Namn: _____ Datum: _____ Poäng: _____

Surfsharks säkerhet

Granskning av Surfshark-säkerhetsfunktioner, inklusive annonsblockeringen CleanWeb, dynamisk MultiHop-routning, SDN-arkitekturen Nexus, serverflottan med enbart RAM och läget Camouflage.

ÖVERSIKT: SURFSHARKS SÄKERHET

ELEV
STUDENTSTATUS
Nätverksförsvararspåret

SÄKER
ANSLUTNINGSSTATUS
Skydda datapaket

AKTIV
LÄCKSKYDD
Skydd mot DNS- och IPv6-läckor

Välkommen! Det här aktivitetshäftet guidar dig genom Surfsharks säkerhetsarkitektur. Du får utforska serverhårdvara med enbart RAM, dynamisk IP-rotation med Nexus SDN, reklamblockerare i CleanWeb och MultiHop-routning.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska konfigurationer för VPN och nätverkssäkerhet.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

Öppna VPN.com:s guide till de bästa VPN-tjänsterna

URL: https://www.vpn.com/sv/vpn/surfshark/sakerhet/

Din inlärningsplan för Surfsharks säkerhet

- Analysera den tekniska arkitekturen och konfigurationsreglerna för Surfshark Security.
- Konfigurera klientinställningar för att förhindra läckor av IP-, DNS- och WebRTC-trafik.
- Jämför egna priser, provperioder och prestandafunktioner med standardmodeller.

INSTRUKTIONER TILL GUIDEN OM SURFSHARKS SÄKERHET

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om infrastruktur med endast RAM, Nexus SDN och CleanWeb. Avsluta med bonusaktiviteten Tänk snabbt.

SERVERFLOTTA MED ENBART RAM, NEXUS SDN OCH CLEANWEB-ARKITEKTUR (INTRODUKTION)

Surfshark skyddar användarnas integritet med en serverflotta med enbart RAM, programvarudefinierade nätverk med Nexus och IP Rotator, annonsblockering med CleanWeb och krypterade vägar med Dynamic MultiHop.

LÄS VARJE KONTROLLPUNKT NOGGRANT OCH VÄLJ ELLER SKRIV DET RÄTTA SVARET.

Kontrollpunkt 1: Utmaning med flerval

1. **1. Vad heter Surfsharks integrerade blockerare av annonser och skadlig kod?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Vilken hårdvaruarkitektur använder Surfshark på alla servrar?**
   - A) Hårddiskar
   - B) 100 % endast RAM
   - C) Optisk lagring
   - D) Magnetband

3. **3. Vilken funktion dirigerar trafiken genom två olika VPN-servrar?**
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) Nexus-nätverk
   - D) Statisk IP-adress

4. **4. Vilken obfuskeringsfunktion får VPN-trafik att se ut som vanlig webbdata?**
   - A) Kill Switch
   - B) Kamouflageläge
   - C) CleanWeb 2.0
   - D) Delad tunnel

5. **5. Vad gör verktyget Surfshark Bypasser?**
   - A) Speed Booster
   - B) Delad tunnel (split tunneling)
   - C) Lösenordshanterare
   - D) DNS-resolver

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Servrar som bara använder RAM raderar alla driftdata omedelbart när servern startar om.

○ Sant ○ Falskt

7 Fråga 7

7. Camouflage Mode hindrar ISP:er från att upptäcka att du använder en VPN.

○ Sant ○ Falskt

8 Fråga 8

8. CleanWeb 2.0 körs i webbläsartillägg för att blockera popup-fönster för cookiesamtycke.

○ Sant ○ Falskt

9 Fråga 9

9. Surfshark sparar tillfälliga tidsstämplar för anslutningar och loggar över bandbreddsanvändning.

○ Sant ○ Falskt

10 Fråga 10

10. Nätverket Nexus roterar regelbundet användarnas IP-adresser utan att koppla från.

○ Sant ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

Läs varje mening nedan och fyll i luckan med rätt term från ordbanken.

