Namn: _____ Datum: _____ Poäng: _____

Säkerhet hos ProtonVPN

En analys av ProtonVPN:s säkerhetsarkitektur, inklusive Secure Core-servrar, DNS-filtrering med NetShield, schweizisk integritetsjurisdiktion, granskade appar med öppen källkod och Stealth-protokollet.

LÄRANDEÖVERSIKT: SÄKERHET HOS PROTONVPN

ELEV
STUDENTSTATUS
Nätverksförsvararspåret

SÄKER
ANSLUTNINGSSTATUS
Skydda datapaket

AKTIV
LÄCKSKYDD
Skydd mot DNS- och IPv6-läckor

Välkommen! Det här aktivitetshäftet guidar dig genom Proton VPN-tjänstens säkerhetsarkitektur. Du utforskar Secure Core-servrar med dubbla hopp, DNS-blockering med NetShield, schweiziska integritetslagar och Stealth-obfuskering.

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/protonvpn/sakerhet/

Din inlärningsplan för ProtonVPN:s säkerhet

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

INSTRUKTIONER FÖR SÄKERHETSGUIDEN FÖR PROTONVPN

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om dubbelhoppsroutning med Secure Core och schweizisk integritetsstyrning. Avsluta med bonusaktiviteten Tänk snabbt.

DUBBELHOPPSARKITEKTUR I SECURE CORE OCH SCHWEIZISK INTEGRITETSJURISDIKTION

Proton VPN skyddar användartrafik med Proton-ägda Secure Core-servrar i Schweiz, Island och Sverige, granskade appar med öppen källkod och obfuskeringsprotokollet Stealth som är utformat för att kringgå djup paketinspektion.

(INTRODUKTION)

Proton VPN skyddar användartrafik med Proton-ägda Secure Core-servrar i Schweiz, Island och Sverige, granskade appar med öppen källkod och obfuskeringsprotokollet Stealth som är utformat för att kringgå djup paketinspektion.

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

Kontrollpunkt 1: Utmaning med flerval

1. Vilken typ av anläggningar rymmer Protons Secure Core-servrar?

- A) Virtuella maskiner i offentligt moln
- B) Platser med hög säkerhet
- C) Offentliga datacenter
- D) Delade rack

2. Vilket protokoll hjälper till att kringgå strikt statlig censur?

- A) PPTP
- B) Stealth-protokoll
- C) OpenVPN UDP
- D) IKEv2

3. Vad gör Proton VPN:s funktion NetShield?

- A) Speed Booster
- B) DNS-blockering av annonser och skadlig kod
- C) Molnlagring
- D) Portvidarebefordran

4. Under vilket lands integritetslagar verkar Proton AG?

- A) USA
- B) Storbritannien
- C) Schweiz
- D) Panama

5. Hur verifieras Proton VPN:s klientprogram av experter?

- A) Hemlig kod
- B) Granskningar av öppen källkod
- C) Proprietär licens
- D) Myndighetsgranskning

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Secure Core routar trafiken via integritetsvänliga länder innan den lämnar nätverket.

○ Sant ○ Falskt

7 Fråga 7

7. Schweiz är medlem i underrättelse- och övervakningsalliansen 14 Eyes.

○ Sant ○ Falskt

8 Fråga 8

8. NetShield blockerar annonser och skadliga domäner direkt på DNS-nivå.

○ Sant ○ Falskt

9 Fråga 9

9. Proton VPN:s appar har till 100 % öppen källkod och granskas offentligt.

○ Sant ○ Falskt

10 Fråga 10

10. Protokollet Stealth använder vanliga WireGuard-huvuden utan obfuskering.

○ Sant ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Multihop-routing via Proton-ägda servrar i integritetsvänliga länder kallas arkitekturen _____ .

