Navn: _____ Dato: _____ Poeng: _____

Surfshark-sikkerhet

Gjennomgang av Surfsharks sikkerhetsfunksjoner, inkludert annonseblokkeringen CleanWeb, dynamisk ruting med MultiHop, Nexus SDN-arkitektur, en serverflåte som bare bruker RAM og Camouflage-modus.

LÆRINGSOVERSIKT: SURFSHARKS SIKKERHET

ELEV
STUDENTSTATUS
Spor for nettverksforsvarere

SIKKER
TILKOBLINGSSTATUS
Beskytte datapakker

AKTIV
LEKKASJEBESKYTTELSE
DNS- og IPv6-lekkasjebeskyttelse

Velkommen! Dette aktivitetsheftet veileder deg gjennom Surfsharks sikkerhetsarkitektur. Du skal utforske servermaskinvare som bare bruker RAM, dynamisk IP-rotasjon i Nexus SDN, annonseblokkereren CleanWeb og MultiHop-ruting.

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/surfshark/sikkerhet/

Din læringsveiledning for Surfshark-sikkerhet

- Analyser den tekniske arkitekturen og konfigurasjonsreglene for Surfshark Security.
- Konfigurer klientinnstillinger for å hindre lekkasjer av IP-, DNS- og WebRTC-trafikk.
- Sammenlign egendefinerte priser, prøveperioder og ytelsesfunksjoner med standardmodeller.

INSTRUKSJONER FOR VEILEDNING OM SURFSHARKS SIKKERHET

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

SERVERPARK SOM KUN BRUKER RAM, NEXUS SDN OG CLEANWEB-ARKITEKTUR (INNLEDNING)

Surfshark beskytter brukernes personvern med en serverpark som bare bruker RAM, programvaredefinert nettverk i Nexus med IP Rotator, annonseblokkering med CleanWeb og krypteringsstier med Dynamic MultiHop.

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

Kontrollpunkt 1: Flervalgsutfordring

1. **1. Hva heter Surfsharks integrerte blokkering av annonser og skadevare?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Hvilken maskinvarearkitektur bruker Surfshark på alle serverne sine?**
   - A) Harddisker
   - B) 100 % kun RAM
   - C) Optisk lagring
   - D) Magnetbånd

3. **3. Hvilken funksjon ruter trafikk gjennom to ulike VPN-servere?**
   - A) Bypasser
   - B) MultiHop (dobbel VPN)
   - C) Nexus-nettverk
   - D) Statisk IP

4. **4. Hvilken obfuskeringsfunksjon skjuler VPN-trafikk som vanlige nettdata?**
   - A) Kill switch
   - B) Kamuflasjemodus
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. **5. Hva er funksjonen til verktøyet Surfshark Bypasser?**
   - A) Speed Booster
   - B) Delt tunnelering
   - C) Passordbehandler
   - D) DNS-resolver

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Servere som kun bruker RAM sletter alle driftsdata umiddelbart når serveren starter på nytt.

○ Sant ○ Usant

7 Spørsmål 7

7. Camouflage Mode hindrer internettleverandører i å oppdage at du bruker en VPN.

○ Sant ○ Usant

8 Spørsmål 8

8. CleanWeb 2.0 fungerer i nettleserutvidelser for å blokkere popup-vinduer for samtykke til informasjonskapsler.

○ Sant ○ Usant

9 Spørsmål 9

9. Surfshark lagrer midlertidige tidsstempler for tilkoblinger og logger over båndbreddebruk.

○ Sant ○ Usant

10 Spørsmål 10

10. Nexus-nettverket bytter jevnlig ut brukernes IP-adresser uten å koble fra.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Irriterende nettannonser, sporingsskript og nettfiskingslenker blokkeres av _____ -filtre.

2. Brukeraktivitet etterlater ingen rettsmedisinsk spor fordi serverne er _____ .

3. Å rute data gjennom to separate krypterte serverhopp oppnås med _____ -tunneler.

4. For å skjule VPN-bruk for internettleverandører aktiverer brukere _____ -modus.

5. Å la nettbankapplikasjoner omgå VPN-tunnelen styres av _____ -innstillinger.