1. Irriterande webbannonser, spårningsskript och nätfiskelänkar blockeras av filtret _____ .

2. Användarens aktivitet lämnar inga kriminaltekniska spår eftersom servrarna arbetar med _____ .

3. Att dirigera data via två separata krypterade serverhopp sker med tunnlar av typen _____ .

4. För att dölja VPN-användning för internetleverantörer aktiverar användare läget _____ .

5. Att låta banktjänster gå förbi VPN-tunneln hanteras med inställningar för _____ .

6. Nästa generations SDN-arkitektur som kopplar samman serverflottan är systemet _____ .

ORDBANK

BYPASSER CAMOUFLAGE CLEANWEB ENDAST RAM KILL SWITCH MULTIHOP NEXUS ROTERANDE IP

Skriv dina svar här:

1. 2.

3. 4.

5. 6.

Kontrollpunkt 4: Matchning av VPN- och nätverksbegrepp

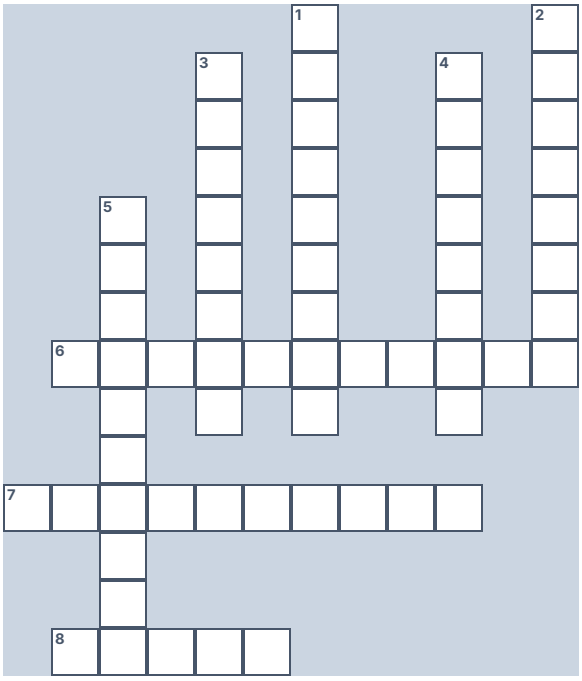
MATCHNING AV DEFINITIONER

Para ihop varje begrepp till vänster med rätt definition till höger genom att skriva motsvarande bokstav (A–H) i det ifyllbara fältet.

☐	1. CLEANWEB	A	En automatisk säkerhetsfunktion som blockerar nätverkstrafik när VPN faller.
☐	2. ENDAST RAM	B	Funktion för delad tunnling som låter utvalda program gå förbi VPN-tjänsten.
☐	3. MULTIHOP	C	Ett avancerat filter som blockerar annonser, skadlig kod och banners för cookiesamtycke.
☐	4. KAMOUFLAGE	D	Serverhårdvara med flyktigt minne som raderar all data vid varje strömcykel.
☐	5. KRINGGÅENDE VERKTYG	E	En funktion som regelbundet byter din externa IP-adress utan att avbryta tunnlar.
☐	6. KILL SWITCH	F	Obfuskeringsteknik som döljer VPN-signaturer så att de efterliknar vanlig HTTPS-trafik.
☐	7. NEXUS NET	G	En dubbel-VPN-funktion som krypterar trafiken över två separata servernoder.
☐	8. ROTERANDE	H	Ett proprietärt programdefinierat nätverk som kopplar samman alla servrar i ett enhetligt mesh.

Kontrollpunkt 5: Korsord

Lös korsordet genom att skriva bokstäver i de aktiva vita rutorna. Siffrorna motsvarar ledtrådarna nedan.