2. För att slå ut djup paketinspektion och nätverksbrandväggar aktiverar användare läget _____ .

3. Skadliga domäner, spårare och annonsskript filtreras av DNS-funktionen _____ .

4. Proton säger att man enligt _____ inte är skyldig att spara loggar över användarnas aktivitet.

5. Om VPN-tunneln oväntat kopplas ned blockeras internettrafiken av skyddet _____ .

6. Oberoende säkerhetsforskare verifierar klientens integritet eftersom apparna har _____ .

ORDBANK

AES-GCM | KILL SWITCH | NETSHIELD | SCHWEIZISK LAG | SECURE CORE | STEALTH | WIREGUARD | ÖPPEN KÄLLKOD

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av VPN- och nätverksbegrepp

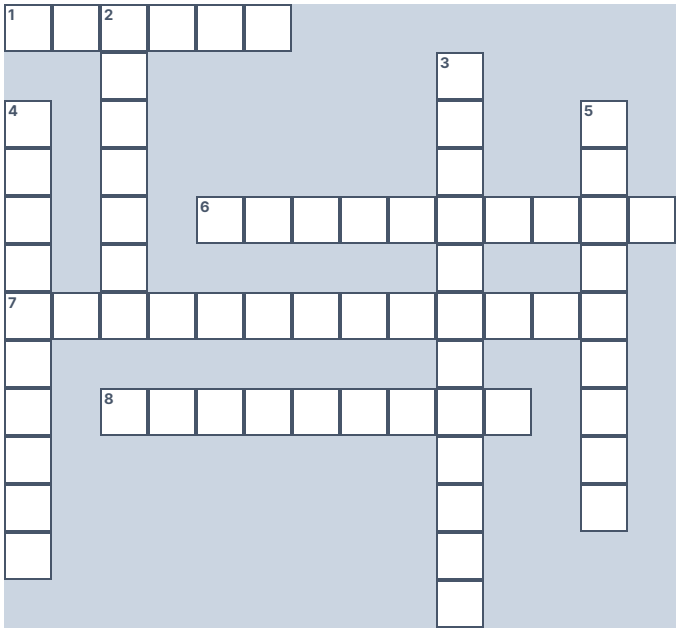
MATCHNING AV DEFINITIONER

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

☐	1. SECURE CORE	A	Klientprogramvara som är offentligt tillgänglig och oberoende granskad.
☐	2. STEALTH	B	Standard för symmetriska chiffer som krypterar VPN-tjänstens datapaket.
☐	3. NETSHIELD	C	Strikta juridiska integritetsregler i Schweiz utanför 14 Eyes-jurisdiktionen.
☐	4. SCHWEIZISK LAG	D	Ett förvrängt tunnlingsprotokoll som maskeras som vanlig HTTPS-webbtrafik.
☐	5. KILL SWITCH	E	Ett modernt lättviktigt protokoll med robust kryptografi och höga hastigheter.
☐	6. ÖPPEN KÄLLKOD	F	Ett DNS-baserat filter som blockerar annonser, telemetrispårare och skadlig kod.
☐	7. WIREGUARD	G	En multihop-design som dirigerar trafiken via servrar som ägs av Proton som första hopp.
☐	8. AES-GCM	H	Ett säkerhetsskydd som stoppar nätverksöverföring när anslutningen bryts.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

1. Militärklassad symmetrisk kryptering som skyddar alla inkapslade VPN-datapaket (6)

6. Multihop-design som dirigerar trafiken via Proton-ägda servrar som första hopp (10)

7. Strikta juridiska integritetsregler i Schweiz, utanför 14 Eyes-jurisdiktion (13)

8. Ett DNS-baserat filter som blockerar annonser, spårare för telemetri och skadlig kod (9)

LODRÄTT

2. Ett förvrängt tunnelprotokoll som ser ut som vanlig HTTPS-webbtrafik (7)

3. Klientprogram som är offentligt tillgängligt och oberoende granskat (12)

4. Ett skydd som stoppar nätverksöverföring vid avbrutna anslutningar (10)

5. Ett modernt, lättviktigt protokoll med robust kryptografi och hög hastighet (9)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

1 vågrätt: Militärklassad symmetrisk kryptering som skyddar alla inkapslade VPN-datapaket (6 bokstäver):

6 vågrätt: Multihop-design som dirigerar trafiken via Proton-ägda servrar som första hopp (10 bokstäver):

7 vågrätt: Strikta juridiska integritetsregler i Schweiz, utanför 14 Eyes-jurisdiktion (13 bokstäver):

8 vågrätt: Ett DNS-baserat filter som blockerar annonser, spårare för telemetri och skadlig kod (9 bokstäver):

