zero Trust-arkitektur som kobler alle klientenheter til sikre servere.

Diskusjonsspørsmål: Hva er den viktigste fordelen med nettverksmikrosegmentering i en Zero Trust VPN-modell?

CASESTUDIE 2: BESKYTTELSE PÅ RAM-ONLY-SERVERE



Scenario: En sikkerhetsfokusert VPN-leverandør oppgraderer serverne sine for å hindre at fysisk beslagleggelse av servere eksponerer brukernes loghistorikk.

Diskusjonsspørsmål: Forklar hvordan maskinvarekonfigurasjoner med kun RAM hindrer forensisk datauthenting ved fysisk beslagleggelse av servere.

Kontrollpunkt 9: Knekk chifferet

En nettverksingeniør sikrer rutingkanaler og klienttunneler. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen 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

19	9	11	18	5		22	16	14		2	5	19	11	25	20	20	5	18
4	9	7	9	20	1	12	5		22	5	18	4	9	5	18			

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 om virtuelle private nettverk (VPN-er) og tunnelering.

Q1: Hva gjør en VPN «mest sikker»?

En kombinasjon av Zero Trust, servere med bare RAM og reviderte protokoller.

Q2: Hva er RAM-only-servere?

Servere som kjører i flyktig minne og er utformet for ikke å lagre logger på disk.

Q3: Hva er en Zero Trust-VPN?

Et rammeverk som kontinuerlig verifiserer hver tilgangsforespørsel og tilkobling.

Q4: Hvorfor anses WireGuard som sikker?

Den har en liten kodebase som er lett å revidere, og bruker moderne chiffer.

Q5: Hvordan forhindrer sikre VPN-er DNS-lekkasjer?

Ved å rute alle spørringer gjennom private, krypterte DNS-løsere.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del B)

Gå gjennom de vanligste spørsmålene og svarene om virtuelle private nettverk (VPN-er) og tunnelering.

Q6: Krever en sikker VPN revisjoner?

Ja, uavhengige revisjoner verifiserer påstandene om null logging og kodesikkerheten.

Q7: Hvilken rolle spiller en kill switch?

Den stanser umiddelbart nettverkstrafikken hvis VPN-tilkoblingen faller ut.

Q8: Hvilken kryptering brukes i sikre VPN-er?

AES-256 og ChaCha20 er bransjestandardene for kryptering.

Q9: Er Multi-Hop-ruting sikker?

Ja, den lenker sammen to eller flere servere for å hindre trafikkanalyse.

Q10: Hvordan hjelper offshore-jurisdiksjon?

Den kan begrense hvilke lover som gjelder, men gir ingen absolutt immunitet.

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

Utforsk avanserte tekniske sider ved VPN-tunnelprotokoller, integrering av mobilklienter og utrulling i bedrifter.

Q1: Hvordan forhindrer servere som bare bruker RAM risikoen for beslag av data?

Fordi de kjører i RAM, sletter det å trekke ut kontakten dataene som ligger i minnet.

Q2: Hvordan erstatter Zero Trust standard perimetersikkerhet?

Den behandler alle klienter som fiendtlige og krever kontinuerlig autentisering.

Q3: Hva gjør at WireGuard-kodebasen er enklere å revidere?

Linux-koden består av under 4 000 linjer, langt mindre enn typiske VPN-stabler. [4]

Q4: Hvordan beskytter DNSSEC DNS-spørringer?

Den signerer DNS-poster slik at løsere kan oppdage forfalskede eller manipulerte svar.

Q5: Hvordan gjør Multi-Hop trafikkkorrelasjon vanskeligere?

Ved å skille innkommende og utgående IP-adresser på tvers av ulike leverandører av hosting.

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

Utforsk avanserte tekniske sider ved VPN-tunnelprotokoller, integrering av mobilklienter og utrulling i bedrifter.

Q6: Hvorfor er Five Eyes-jurisdiksjoner risikable for VPN-er?

Medlemsland deler etterretning og kan bruke rettslige pålegg for å kreve ut brukerdata.

Q7: Hvordan implementeres en kill switch på kjernenivå?

Den bruker systemets brannmurregler (som iptables eller WFP) til å blokkere utgående trafikk.

Q8: Hva er forward secrecy i VPN-håndtrykk?

Den genererer unike øktnøkler slik at tidligere økter ikke kan dekrypteres.

