Namn: _____ Datum: _____ Poäng: _____

Så döljer du din IP-adress Arbetsblad

Dölja IP-adresser, maskera plats, proxy, Tor och förhindra DNS-/WebRTC-läckor

LÄRANDEÖVERSIKT OM VPN

ELEV
STUDENTSTATUS
Nätverksförsvararspåret

SÄKER
ANSLUTNINGSSTATUS
Skydda datapaket

AKTIV
LÄCKSKYDD
Skydd mot DNS- och IPv6-läckor

Välkommen! Det här aktivitetshäftet guidar dig genom grundläggande principer för virtuella privata nätverk (VPN). Du utforskar hur krypterade tunnlar skyddar dina data, hur nätverksprotokoll fungerar och hur du identifierar och åtgärdar integritetsläckor.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska VPN-begrepp och protokoll.**
- [ ] **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 VPN-guide

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

Din inlärningsplan för VPN

- Förklara hur IP-adresser fungerar och hur de läcker platser.
- Jämför proxyer, Tor och VPN för att dölja nätverksadresser.
- Identifiera metoder för att upptäcka och förhindra DNS- och WebRTC-läckor.
- Förstå hur webbplatser spårar användare via deras publika IP-adress.
- Utvärdera multi-hop-routning och krypterade tunnlar för IP-skydd.

INSTRUKTIONER FÖR ARBETSBLAD OM IP-SKYDD

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om att dölja din IP-adress och förhindra läckor. Avsluta med bonusaktiviteten Tänk snabbt.

DÖLJ DIN IP-ADRESS (INTRODUKTION)

Din IP-adress är en digital postadress som avslöjar din fysiska plats och dina nätvanor. Att dölja din IP-adress är det första försvaret mot spårning på nätet, målprofilering och geografisk blockering. Att förstå hur du säkert maskerar din adress hjälper dig att skydda din integritet online.

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

Kontrollpunkt 1: Utmaning med flerval

1. Vad avslöjar en enhets offentliga IP-adress för de webbplatser du besöker?

- A. Användarens kreditkortsnummer
- B. Din ungefärliga plats och namnet på din internetleverantör
- C. Hela den lokala filkatalogen
- D. Tangentbordets språkinställningar

2. Vilken metod döljer din IP-adress och krypterar all trafik i hela systemet?

- A. En vanlig webbproxy
- B. Att rensa webbläsarens cookies
- C. Ett virtuellt privat nätverk (VPN)
- D. Att inaktivera din egen brandvägg

3. Vad är en stor integritetsbegränsning med att använda en gratis webbproxy?

- A. Den krypterar inte datatrafik i offentliga nätverk
- B. Den kräver att ett externt operativsystem installeras
- C. Den är helt olaglig i USA
- D. Den kräver en dedikerad telefonlinje

4. Hur ger nätverket Tor hög anonymitet åt användare?

- A. Genom att öka anslutningshastigheterna
- B. Genom att dirigera trafiken via tre relän som drivs av frivilliga
- C. Genom att registrera ditt namn i en global databas
- D. Genom att begränsa åtkomsten till enbart statliga myndigheter

5. Vad är en DNS-läcka?

- A. Ett fel som skickar e-post till fel adress
- B. När DNS-förfrågningar går förbi VPN-tunneln och går till internetleverantören
- C. Ett maskinvarufel i den lokala routerns nätaggregat
- D. En uppdatering av drivrutinen för det lokala nätverkskortet

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. En proxyserver krypterar operativsystemets bakgrundstrafik precis som ett VPN.

- ○ Sant
- ○ Falskt

7 Fråga 7

7. Tor-routning är mycket säker men minskar surfhastigheten i nätverket.

- ○ Sant
- ○ Falskt

8 Fråga 8

8. WebRTC-läckor kan avslöja din verkliga IP-adress under en aktiv VPN-session.

- ○ Sant
- ○ Falskt

9 Fråga 9

9. Med ett VPN påslaget och utan läckor kan din internetleverantör inte se vilka webbplatser du besöker.

- ○ Sant
- ○ Falskt

10 Fråga 10

10. Att dölja din IP-adress blockerar spårning via webbläsarens fingeravtryck.

- ○ Sant
- ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. En förbigången säker tunnel som avslöjar dina domänfrågor kallas en _____ .