LODRÄTT

2 lodrätt: Ett förvrängt tunnelprotokoll som ser ut som vanlig HTTPS-webbtrafik (7 bokstäver):

3 lodrätt: Klientprogram som är offentligt tillgängligt och oberoende granskat (12 bokstäver):

4 lodrätt: Ett skydd som stoppar nätverksöverföring vid avbrutna anslutningar (10 bokstäver):

5 lodrätt: Ett modernt, lättviktigt protokoll med robust kryptografi och hög hastighet (9 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

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

ORDLISTA

SECURECORE STEALTH NETSHIELD SCHWEIZISKLAG KILLSWITCH
ÖPPENKÄLLKOD WIREGUARD AESGCM

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. SECURECORE**
- **B. STEALTH**
- **C. NETSHIELD**
- **D. SCHWEIZISKLAG**
- **E. KILLSWITCH**
- **F. ÖPPENKÄLLKOD**
- **G. WIREGUARD**
- **H. AESGCM**

DEFINITIONER OCH MATCHNINGSFÄLT

_____ 1. Ett förvrängt tunnelprotokoll som ser ut som vanlig HTTPS-webbtrafik.

_____ 2. Ett modernt, lättviktigt protokoll med robust kryptografi och hög hastighet.

_____ 3. Strikta juridiska integritetsregler i Schweiz, utanför 14 Eyes-jurisdiktion.

_____ 4. Multihop-design som dirigerar trafiken via Proton-ägda servrar som första hopp.

_____ 5. Militärklassad symmetrisk kryptering som skyddar alla inkapslade VPN-datapaket.

_____ 6. Ett skydd som stoppar nätverksöverföring vid avbrutna anslutningar.

_____ 7. Ett DNS-baserat filter som blockerar annonser, spårare för telemetri och skadlig kod.

_____ 8. Klientprogram som är offentligt tillgängligt och oberoende granskat.

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. RCERESOEUC
2. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. EKZILHASSCI GW
7. LLNÖPÄDKOP KE
8. SMACGE

Bonusaktivitet: Tänk snabbt

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

1	Saker du gör på nätet varje dag			
2	Länder som är kända för starka integritetslagar			
3	Säkerhetsfunktioner i Proton VPN			
4	Typer av VPN-läckor			
5	Situationer där en kill switch hjälper			
6	Saker som en granskning kan kontrollera			
7	Inställningar du slår på för extra säkerhet			
8	Saker som kryptering skyddar			
9	Ord som beskriver en bra VPN-app			
10	Skäl till att välja Proton VPN			
11	Knappar eller menyer i en VPN-app			
12	Streamingtjänster du tittar på			
13	Hot på offentligt wifi			
14	Sätt att skapa ett starkt lösenord			
15	Länder där du skulle vilja ha Proton VPN-servrar			

Kontrollpunkt 8: Fallstudier om VPN och nätverk

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

FALLSTUDIE 1: KRINGGÅ RESTRIKTIVA BRANDVÄGGAR



Scenario: En användare reser till ett land där vanlig VPN-trafik som OpenVPN och WireGuard blockeras med DPI.

Diskussionsfråga: Vilken protokollkonfiguration i Proton VPN gör att användaren kan kringgå inspektion på statlig nivå?

FALLSTUDIE 2: AVANCERAT SKYDD MOT MOTSTÅNDARE



Scenario: En finansrevisor misstänker att den lokala internetleverantörens utgångsnod kan vara komprometterad av avancerade ihållande hot.

Diskussionsfråga: Hur skyddar Secure Core revisorns identitet mot en komprometterad utgångsnod?

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	5	3	21	18	5		3	15	18	5		8	28	18	4	1	4	5
19	5	18	22	18	1	18		19	11	25	4	4	1	18				
1	14	22	28	14	4	1	18	4	1	20	1							

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 Proton VPN Secure Core?

Secure Core routar trafiken via flera servrar i integritetsvänliga länder innan den lämnar nätverket.

Q2: Vad är protokollet Stealth?

Stealth är ett obfuskerat protokoll som döljer VPN-anslutningar som vanlig TLS/HTTPS-trafik.

Q3: Hur skyddar NetShield användare?