6. Neste generasjons SDN-arkitektur som kobler serverparken sammen, er _____ -systemet.

ORDBANK

BYPASSER CAMOUFLAGE CLEANWEB KILL SWITCH MULTI-HOP NEXUS RAM-BASERTE ROTERENDE IP

Skriv svarene dine her:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Koble VPN- og nettverksbegreper

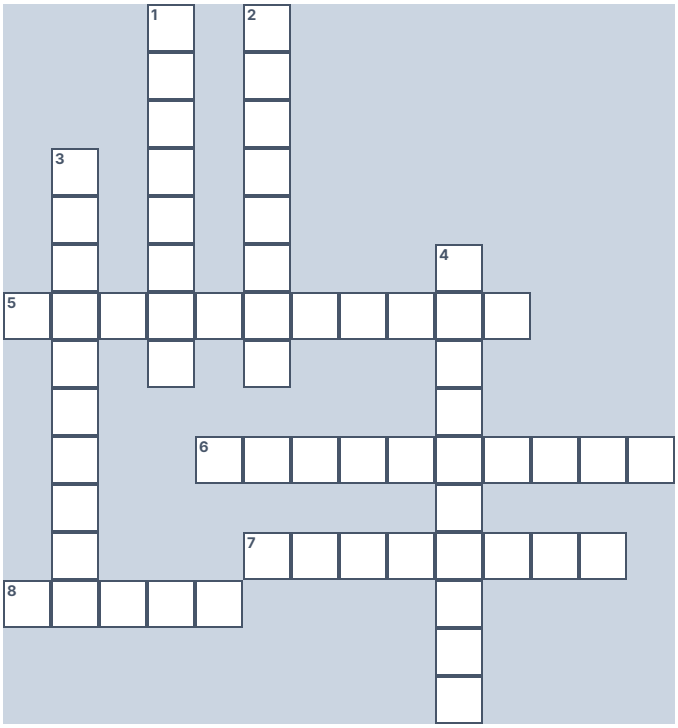
KOBLE DEFINISJONER

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

☐	1. CLEANWEB	A	En automatisk sikkerhetsfunksjon som blokkerer nettverkstrafikk når VPN-en faller ut.
☐	2. RAM-BASERTE	B	Split tunneling-funksjon som lar utvalgte applikasjoner omgå VPN-en.
☐	3. MULTI-HOP	C	Et avansert filter som blokkerer annonser, skadevare og samtykkebannere for infokapsler.
☐	4. CAMOUFLAGE	D	Servermaskinvare med flyktig minne som sletter alle data hver gang strømmen slås av og på.
☐	5. BYPASSER	E	En funksjon som jevnlig endrer din eksterne IP-adresse uten å avbryte tunneler.
☐	6. KILL SWITCH	F	Obfuskeringsteknologi som skjuler VPN-signaturer for å etterligne vanlig HTTPS-trafikk.
☐	7. NEXUS	G	En dobbel-VPN-rutingfunksjon som krypterer trafikk på tvers av to ulike servernoder.
☐	8. ROTERENDE	H	Et proprietært programvaredefinert nettverk som kobler alle servere sammen i ett samlet mesh-nettverk.

Kontrollpunkt 5: Kryssord

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



VANNRETT

5. En funksjon som jevnlig endrer din eksterne IP-adresse uten å avbryte tunneler (11)

6. Servermaskinvare med flyktig minne som sletter alle data ved hver strømsyklus (10)

7. En funksjon for dobbel VPN-ruting som krypterer trafikk over to separate servernoder (8)

8. Et proprietært programvaredefinert nettverk som kobler alle servere sammen til ett samlet mesh (5)

LODDRETT

1. Et avansert filter som blokkerer annonser, skadevare og bannere for samtykke til informasjonskapsler (8)

2. Split tunneling-funksjonalitet som lar utvalgte applikasjoner omgå VPN-en (8)

3. Tilsløringsteknologi som skjuler VPN-signaturer for å etterligne vanlig HTTPS-trafikk (10)

4. En automatisk sikkerhetsfunksjon som blokkerer nettverkstrafikk når VPN-en faller ut (10)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

5 vannrett: En funksjon som jevnlig endrer din eksterne IP-adresse uten å avbryte tunneler (11 bokstaver):

6 vannrett: Servermaskinvare med flyktig minne som sletter alle data ved hver strømsyklus (10 bokstaver):