2. Webbläsarens API för realtidskommunikation, _____ , kan oavsiktligt läcka din verkliga IP-adress.

3. En _____ omdirigerar webbläsartrafik men krypterar inte paketens innehåll.

4. Den flerlagrade krypteringen i nätverket _____ ger hög anonymitet.

5. Din offentliga _____ tilldelas av din teleoperatör och avslöjar ditt område.

6. Att kringgå regionala mediablockeringar sker genom _____ av din plats.

ORDBANK

DNS-LÄCKA IP-ADRESS ISP-SPÅRNING KILL SWITCH MASKERING TOR WEBBPROXY WEBRTC

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av nätverksbegrepp

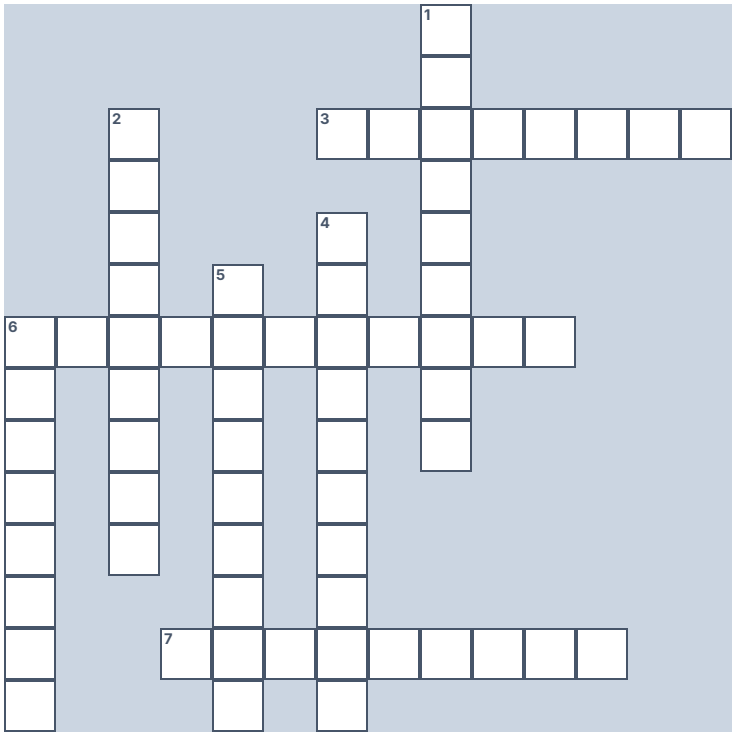
MATCHNING AV DEFINITIONER

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

☐	1. IP-adress	A	Krypterar all trafik från en enhet och dirigerar den via en VPN-server.
☐	2. VPN-tunnel	B	Dirigerar data genom tre frivilliga servrar och krypterar lager i varje steg.
☐	3. Tor-nätverket	C	Att dirigera anslutningen via en server i ett annat land för att kringgå geoblockering.
☐	4. Webbproxy	D	Unik numerisk etikett som identifierar ett enhetsgränssnitt på internet.
☐	5. DNS-läcka	E	Omdirigerar webbläsartrafik på applikationsnivå utan kryptering på systemnivå.
☐	6. WebRTC-API	F	Teleoperatörens loggning av målen för din okrypterade internettrafik.
☐	7. Platsmaskering	G	Frågor som löses utanför VPN-tunneln och därmed visar besökta domäner för internetleverantören.
☐	8. Spårning från internetleverantören	H	Webbläsarfunktion för röst/video som kan kringgå tunnlar och avslöja riktiga IP-adresser.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