NetShield är ett DNS-baserat verktyg som automatiskt blockerar annons-, spårnings- och skadekoddomäner.

Q4: Är Proton VPN juridiskt skyddat i Schweiz?

Ja, Schweiz har strikta integritetslagar och ligger utanför jurisdiktionen för USA och EU/14 Eyes. [4]

Q5: Är Proton VPN:s appar öppen källkod?

Ja. Proton VPN:s appar är öppen källkod och har genomgått publicerade säkerhetsgranskningar.

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

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

Q6: Vilka krypteringschiffer används?

Proton VPN använder AES-256-GCM eller ChaCha20-Poly1305 med HMAC-SHA384 och RSA-4096-handskakningar.

Q7: Har Proton VPN en kill switch?

Ja, Proton VPN har en vanlig kill switch och en Permanent Kill Switch för att förhindra okrypterade läckor.

Q8: Kan Proton VPN läcka DNS-frågor?

Nej, alla DNS-frågor dirigeras via krypterade privata DNS-servrar som ägs av Proton.

Q9: Sparar Proton VPN anslutningsloggar?

Nej, Proton VPN tillämpar en strikt no-logs-policy, bekräftad av årliga granskningar från Securitum. [3]

Q10: Är Proton VPN sårbart för WebRTC-läckor?

Nej, Proton-klienter har inbyggda brandväggsregler och routingpolicyer som blockerar WebRTC-läckor.

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

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

Q1: Var ligger Secure Core-datacentren fysiskt?

De finns i Schweiz, på en före detta militärbas på Island och på en underjordisk plats i Sverige. [1]

Q2: Hur fungerar Perfect Forward Secrecy i Proton VPN?

En unik tillfällig krypteringsnyckel genereras för varje session, vilket förhindrar retroaktiv dekryptering.

Q3: Vad är Permanent Kill Switch i Windows/Linux?

Permanent Kill Switch blockerar all nätverkstrafik även om VPN-appen är helt stängd eller kraschar.

Q4: Stöder Proton VPN IPv6-routning och skydd mot läckor?

Proton VPN routar IPv6-trafik helt genom tunnlarna eller inaktiverar den på ett säkert sätt för att förhindra läckor.

Q5: Hur hanterar NetShields DNS-filtrering HTTPS-inspektion?

NetShield arbetar enbart i DNS-uppslagslagret utan att kräva ingripande TLS-dekryptering.

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

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

Q6: Vem utförde Proton VPN:s kodgranskningar från tredje part?

SEC Consult granskade apparna, och Securitum granskar apparna och policyn utan loggning.

Q7: Hur står sig Stealth-protokollet mot OpenVPN XOR eller Shadowsocks?

Stealth tunnlar WireGuard över obfuskerad TLS och presterar bättre än äldre OpenVPN-baserad obfuskering. [5]

Q8: Kan schweiziska myndigheter tvinga Proton VPN att logga trafik?

Proton uppger att företaget enligt schweizisk lag inte är skyldigt att spara loggar över användaraktivitet eller data.

Q9: Hur skyddas Proton VPN:s servrar mot beslag?

Alla Proton VPN-servrar är bare-metal-maskiner skyddade med fulldiskkryptering. [2]

Q10: Stöder Proton VPN konfigurationer med egna DNS-servrar?

Ja, betalande prenumeranter kan konfigurera egna uppströms DNS-servrar direkt i appens inställningar.

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. Proton äger och installerar själv sina Secure Core-servrar på högsäkra platser i Schweiz, Island och Sverige. [1]

2. VPN-INSIKT

2. Proton VPN:s klientappar har öppen källkod och genomgår återkommande kodgranskningar av tredje part.

3. VPN-INSIKT

3. Stealth-förvrängningsprotokollet kringgår djup paketinspektion genom att simulera vanlig TLS-trafik.

4. VPN-INSIKT

4. Schweiz står utanför de internationella underrättelsesamarbetena 5 Eyes, 9 Eyes och 14 Eyes. [4]

5. VPN-INSIKT

5. NetShield arbetar på DNS-upplösarnivå och förhindrar annonser och skadlig kod innan nyttolasten laddas ned.

6. VPN-INSIKT

6. Perfect Forward Secrecy säkerställer att kompromitterade nycklar inte kan dekryptera tidigare infångade trafiksessioner. [7]