7 vannrett: En funksjon for dobbel VPN-ruting som krypterer trafikk over to separate servernoder (8 bokstaver):

8 vannrett: Et proprietært programvaredefinert nettverk som kobler alle servere sammen til ett samlet mesh (5 bokstaver):

LODDRETT

1 loddrett: Et avansert filter som blokkerer annonser, skadevare og bannere for samtykke til informasjonskapsler (8 bokstaver):

2 loddrett: Split tunneling-funksjonalitet som lar utvalgte applikasjoner omgå VPN-en (8 bokstaver):

3 loddrett: Tilsløringsteknologi som skjuler VPN-signaturer for å etterligne vanlig HTTPS-trafikk (10 bokstaver):

4 loddrett: En automatisk sikkerhetsfunksjon som blokkerer nettverkstrafikk når VPN-en faller ut (10 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

CLEANWEB RAMBASERTE MULTIHOP CAMOUFLAGE BYPASSER KILLSWITCH NEXUS ROTERENDEIP

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. CLEANWEB
B. RAMBASERTE
C. MULTIHOP
D. CAMOUFLAGE
E. BYPASSER
F. KILLSWITCH
G. NEXUS
H. ROTERENDEIP

DEFINISJONER OG TILHØRENDE FELT	
	1. Tilsløringsteknologi som skjuler VPN-signaturer for å etterligne vanlig HTTPS-trafikk.
	2. En automatisk sikkerhetsfunksjon som blokkerer nettverkstrafikk når VPN-en faller ut.
	3. Et avansert filter som blokkerer annonser, skadevare og bannere for samtykke til informasjonskapsler.
	4. Split tunneling-funksjonalitet som lar utvalgte applikasjoner omgå VPN-en.
	5. Servermaskinvare med flyktig minne som sletter alle data ved hver strømsyklus.
	6. En funksjon som jevnlig endrer din eksterne IP-adresse uten å avbryte tunneler.
	7. En funksjon for dobbel VPN-ruting som krypterer trafikk over to separate servernoder.
	8. Et proprietært programvaredefinert nettverk som kobler alle servere sammen til ett samlet mesh.

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. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. RSEABEARTM
6. GUOLACAFEM
7. ILKIWTCHSL
8. ENPETRROIDE

Bonusaktivitet: Tenk raskt

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

1	Sikkerhetsfunksjoner i Surfshark			
2	Tegn på at VPN-tilkoblingen din er treg			
3	VPN-protokoller du kjenner til			
4	Ting kryptering beskytter			
5	Trusler på offentlig Wi-Fi			
6	Land kjent for sterk personvernlovgivning			
7	Måter å lage et sterkt passord på			
8	Enheter du ville installert Surfshark på			
9	Spørsmål til kundestøtten i Surfshark			
10	Innstillinger du slår på for ekstra sikkerhet			
11	Ting Surfshark kan skjule for nettverket ditt			
12	Typer VPN-lekkasjer			
13	Data en VPN aldri bør lagre			
14	Ord som beskriver en god VPN-app			
15	Ting en revisjon kan kontrollere			

Kontrollpunkt 8: Casestudier om VPN og nettverk

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

CASESTUDIE 1: OMGÅ FILTRE PÅ CAMPUS OG ARBEIDSPLASS



Scenario: En student oppdager at campus-Wi-Fi på universitetet blokkerer alle vanlige OpenVPN- og WireGuard-porter.

Diskusjonsspørsmål: Hvilken Surfshark-funksjon gjør at studenten kan koble til uten å bli oppdaget av nettverksadministratorene?

CASESTUDIE 2: JOURNALISTISK UNDERSØKELSE MED HØY RISIKO



Scenario: En undersøkende journalist trenger ekstra beskyttelse mot overvåking mens vedkommende undersøker sensitive selskapsregistre.

Diskusjonsspørsmål: Hvordan gir Dynamic MultiHop bedre personvern enn ruting via én server?

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	21	18	6	19	8	1	18	11		14	5	24	21	19
18	15	20	5	18	5	14	4	5		9	16		7	9	18
16	5	18	19	15	14	22	5	18	14					

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 er Surfshark CleanWeb?

CleanWeb er en integrert sikkerhetsfunksjon som blokkerer reklame, sporere, skadevare og nettfiskingsnettsteder.