3. Förfrågningar som löses utanför VPN-tunneln och avslöjar besökta domäner för internetleverantören (8)

6. Teleoperatörens loggning av mål för okrypterad internettrafik (11)

7. Webbläsarfunktion för röst och video som kan kringgå tunnlar och avslöja verkliga IP-adresser (9)

LODRÄTT

1. Att dirigera anslutningen via en server i ett annat land för att kringgå geoblockeringar (9)

2. Omdirigerar webbläsartrafik på applikationsnivå utan kryptering av systemet (9)

4. Dirigerar data via tre frivilliga servrar och krypterar lager för lager i varje steg (10)

5. Krypterar all trafik från en enhet och dirigerar den via en VPN-server (9)

6. Unik numerisk etikett som identifierar en enhets gränssnitt på internet (8)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

3 vågrätt: Förfrågningar som löses utanför VPN-tunneln och avslöjar besökta domäner för internetleverantören (8 bokstäver):

6 vågrätt: Teleoperatörens loggning av mål för okrypterad internettrafik (11 bokstäver):

7 vågrätt: Webbläsarfunktion för röst och video som kan kringgå tunnlar och avslöja verkliga IP-adresser (9 bokstäver):

LODRÄTT

1 lodrätt: Att dirigera anslutningen via en server i ett annat land för att kringgå geoblockeringar (9 bokstäver):

2 lodrätt: Omdirigerar webbläsartrafik på applikationsnivå utan kryptering av systemet (9 bokstäver):

4 lodrätt: Dirigerar data via tre frivilliga servrar och krypterar lager för lager i varje steg (10 bokstäver):

5 lodrätt: Krypterar all trafik från en enhet och dirigerar den via en VPN-server (9 bokstäver):

6 lodrätt: Unik numerisk etikett som identifierar en enhets gränssnitt på internet (8 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 W A B C Q Å M L
Å A M Å W L E E S O M K E J O
K K O L S R H B O O A S T U W
R C V H C U S R Q I S U C Y E
E Ä V Ä X I C T Ö Y K G L V I
V L Ö D O S E C S Z E R C P W
T S B A Ö P P A W E R M A N E
Ä N Q E F S H P E I I J D T T
N D S N F P J I B P N U Ö U U
R G S Y F Å A A B A G S Q N O
O R W Å S R L T P D W U D N O
T Ä B G U N Z Z R R K A T E Ö
Ä Ä M H J I O T O E L N N L V
Q I S S H N Ö A X S Q X G X C
Ä T Ä B I G N Ö Y S H K P R P

ORDLISTA

IPADRESS, VPNTUNNEL, TORNÄTVERK, MASKERING, WEBBPROXY, ISPSPÅRNING, DNSLÄCKA, WEBRTCAPI

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. IPADRESS**
- **B. VPNTUNNEL**
- **C. TORNÄTVERK**
- **D. WEBBPROXY**
- **E. DNSLÄCKA**
- **F. WEBRTCAPI**
- **G. MASKERING**
- **H. ISPSPÅRNING**

DEFINITIONER OCH MATCHNINGSFÄLT

_____ 1. Omdirigerar webbläsartrafik på applikationsnivå utan kryptering av systemet.

_____ 2. Att dirigera anslutningen via en server i ett annat land för att kringgå geoblockeringar.

_____ 3. Webbläsarfunktion för röst och video som kan kringgå tunnlar och avslöja verkliga IP-adresser.

_____ 4. Unik numerisk etikett som identifierar en enhets gränssnitt på internet.

_____ 5. Dirigerar data via tre frivilliga servrar och krypterar lager för lager i varje steg.

_____ 6. Teleoperatörens loggning av mål för okrypterad internettrafik.

_____ 7. Förfrågningar som löses utanför VPN-tunneln och avslöjar besökta domäner för internetleverantören.

_____ 8. Krypterar all trafik från en enhet och dirigerar den via en VPN-server.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga VPN-begrepp och termer. Skriv dina svar i de ifyllbara rutorna.