7. VPN-INSIKT

7. Proton VPN använder fulldiskkryptering på bare-metal-servrar för att skydda serverkonfigurationer. [2]

8. VPN-INSIKT

8. Permanent Kill Switch förhindrar läckor av okrypterad data även vid omstart av operativsystemet.

9. VPN-INSIKT

9. Securitum har granskat och bekräftat Proton VPN:s policy om ingen loggning i fem årliga granskningar i följd. [3]

10. VPN-INSIKT

10. Proton VPN utvecklades av forskare som träffades på CERN (Europeiska organisationen för kärnforskning). [4]

Tekniska referenser och källor

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

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[1] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

Facit: Kontrollpunkt 1 – Flerval

1 **Fråga 1** Rätt svar: B

ANTECKNING FÖR LÄRAREN

Secure Core-servrar finns på platser med hög säkerhet, bland annat en tidigare militärbas på Island och ett underjordiskt datacenter i Sverige.

2 **Stealth-obfuskeringsprotokoll** CENSURFÖRSVAR Rätt svar: B

ANTECKNING FÖR LÄRAREN

Protons Stealth-protokoll förklär WireGuard-anslutningar som vanlig TLS/HTTPS-trafik för att kringgå brandväggar med djup paketinspektion (DPI). Källa: Proton Stealth Protocol Whitepaper.

3 **NetShield DNS-annonsblockerare** DNS-FILTRERING Rätt svar: B

ANTECKNING FÖR LÄRAREN

NetShield använder filtrering på DNS-nivå för att blockera domäner med skadlig kod, spionprogram, påträngande annonser och telemetrispårare innan webbsidor laddas. Källa: NetShield Security Specs.

4 **Schweizisk rättslig jurisdiktion** JURISDIKTION Rätt svar: C

ANTECKNING FÖR LÄRAREN

Proton AG har sitt huvudkontor i Genève i Schweiz och drar nytta av starka schweiziska integritetslagar utanför USA:s och EU:s övervakningsallianser 14 Eyes. Källa: Swiss Federal Data Protection Act.

5 **Fråga 5** Rätt svar: B

ANTECKNING FÖR LÄRAREN

Alla Proton VPN-appar har öppen källkod; SEC Consult och senare Securitum har granskat dem.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Secure Core med flera jurisdiktioner** ROUTNINGSARKITEKTUR Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Secure Core routar trafiken via integritetsstarka jurisdiktioner innan den lämnar nätverket till målet, vilket kan skydda mot en kompromitterad utgångsserver. Källa: Secure Core Architecture.

7 **Schweiziska övervakningsalliansen** ÖVERVAKNINGSALLIANSER Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Schweiz är inte medlem i avtalen om underrättelsedelning 5 Eyes, 9 Eyes eller 14 Eyes, vilket bevarar en självständig rättslig suveränitet. Källa: International Surveillance Treaties.

8 **Fråga 8** Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

NetShield använder Protons DNS-servrar för att kontrollera domäner mot listor över kända annons-, spårnings- och skadekodsdomäner.

9 **Granskning av klienter med öppen källkod** SÄKERHETSTRANSPARENS Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Proton har gjort sina appar för dator och mobil till öppen källkod och publicerar granskningsrapporter från tredje part. Källa: SEC Consult Security Report.

10 **Fråga 10** Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: Stealth tunnlar WireGuard inuti obfuskerad TLS över TCP så att trafiken ser ut som vanlig HTTPS.

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

G 1. SECURE CORE	D 2. STEALTH	F 3. NETSHIELD	C 4. SCHWEIZISK LAG
H 5. KILL SWITCH	A 6. ÖPPEN KÄLLKOD	E 7. WIREGUARD	B 8. AES-GCM

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 SCHWEIZISK LAG
5 KILL SWITCH	6 ÖPPEN KÄLLKOD		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 B – STEALTH	2 G – WIREGUARD	3 D – SCHWEIZISKLAG	4 A – SECURECORE
5 H – AESGCM	6 E – KILLSWITCH	7 C – NETSHIELD	8 F – ÖPPENKÄLLKOD

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara SECURE CORE, STEALTH och NETSHIELD med egna ord och ge ett exempel på varje.