Q9: Hvordan reduserer sikre VPN-er WebRTC-lekkasjer?

Ved å blokkere WebRTC-forespørsler eller rute dem gjennom tunnelen.

Q10: Hvordan sikrer uavhengige revisjoner etterlevelse av personvern?

Revisorer utfører penetrasjonstesting og inspiserer serverkonfigurasjoner.

Del 11: 10 fakta om VPN fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om VPN-krypteringshastigheter, protokollrevisjoner, mobiltilkobling og fjernarbeid i bedrifter.

1. VPN-INNSIKT

Servere som kun bruker RAM laster operativsystemet inn i minnet ved oppstart, slik at ingenting blir liggende igjen på disk etter en omstart.

2. VPN-INNSIKT

WireGuard bruker Noise-rammeverket med Curve25519, ChaCha20, Poly1305, BLAKE2s og HKDF. [3]

3. VPN-INNSIKT

Zero Trust gir tilgang per ressurs og gir ingen implisitt tillit basert på nettverksplassering (NIST SP 800-207). [1]

4. VPN-INNSIKT

Etterretningsalliansen Five Eyes omfatter USA, Storbritannia, Canada, Australia og New Zealand.

5. VPN-INNSIKT

WebRTC-lekkasjer oppstår når nettlesere avslører klientens ekte offentlige IP-adresse gjennom STUN-forespørsler.

6. VPN-INNSIKT

Perfect forward secrecy (PFS) sørger for at kompromittering av en langvarig nøkkel ikke avslører tidligere øktnøkler. [3]

7. VPN-INNSIKT

Cure53, et sikkerhetsselskap i Berlin, har publisert revisjoner av flere VPN-leverandører.

8. VPN-INNSIKT

DNS-lekkasjer oppstår når DNS-forespørsler omgår VPN-tunnelen og går til den lokale internettleverandørens navnetjenere.

9. VPN-INNSIKT

Flyktige RAM-brikker trenger konstant strømforsyning for å beholde data, og mister innholdet når strømmen slås av.

10. VPN-INNSIKT

Zero Trust-systemer for bedrifter håndhever kontroller av enhetens sikkerhetstilstand før de tillater tilkobling til sikre ressurser. [1]

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale tekniske standarder, spesifikasjoner og regelverk.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Fasit: Kontrollpunkt 1 – flervalg

1 **Server som kun bruker RAM** KUN RAM

Riktig svar: A

MERKNAD TIL LÆREREN

Servere som kun bruker RAM lagrer ingen logger på disk og tømmer data ved omstart.

2 **Spørsmål 2**

Riktig svar: A

MERKNAD TIL LÆREREN

WireGuard kombinerer en liten kodebase som kan revideres med moderne chiffer.

3 **Zero Trust-modellen** ZERO TRUST

Riktig svar: A

MERKNAD TIL LÆREREN

Zero Trust-modeller verifiserer kontinuerlig at enheter oppfyller kravene før tilgang gis.

4 **DNS-beskyttelse** DNS-BESKYTTELSE

Riktig svar: A

MERKNAD TIL LÆREREN

DNS-lekkasjebeskyttelse ruter oppslagsforespørsler gjennom private resolvere.

5 **Multi-hop-tunneler** MULTI-HOP

Riktig svar: A

MERKNAD TIL LÆREREN

Multi-hop-ruting kjeder to separate servernoder i serie.

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Server som kun bruker RAM** KUN RAM — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Servermaskinvare som kun bruker RAM skriver ingen data til disk og tømmes ved omstart.

7 **WireGuard-hastighet** WIREGUARD — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

WireGuard bruker moderne kryptografi som unngår flaskehalser i prosesseringen.

8 **Kill Switch** SIKKERHETSBRYTER — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

En kill switch blokkerer all trafikk hvis VPN-tilkoblingen faller ut.

9 **Revisjoner fra tredjepart** REVISJONER ER VIKTIGE — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Revisjoner fra tredjepart er avgjørende for å verifisere selskapers påstander om personvern.