VÅGRÄTT

6. En funktion som regelbundet byter din externa IP-adress utan att avbryta tunnlarna (11)

7. En automatisk säkerhetsfunktion som blockerar nätverkstrafiken när VPN-anslutningen faller (10)

8. Ett egenutvecklat programvarudefinierat nätverk som kopplar ihop alla servrar till ett enhetligt mesh (5)

LODRÄTT

1. Serverhårdvara med flyktigt minne som raderar all data vid varje omstart av strömmen (9)

2. Dubbel-VPN-funktion som krypterar trafiken över två skilda servernoder (8)

3. Avancerat filter som blockerar annonser, skadlig kod och banners för cookiesamtycke (8)

4. Funktion för delad tunneling som låter vissa program gå förbi VPN (8)

5. Förvrängningsteknik som döljer VPN-signaturer så att trafiken liknar vanlig HTTPS-trafik (10)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

Användare av skärmläsare och tangentbord kan skriva korsordssvaren direkt i textfälten nedan.

VÅGRÄTT

6 vågrätt: En funktion som regelbundet byter din externa IP-adress utan att avbryta tunnlarna (11 bokstäver):

7 vågrätt: En automatisk säkerhetsfunktion som blockerar nätverkstrafiken när VPN-anslutningen faller (10 bokstäver):

8 vågrätt: Ett egenutvecklat programvarudefinierat nätverk som kopplar ihop alla servrar till ett enhetligt mesh (5 bokstäver):

LODRÄTT

1 lodrätt: Serverhårdvara med flyktigt minne som raderar all data vid varje omstart av strömmen (9 bokstäver):

2 lodrätt: Dubbel-VPN-funktion som krypterar trafiken över två skilda servernoder (8 bokstäver):

3 lodrätt: Avancerat filter som blockerar annonser, skadlig kod och banners för cookiesamtycke (8 bokstäver):

4 lodrätt: Funktion för delad tunneling som låter vissa program gå förbi VPN (8 bokstäver):

5 lodrätt: Förvrängningsteknik som döljer VPN-signaturer så att trafiken liknar vanlig HTTPS-trafik (10 bokstäver):

Kontrollpunkt 6: Dolt ordsök

Hitta de 8 viktiga ordförrådstermerna som är gömda i rutnätet nedan. Orden kan vara vågräta, lodräta eller diagonala.

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

ORDLISTA

CLEANWEB, ENDASTRAM, MULTIHOP, CAMOUFLAGE, BYPASSER, KILLSWITCH, NEXUS, ROTERANDEIP

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

ORDLISTA

- **A. CLEANWEB**
- **B. ENDASTRAM**
- **C. MULTIHOP**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. ROTERANDEIP**

DEFINITIONER OCH MATCHNINGSFÄLT

_____ 1. Förvrängningsteknik som döljer VPN-signaturer så att trafiken liknar vanlig HTTPS-trafik.

_____ 2. En automatisk säkerhetsfunktion som blockerar nätverkstrafiken när VPN-anslutningen faller.

_____ 3. Avancerat filter som blockerar annonser, skadlig kod och banners för cookiesamtycke.

_____ 4. Funktion för delad tunneling som låter vissa program gå förbi VPN.

_____ 5. Serverhårdvara med flyktigt minne som raderar all data vid varje omstart av strömmen.

_____ 6. En funktion som regelbundet byter din externa IP-adress utan att avbryta tunnlarna.

_____ 7. Dubbel-VPN-funktion som krypterar trafiken över två skilda servernoder.

_____ 8. Ett egenutvecklat programvarudefinierat nätverk som kopplar ihop alla servrar till ett enhetligt mesh.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga begrepp och termer om Virtual Private Network (VPN). Skriv dina svar i rutorna.