Q2: Hva er RAM-only-servere?

Servere som kun bruker RAM kjører på flyktig minne, noe som betyr at data i minnet slettes hver gang serverne starter på nytt.

Q3: Hva er Surfshark MultiHop?

MultiHop (Double VPN) ruter og krypterer internettforbindelsen din gjennom to ulike serverplasseringer.

Q4: Hvordan fungerer Camouflage Mode?

Camouflage Mode obfuskerer VPN-trafikk slik at internettleverandøren din ikke kan se at du bruker en VPN.

Q5: Hva er Bypasser-funksjonen?

Bypasser er Surfsharks verktøy for delt tunnelering som lar bestemte apper eller nettsteder omgå VPN-en.

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: Har Surfshark en Kill Switch?

Ja, Kill Switch kobler deg fra internett hvis VPN-en uventet faller ut.

Q7: Hvilken krypteringsstandard bruker Surfshark?

Surfshark bruker AES-256-GCM og ChaCha20, pluss AEGIS-256X2 i den nye Dausos-protokollen.

Q8: Har Surfsharks policy om ingen logging blitt revidert?

Ja, Deloitte bekreftet Surfsharks policy om ingen logging i 2023 og igjen i 2025.

Q9: Hva er Surfshark Nexus?

Nexus er en avansert SDN-arkitektur som kobler alle servere sammen til ett samlet nettverk for jevnere ruting.

Q10: Hva er IP Rotator-funksjonen?

IP-rotator endrer IP-adressen din automatisk hvert par minutter uten å koble fra VPN-økten.

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 skiller Dynamic MultiHop seg fra tradisjonell Double VPN?

Dynamic MultiHop lar deg tilpasse hvilken som helst kombinasjon av inngangs- og utgangsservere verden over.

Q2: Fungerer CleanWeb 2.0 i nettleserutvidelser?

Ja, CleanWeb 2.0 blokkerer videoannonser, popup-vinduer for samtykke til informasjonskapsler og varselbannere i Chrome og Firefox.

Q3: Hva er Alternative ID i sikkerhetspakken?

Alternative ID genererer unike personlige pseudonymer, e-postadresser og telefonmasker.

Q4: Hvordan forhindrer Surfshark DNS-lekkasjer?

Surfshark ruter alle domeneforespørsler gjennom sine egne private DNS-servere på hver node.

Q5: Støtter Surfshark ChaCha20-kryptering på mobil?

Ja, WireGuard på Android og iOS bruker ChaCha20-Poly1305 for overlegen effektivitet på mobil.

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

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

Q6: Hva er NoBorders-modus i Surfshark?

NoBorders oppdager automatisk restriktive nettverksmiljøer og leverer spesialiserte servere.

Q7: Hvem utførte sikkerhetsrevisjonene av Surfsharks nettleserutvidelser?

Det uavhengige cybersikkerhetsselskapet Cure53 gjennomførte revisjoner av nettleserutvidelser og serversystemer.

Q8: Hvordan beskytter Surfshark mot IPv6-lekkasjer?

Surfshark ruter IPv6-trafikk på en sikker måte eller begrenser den på en trygg måte for å hindre ukryptert lekkasje.

Q9: Hvor har Surfshark sin juridiske jurisdiksjon?

Surfshark opererer under nederlandsk lov og følger strenge europeiske personvernstandarder i GDPR.

Q10: Støtter Surfshark tofaktorautentisering (2FA)?

Ja, og Surfshark One legger til en 2FA-lås slik at bare du kan endre funksjonsinnstillinger.

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

1. Surfshark sier at hele serverparken på over 4 500 servere kjører på diskløs, flyktig maskinvare som bare bruker RAM.

2. VPN-INNSIKT

2. Storselskapet Deloitte, ett av de fire store, verifiserte Surfsharks policy om ingen logging i 2023 og igjen i november 2025.

3. VPN-INNSIKT

3. Den proprietære Nexus-arkitekturen kobler alle globale servere sammen i et dynamisk programvaredefinert nettverk.

4. VPN-INNSIKT

4. Rotating IP endrer IP-adressen din omtrent hvert femte minutt uten å bryte VPN-tilkoblingen.

5. VPN-INNSIKT

5. CleanWeb 2.0 blokkerer påtrengende popup-vinduer for samtykke til informasjonskapsler og videoannonser direkte i nettlesere.