10 **Spørsmål 10** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Zero Trust gir ingen implisitt tillit basert på nettverksplassering. [1]

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

C 1. Zero Trust	E 2. Multi-hop	F 3. Server som kun bruker RAM	G 4. DNS-beskyttelse
H 5. Kill Switch	A 6. Revidert system	B 7. Kryptering	D 8. Protokoll

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 NULLTILLIT	2 MULTI-HOP	3 RAM-SERVER	4 DNS-BESKYTTELSE
5 KILL SWITCH	6 REVIDERT OPPSETT		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 E – KILLSWITCH	2 D – DNSBESKYTTELSE	3 B – MULTIHOP	4 H – PROTOKOLL
5 G – KRYPTERING	6 C – RAMSERVER	7 F – REVIDERTOPPSETT	8 A – NULLTILLIT

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare Zero Trust, Multi-hop og Server som kun bruker RAM med egne ord og gi et eksempel på hvert.

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

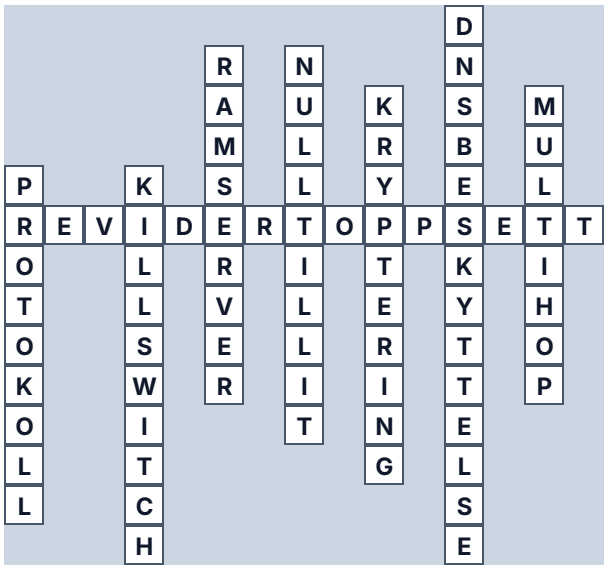
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

8 vannrett: REVIDERTOPPSETT Uavhengig inspisert oppsett som bekrefter at ingen logger lagres (15 bokstaver)

LODDRETT

1 loddrett: DNSBESKYTTELSE Håndheving av private DNS-forespørsler for å beskytte navneserveroppslag (14 bokstaver)

2 loddrett: RAMSERVER Serverarkitektur som bruker flyktig minne til å lagre datanyttelast (9 bokstaver)

3 loddrett: NULLTILLIT Sikkerhetsrammeverk som krever kontinuerlig autentisering av alle brukere (10 bokstaver)

4 loddrett: KRYPTERING Kryptografisk sammenblanding av datanyttelast for å sikre dataoverføring (10 bokstaver)

5 loddrett: MULTIHOP Kaskadert VPN-ruting som kobler to servernoder sammen (8 bokstaver)

6 loddrett: PROTOKOLL Sett med tekniske regler som bestemmer hvordan data pakkes og sendes (9 bokstaver)

7 loddrett: KILLSWITCH Sikkerhetsmekanisme som blokkerer trafikk hvis VPN-en svikter (10 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. I L I T U N L T L L — **NULLTILLIT**
2. R R E S A R V E M — **RAMSERVER**
3. K W C I I S H L T L — **KILLSWITCH**
4. E N T G P I R K R Y — **KRYPTERING**
5. I H U P T M O L — **MULTIHOP**
6. S K E E S L Y S T D N T E B — **DNSBESKYTTELSE**
7. P P R O R S E V T E E T I T D — **REVIDERTOPPSETT**
8. L O L P T R K O O — **PROTOKOLL**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"SIKRE VPN BESKYTTER DIGITALE VERDIER"

Fasit til casestudiene

A CASESTUDIE 1: HERDING AV BEDRIFTENS INFRASTRUKTUR

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En bedriftsbank utformer topologien for ekstern tilgang på nytt. Den krever en zero trust-arkitektur som kobler alle klientenheter til sikre servere.
- Anbefalt strategi og løsning: Vurderingsveiledning: Forklar at mikrosegmentering begrenser tilgangen til bestemte ressurser og hindrer lateral trusselbevegelse hvis en enhet blir kompromittert.

B CASESTUDIE 2: BESKYTTELSE PÅ RAM-ONLY-SERVERE

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En sikkerhetsfokusert VPN-leverandør oppgraderer serverne sine for å hindre at fysisk beslagleggelse av servere avslører brukerloggers historikk.
- Anbefalt strategi og løsning: Vurderingsveiledning: Beskriv at RAM-only-servere ikke har fysisk disklagring. Strømbrudd sletter automatisk alle midlertidige data i flyktig minne.