1. E A N C W L B E
2. T M P U O H I L
3. A Y B S S R E P
4. X S U N E
5. R S N M T A E A D
6. G U O L A C A F E M
7. I L K I W T C H S L
8. E N P A T R R O I D E

Bonusaktivitet: Tänk snabbt

3 SVAR PER KATEGORI. DEN SOM FÖRST FYLLER I LISTAN VINNER.

1	Säkerhetsfunktioner i Surfshark			
2	Tecken på att din VPN-anslutning är långsam			
3	VPN-protokoll du känner till			
4	Saker som kryptering skyddar			
5	Hot på offentligt wifi			
6	Länder som är kända för starka integritetslagar			
7	Sätt att skapa ett starkt lösenord			
8	Enheter du skulle installera Surfshark på			
9	Frågor till kundsupporten hos Surfshark			
10	Inställningar du slår på för extra säkerhet			
11	Saker som Surfshark kan dölja för ditt nätverk			
12	Typer av VPN-läckor			
13	Data som ett VPN aldrig bör lagra			
14	Ord som beskriver en bra VPN-app			
15	Saker som en granskning kan kontrollera			

Kontrollpunkt 8: Fallstudier om VPN och nätverk

Tillämpa de begrepp du har lärt dig för att lösa de verkliga scenarierna nedan.

FALLSTUDIE 1: KRINGGÅ FILTER PÅ CAMPUS OCH ARBETSPLATS



Scenario: En student upptäcker att wifi på universitetscampuset blockerar alla vanliga OpenVPN- och WireGuard-portar.

Diskussionsfråga: Vilken Surfshark-funktion gör att studenten kan ansluta utan att upptäckas av nätverksadministratörerna?

FALLSTUDIE 2: RISKFYLLD GRANSKANDE JOURNALISTIK



Scenario: En undersökande journalist behöver extra skydd mot övervakning när hen granskar känsliga företagsregister.

Diskussionsfråga: Hur ger Dynamic MultiHop bättre integritet än routing via en enda server?

Kontrollpunkt 9: Knäck chiffret

En nätverksingenjör skyddar dirigeringskanaler och klienttunnlar. Använd bokstav-till-siffra-nyckeln nedan för att avkoda meddelandet genom att skriva de matchande bokstäverna på de tomma raderna.

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

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 Å=27 Ä=28 Ö=29

19	21	18	6	19	8	1	18	11	14	5	24	21	19	15	3	8	
18	15	20	5	18	1	14	4	5	9	16	19	11	25	4	4	1	18

Avkodat meddelande:

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

Kontrollpunkt 10: Grundläggande vanliga frågor om VPN (Del A)

Gå igenom de vanligaste frågorna och svaren om virtuella privata nätverk (VPN) och tunnling.

Q1: Vad är Surfshark CleanWeb?

CleanWeb är en integrerad säkerhetsfunktion som blockerar annonser, spårare, skadlig kod och nätfiskewebbplatser.

Q2: Vad är servrar med enbart RAM?

Servrar som bara använder RAM körs på flyktigt minne, vilket betyder att data i minnet raderas varje gång servrarna startar om.

Q3: Vad är Surfshark MultiHop?

MultiHop (Double VPN) dirigerar och krypterar din internetanslutning via två olika serverplatser.

Q4: Hur fungerar Camouflage Mode?

Camouflage Mode obfuskerar VPN-trafik så att din ISP inte kan se att du använder en VPN.

Q5: Vad är funktionen Bypasser?

Bypasser är Surfsharks verktyg för delad tunnel (split tunneling) som låter vissa appar eller webbplatser kringgå VPN.

Kontrollpunkt 10: Grundläggande vanliga frågor om VPN (Del B)

Gå igenom de vanligaste frågorna och svaren om virtuella privata nätverk (VPN) och tunnling.

Q6: Har Surfshark en kill switch?

Ja, Kill Switch kopplar bort dig från internet om VPN:et oväntat bryts.

Q7: Vilken krypteringsstandard använder Surfshark?

Surfshark använder AES-256-GCM och ChaCha20, plus AEGIS-256X2 i sitt nya protokoll Dausos.

Q8: Har Surfsharks policy om inga loggar granskats?

Ja, Deloitte verifierade Surfsharks policy om inga loggar 2023 och igen 2025.

Q9: Vad är Surfshark Nexus?

Nexus är en avancerad SDN-arkitektur som kopplar samman alla servrar i ett enhetligt nätverk för smidigare routing.

Q10: Vad är funktionen IP Rotator?

IP Rotator byter din IP-adress automatiskt var några minuter utan att koppla från din VPN-session.