6. VPN-INNSIKT

6. Dynamic MultiHop lar brukere lage tilpassede krypteringsveier med to servere på tvers av 100 land.

7. VPN-INNSIKT

7. Kamuflasjemodus fjerner VPN-hodesignaturer, slik at trafikken ikke kan skilles fra vanlig HTTPS.

8. VPN-INNSIKT

8. Alternative ID genererer engangspseudonymer og e-postmasker for å beskytte brukere mot databaselekkasjer.

9. VPN-INNSIKT

9. Surfshark håndhever symmetrisk AES-256-GCM-kryptering sammen med ChaCha20 i WireGuard-protokoller.

10. VPN-INNSIKT

10. NoBorders-modus aktiveres automatisk på begrensede nettverk for å gi robust tunneltilgang.

Tekniske referanser og kilder

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

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Fasit: Kontrollpunkt 1 – flervalg

1 **Integrert innholdsblokkering** FORSVAR MOT ANNONSER OG SKADEVARE **Riktig svar: B**

MERKNAD TIL LÆREREN

CleanWeb er Surfsharks integrerte sikkerhetsfilter som blokkerer reklame, sporerdomener, nettfiskingsnettsteder og skadelige URL-skript på nettverksnivå.

2 **100 % infrastruktur kun med RAM** RAM-ARKITEKTUR **Riktig svar: B**

MERKNAD TIL LÆREREN

Surfshark kjører servere som bare bruker RAM, så data i servernes minne slettes når en server slås av eller startes på nytt.

3 **MultiHop dobbel tunnelering** MULTIHOP-VPN **Riktig svar: B**

MERKNAD TIL LÆREREN

MultiHop (Double VPN) krypterer trafikk gjennom to ulike servernoder i separate land for å forhindre trafikkkorrelasjonsangrep.

4 **Camouflage Mode: obfuskering** OBFUSKERING **Riktig svar: B**

MERKNAD TIL LÆREREN

Camouflage Mode endrer OpenVPN-pakkehoder for å få VPN-trafikk til å se ut som vanlig HTTPS-trafikk, slik at restriktive brannmurblokkeringer omgås.

5 **Bypasser – delt tunnelering** SPLIT TUNNELING **Riktig svar: B**

MERKNAD TIL LÆREREN

Bypasser er Surfsharks verktøy for delt tunnelering som lar brukere velge bestemte apper eller nettsteder som skal rutes direkte gjennom den vanlige tilkoblingen til internettleverandøren.

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Sletting av data i flyktig minne** SERVERSIKKERHET **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Servere som kun bruker RAM lagrer ingen data på permanente harddisker; en omstart av maskinvaren tømmer umiddelbart alt driftsminne.

7 **Camouflage Mode: skjuling av internettleverandøren** SKJULING AV TRAFIKK **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Camouflage Mode fjerner OpenVPN-protokollsignaturer og hindrer dermed internettleverandører i å oppdage at brukeren er koblet til en VPN-tunnel.

8 **CleanWeb 2.0-nettleserutvidelser** NETTLESERUTVIDELSE **Riktig svar: Sant**

MERKNAD TIL LÆREREN

CleanWeb 2.0 fungerer i nettleserutvidelser for å blokkere popup-vinduer for samtykke til informasjonskapsler, videoreklame og skadelige omdirigeringsskript i sanntid.

9 **Ingen lagring av tilkoblingslogger** POLICY OM INGEN LOGGING **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Surfshark har en streng policy om null logging som er uavhengig revidert, og registrerer ingen IP-adresser, tidsstempler for tilkoblinger eller båndbreddelogger.

10 **Dynamisk IP-rotasjon i Nexus** NEXUS-NETTVERK **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Det programvaredefinerte nettverket Surfshark Nexus bytter ut brukernes IP-adresser dynamisk med få minutters mellomrom uten å avbryte den aktive VPN-tilkoblingen.

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. CLEANWEB	D 2. RAM-BASERTE	G 3. MULTI-HOP	F 4. CAMOUFLAGE
B 5. BYPASSER	A 6. KILL SWITCH	H 7. NEXUS	E 8. ROTERENDE

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 CLEANWEB	2 RAM-BASERTE	3 MULTI-HOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – RAMBASERTE	6 H – ROTERENDEIP	7 C – MULTIHOP	8 G – NEXUS

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare CLEANWEB, RAM-BASERTE og MULTI-HOP med egne ord og gi et eksempel på hvert.