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

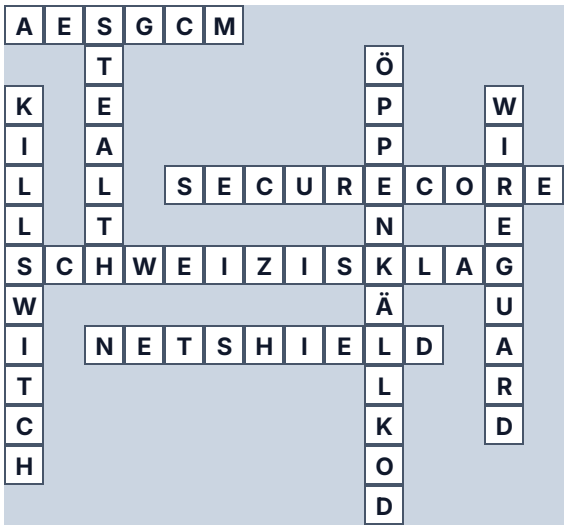
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

1 vågrätt: AESGCM Militärklassad symmetrisk kryptering som skyddar alla inkapslade VPN-datapaket (6 bokstäver)

6 vågrätt: SECURECORE Multihop-design som dirigerar trafiken via Proton-ägda servrar som första hopp (10 bokstäver)

7 vågrätt: SCHWEIZISKLAG Strikta juridiska integritetsregler i Schweiz, utanför 14 Eyes-jurisdiktion (13 bokstäver)

8 vågrätt: NETSHIELD Ett DNS-baserat filter som blockerar annonser, spårare för telemetri och skadlig kod (9 bokstäver)

LODRÄTT

2 lodrätt: STEALTH Ett förvrängt tunnelprotokoll som ser ut som vanlig HTTPS-webbtrafik (7 bokstäver)

3 lodrätt: ÖPPENKÄLLKOD Klientprogram som är offentligt tillgängligt och oberoende granskat (12 bokstäver)

4 lodrätt: KILLSWITCH Ett skydd som stoppar nätverksöverföring vid avbrutna anslutningar (10 bokstäver)

5 lodrätt: WIREGUARD Ett modernt, lättviktigt protokoll med robust kryptografi och hög hastighet (9 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. RCERESOEUC	SECURECORE	5. LHAESTT	STEALTH
2. DNLSEIEHT	NETSHIELD	6. EKZILHASSCIGW	SCHWEIZISKLAG
3. KWCIISHLTL	KILLSWITCH	7. LLNÖPÄDKOPKE	ÖPPENKÄLLKOD
4. GDREAUWIR	WIREGUARD	8. SMACGE	AESGCM

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"SECURE CORE HÄRDADE SERVRAR SKYDDAR ANVÄNDARDATA"

Facit till fallstudierna

A FALLSTUDIE 1: KRINGGÅ RESTRIKTIVA BRANDVÄGGAR

Lärarens lösning

BEDÖMNINGSMATRIS OCH LÖSNINGSRIKTLINJER

- Scenarioanalys: En användare reser till ett land där vanlig VPN-trafik som OpenVPN och WireGuard blockeras med DPI.
- Fokusfråga: Vilken protokollkonfiguration i Proton VPN gör att användaren kan kringgå granskning på statlig nivå?
- Rekommenderad strategi och lösning: Användaren bör aktivera protokollet Stealth, som döljer VPN-paketens huvuden som vanlig TLS-/HTTPS-webbtrafik och slinker förbi DPI-filter.

B FALLSTUDIE 2: AVANCERAT SKYDD MOT MOTSTÅNDARE

Lärarens lösning

BEDÖMNINGSMATRIS OCH LÖSNINGSRIKTLINJER

- Scenarioanalys: En finansrevisor misstänker att den lokala internetleverantörens utgångsnod kan vara komprometterad av avancerade ihållande hot (APT).
- Fokusfråga: Hur skyddar Secure Core revisorns identitet om en utgångsnod kompromet teras?
- Rekommenderad strategi och lösning: Secure Core dirigerar trafiken först via Proton-ägda servrar i Schweiz, Island eller Sverige, så att en komprometterad utgångsserver inte kan spåra användarens IP-adress.