Kontrollpunkt 10: Avancerade vanliga frågor om VPN (Del C)

Utforska avancerade tekniska aspekter av VPN-tunnelprotokoll, integrationer med mobilklienter och driftsättning i företag.

Q1: Hur skiljer sig Dynamic MultiHop från traditionellt Double VPN?

Dynamic MultiHop låter dig anpassa valfri kombination av ingångs- och utgångsservrar över hela världen.

Q2: Fungerar CleanWeb 2.0 i webbläsartillägg?

Ja, CleanWeb 2.0 blockerar videoannonser, popup-fönster för cookiesamtycke och varningsbanners i Chrome/Firefox.

Q3: Vad är Alternative ID i säkerhetspaketet?

Alternative ID skapar unika personliga pseudonymer, e-postadresser och telefonmasker.

Q4: Hur förhindrar Surfshark DNS-läckor?

Surfshark routar alla domänförfrågningar via sina egna privata DNS-servrar på varje nod.

Q5: Stöder Surfshark ChaCha20-kryptering på mobilen?

Ja, WireGuard på Android och iOS använder ChaCha20-Poly1305 för överlägsen effektivitet på mobil.

Kontrollpunkt 10: Avancerade vanliga frågor om VPN (Del D)

Utforska avancerade tekniska aspekter av VPN-tunnelprotokoll, integrationer med mobilklienter och driftsättning i företag.

Q6: Vad är NoBorders-läget i Surfshark?

NoBorders upptäcker automatiskt begränsade nätverksmiljöer och tillhandahåller specialiserade servrar.

Q7: Vem utförde säkerhetsgranskningarna av Surfsharks webbläsartillägg?

Det oberoende cybersäkerhetsföretaget Cure53 slutförde granskningar av webbläsartillägg och serversystem.

Q8: Hur skyddar Surfshark mot IPv6-läckor?

Surfshark routar IPv6-trafik säkert eller begränsar den på ett säkert sätt för att förhindra okrypterade läckor.

Q9: Var finns Surfsharks juridiska jurisdiktion?

Surfshark verkar enligt nederländsk lag och följer stränga europeiska integritetsstandarder enligt GDPR.

Q10: Stöder Surfshark tvåfaktorsautentisering (2FA)?

Ja, och Surfshark One lägger till ett 2FA-lås så att bara du kan ändra funktionsinställningar.

Del 11: 10 verkliga fakta och insikter om VPN

Gå igenom verkliga fakta om VPN-kryptering och hastigheter, protokollgranskningar, mobil anslutning och distansarbete i företag.

1. VPN-INSIKT

1. Surfshark uppger att hela nätverket med över 4,500 servrar körs på diskless, flyktig hårdvara med enbart RAM.

2. VPN-INSIKT

2. Det stora fyra-företaget Deloitte verifierade Surfsharks policy om att inte spara loggar 2023 och på nytt i november 2025.

3. VPN-INSIKT

3. Den proprietära Nexus-arkitekturen kopplar samman alla globala servrar i ett dynamiskt programvarudefinierat nätverk.

4. VPN-INSIKT

4. Roterande IP byter din IP-adress ungefär var femte minut utan att VPN-anslutningen bryts.

5. VPN-INSIKT

5. CleanWeb 2.0 blockerar påträngande popup-fönster för cookiegodkännande och videoannonser direkt i webbläsare.

6. VPN-INSIKT

6. Dynamic MultiHop låter användare skapa anpassade krypteringsvägar via två servrar över 100 länder.

7. VPN-INSIKT

7. Camouflage Mode tar bort VPN-huvudsignaturer, vilket gör trafiken omöjlig att skilja från vanlig HTTPS.

8. VPN-INSIKT

8. Alternative ID skapar engångspseudonymer och e-postmasker för att skydda användare mot dataläckor.

9. VPN-INSIKT

9. Surfshark tillämpar symmetrisk AES-256-GCM-kryptering tillsammans med ChaCha20 i WireGuard-protokoll.

10. VPN-INSIKT

10. NoBorders-läget aktiveras automatiskt på begränsade nätverk för att ge motståndskraftig tunnelåtkomst.

Tekniska referenser och källor

Studieguiden och de interaktiva pusslen är sammanställda utifrån globala tekniska standarder, specifikationer och regelverk.