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

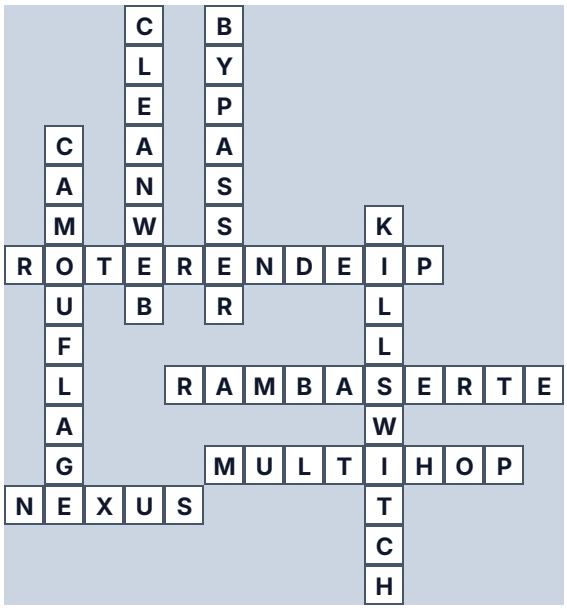
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

5 vannrett: ROTERENDEIP En funksjon som jevnlig endrer din eksterne IP-adresse uten å avbryte tunneler (11 bokstaver)

6 vannrett: RAMBASERTE Servermaskinvare med flyktig minne som sletter alle data ved hver strømsyklus (10 bokstaver)

7 vannrett: MULTIHOP En funksjon for dobbel VPN-ruting som krypterer trafikk over to separate servernoder (8 bokstaver)

8 vannrett: NEXUS Et proprietært programvaredefinert nettverk som kobler alle servere sammen til ett samlet mesh (5 bokstaver)

LODDRETT

1 loddrett: CLEANWEB Et avansert filter som blokkerer annonser, skadevare og bannere for samtykke til informasjonskapsler (8 bokstaver)

2 loddrett: BYPASSER Split tunneling-funksjonalitet som lar utvalgte applikasjoner omgå VPN-en (8 bokstaver)

3 loddrett: CAMOUFLAGE Tilsløringsteknologi som skjuler VPN-signaturer for å etterligne vanlig HTTPS-trafikk (10 bokstaver)

4 loddrett: KILLSWITCH En automatisk sikkerhetsfunksjon som blokkerer nettverkstrafikk når VPN-en faller ut (10 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. R S E A B E A R T M — **RAMBASERTE**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. E N P E T R R O I D E — **ROTERENDEIP**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"SURFSHARK NEXUS ROTERENDE IP GIR PERSONVERN"

Fasit til casestudiene

A CASESTUDIE 1: OMGÅ FILTRE PÅ CAMPUS OG ARBEIDSPLASS

Løsning for læreren

RETTEMAL OG VEILEDNING FOR LØSNINGER

- Scenarioanalyse: En student oppdager at campusens Wi-Fi på universitetet blokkerer alle standardporter for OpenVPN og WireGuard.
- Fokusspørsmål: Hvilken Surfshark-funksjon lar studenten koble til uten å bli oppdaget av nettverksadministratorer?
- Anbefalt strategi og løsning: Aktiver Camouflage Mode (OpenVPN), som skjuler VPN-metadata slik at brannmurer ser vanlig HTTPS-surfing.

B CASESTUDIE 2: JOURNALISTISK UNDERSØKELSE MED HØY RISIKO

Løsning for læreren

RETTEMAL OG VEILEDNING FOR LØSNINGER

- Scenarioanalyse: En undersøkende journalist trenger ekstra beskyttelse mot overvåking mens vedkommende undersøker sensitive bedriftsregistre.
- Fokusspørsmål: Hvordan gir Dynamic MultiHop bedre personvern enn ruting via én enkelt server?
- Anbefalt strategi og løsning: Dynamisk MultiHop ruter trafikken gjennom inngangs- og utgangsservere i to land, slik at ingen enkeltserver kan avsløre brukeren.