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[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

Facit: Kontrollpunkt 1 – Flerval

1 **Integrerad innehållsblockerare** SKYDD MOT ANNONSER OCH SKADLIG KOD — Rätt svar: B

ANTECKNING FÖR LÄRAREN

CleanWeb är Surfsharks integrerade säkerhetsfilter som blockerar annonser, spårardomäner, nätfiskewebbplatser och skadliga URL-skript på nätverksnivå. Källa: CleanWeb Security Specs.

2 **100% infrastruktur med enbart RAM** RAM-ARKITEKTUR — Rätt svar: B

ANTECKNING FÖR LÄRAREN

Surfshark kör servrar med enbart RAM, så data i serverminnet raderas när en server stängs av eller startas om. Källa: Cure53 Infrastructure Audit.

3 **MultiHop-dubbeltunnling** MULTIHOP-VPN — Rätt svar: B

ANTECKNING FÖR LÄRAREN

MultiHop (Double VPN) krypterar trafiken genom två olika servernoder i separata länder för att förhindra korrelationsattacker mot trafik. Källa: Surfshark MultiHop Guide.

4 **Obfuskering med Camouflage Mode** OBFUSKERING — Rätt svar: B

ANTECKNING FÖR LÄRAREN

Camouflage Mode ändrar paketrubriker i OpenVPN för att få VPN-trafiken att likna vanlig HTTPS-trafik och kringgår restriktiva brandväggsblockeringar. Källa: Surfshark Stealth Whitepaper.

5 **Delad tunnel med Bypasser** SPLIT TUNNELING — Rätt svar: B

ANTECKNING FÖR LÄRAREN

Bypasser är Surfsharks verktyg för delad tunnel (split tunneling) som låter användare välja specifika appar eller webbplatser som ska dirigeras direkt via den vanliga internetanslutningen. Källa: Surfshark Client Features.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Radering av data i flyktigt minne** SERVERSÄKERHET — Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Servrar som bara använder RAM lagrar inga data på permanenta hårddiskar. När hårdvaran startas om rensas hela arbetsminnet omedelbart. Källa: RAM Server Architecture.

7 **Dold ISP-identifiering med Camouflage Mode** TRAFIKDÖLJNING — Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Camouflage Mode tar bort OpenVPN-protokollets signaturer, vilket hindrar ISP:er från att upptäcka att användaren är ansluten till en VPN-tunnel. Källa: Deep Packet Inspection Guide.

8 **Webbläsartillägg för CleanWeb 2.0** WEBBLÄSARTILLÄGG — Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

CleanWeb 2.0 körs i webbläsartillägg för att i realtid blockera popup-fönster för cookiesamtycke, videoannonser och skadliga omdirigeringsskript. Källa: CleanWeb 2.0 Release Notes.

9 **Noll lagring av anslutningsloggar** NO-LOGS-POLICY — Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Surfshark upprätthåller en strikt, oberoende granskad policy utan loggar och registrerar inga IP-adresser, tidsstämplar för anslutningar eller bandbreddsloggar. Källa: Deloitte No-Logs Audit.

10 **Nexus dynamisk IP-rotation** NEXUS-NÄTVERK — Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Det programvarudefinierade nätverket Surfshark Nexus roterar användarnas IP-adresser dynamiskt med några minuters mellanrum utan att den aktiva VPN-anslutningen bryts. Källa: Surfshark Nexus Architecture.

Facit för ordförråd och bedömningsmall

Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

C 1. CLEANWEB	D 2. ENDAST RAM	G 3. MULTIHOP	F 4. KAMOUFLAGE
B 5. KRINGGÅENDE VERKTYG	A 6. KILL SWITCH	H 7. NEXUS NET	E 8. ROTERANDE

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 CLEANWEB	2 ENDAST RAM	3 MULTIHOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

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

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara CLEANWEB, ENDAST RAM och MULTIHOP med egna ord och ge ett exempel på varje.

Fallstudier:
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

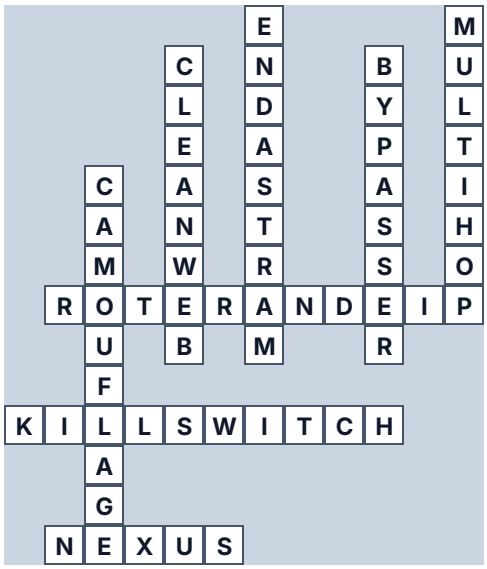
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

6 vågrätt: ROTERANDEIP En funktion som regelbundet byter din externa IP-adress utan att avbryta tunnlarna (11 bokstäver)

7 vågrätt: KILLSWITCH En automatisk säkerhetsfunktion som blockerar nätverkstrafiken när VPN-anslutningen faller (10 bokstäver)

8 vågrätt: NEXUS Ett egenutvecklat programvarudefinierat nätverk som kopplar ihop alla servrar till ett enhetligt mesh (5 bokstäver)

LODRÄTT

1 lodrätt: ENDASTRAM Serverhårdvara med flyktigt minne som raderar all data vid varje omstart av strömmen (9 bokstäver)

2 lodrätt: MULTIHOP Dubbel-VPN-funktion som krypterar trafiken över två skilda servernoder (8 bokstäver)

3 lodrätt: CLEANWEB Avancerat filter som blockerar annonser, skadlig kod och banners för cookiesamtycke (8 bokstäver)

4 lodrätt: BYPASSER Funktion för delad tunneling som låter vissa program gå förbi VPN (8 bokstäver)

5 lodrätt: CAMOUFLAGE Förvrängningsteknik som döljer VPN-signaturer så att trafiken liknar vanlig HTTPS-trafik (10 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

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 N M T A E A D — **ENDASTRAM**
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 A T R R O I D E — **ROTERANDEIP**

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"SURFSHARK NEXUS OCH ROTERANDE IP SKYDDAR"

Facit till fallstudierna

A FALLSTUDIE 1: KRINGGÅ FILTER PÅ CAMPUS OCH ARBETSPLATS

Lärarens lösning

BEDÖMNINGSMATRIS OCH LÖSNINGSRIKTLINJER

- Scenarioanalys: En student upptäcker att universitetets campus-Wi-Fi blockerar alla vanliga portar för OpenVPN och WireGuard.
- Fokusfråga: Vilken funktion i Surfshark gör att studenten kan ansluta utan att nätverksadministratörer upptäcker det?
- Rekommenderad strategi och lösning: Aktivera Camouflage Mode (OpenVPN), som döljer VPN-metadata så att brandväggar ser vanlig HTTPS-surfning.

B FALLSTUDIE 2: RISKFYLLD GRANSKANDE JOURNALISTIK

Lärarens lösning

BEDÖMNINGSMATRIS OCH LÖSNINGSRIKTLINJER

- Scenarioanalys: En grävande journalist behöver extra skydd mot övervakning när hen undersöker känsliga företagshandlingar.
- Fokusfråga: Hur ger Dynamic MultiHop bättre integritet än routning via en enda server?
- Rekommenderad strategi och lösning: Dynamic MultiHop dirigerar trafiken via ingångs- och utgångsservrar i två länder, så att ingen enskild server kan exponera användaren.