1. SDRIEPSA
2. RNTOÄKVETR
3. LNDÄCAKS
4. EGNKIRMAS
5. NUPLNTVEN
6. XBEORWPYB
7. CWPIARETB
8. IRGÅPIPSNNS

Bonusaktivitet: Tänk snabbt

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

1	Skäl till att använda ett VPN under resor			
2	Webbläsare du känner till			
3	Saker som ett VPN kan dölja			
4	Ord som hör ihop med integritet			
5	Ord från det här arbetsbladet som du vill komma ihåg			
6	Saker som en webbplats kan gissa utifrån din IP-adress			
7	Siffror eller tecken i en IP-adress			
8	Myter om VPN			
9	VPN-tjänster du känner till			
10	Saker som din internetleverantör kan se			
11	Löften som en bra VPN-leverantör ger			
12	Saker som kan läcka din verkliga IP-adress			
13	Skäl till att dölja din plats			
14	Sätt att dölja din IP-adress			
15	Enheter som kan använda ett VPN			

Kontrollpunkt 8: Fallstudier om VPN

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

SARAH (STUDENT PÅ KAFÉ)

👷 "Hej! Jag sitter på Coffee & Bytes. Det finns ett osäkrat offentligt nätverk som heter 'Free_Wi-Fi_No_Password'. Jag vill logga in på min skolmejl och ladda upp min uppgift, men jag är orolig för hackare. Vilka risker finns med att använda det här nätverket utan VPN, och hur skyddar ett VPN mina data?"

ALEX (RESANDE STUDENT)

👷 "Åh nej! Jag reser utomlands för ett projekt och försöker titta på en biologidokumentär som finns på en server i mitt hemland. Men webbplatsen säger 'Den här videon är inte tillgänglig på din nuvarande plats.' Varför är jag blockerad, och hur kan ett VPN hjälpa mig att titta på den?"

Kontrollpunkt 9: Knäck chiffret

För att slutföra din träning i IP-maskering ska du dekryptera det här hemliga meddelandet om hur du döljer dina digitala spår.

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

4 15 12 10 4 9 14 1 4 18 5 19 19 13 5 4

5 20 20 4 15 12 20 19 25 19 20 5 13

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 som presumtiva kunder har om att använda virtuella privata nätverk.

Q1: Vad är ett VPN och hur fungerar det?

Ett virtuellt privat nätverk (VPN) krypterar din internetanslutning och dirigerar din trafik via en säker fjärrserver. Det döljer din publika IP-adress och begränsar vad lokala nätverksobservatörer och din internetleverantör kan se av trafik som dirigeras genom VPN-tunneln.

Q2: Varför ska jag använda ett VPN?

Ett VPN skyddar din digitala integritet, skyddar din anslutning på offentliga Wi-Fi-nätverk (som på kaféer eller flygplatser), kan minska aktivitetsbaserad strypning när internetleverantören inte kan identifiera typen av krypterad trafik, kringgår geografiska begränsningar för att nå globalt innehåll och hjälper till att skydda resurser vid distansarbete.

Q3: Gör ett VPN mig helt anonym online?

Nej. En VPN döljer din IP-adress och krypterar trafiken, men du kan ändå spåras via webbläsarens cookies, aktiva konton (som Google eller Facebook), webbläsarens fingeravtryck eller om din VPN-leverantör loggar dina data.

Q4: Döljer en webbproxy min IP-adress?

Ja, men bara för trafik som skickas genom den, vanligtvis din webbläsare. De flesta webbproxyer krypterar inte din data, så din internetleverantör eller nätverksoperatören kan fortfarande se vad du skickar och tar emot.

Q5: Är det lagligt att dölja min IP-adress?

I många länder, ja, men vissa begränsar eller förbjuder VPN och andra verktyg som används för att dölja en IP-adress. Att dölja din IP-adress gör aldrig en olaglig handling laglig, så kontrollera lokala lagar innan du använder ett.

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

Gå igenom de vanligaste frågorna och svaren som presumtiva kunder har om att använda virtuella privata nätverk.

Q6: Döljer Tor min IP-adress?

Ja. Tor skickar din trafik via tre frivilliga reläer (guard, middle och exit), så webbplatser ser exitreläets adress, och inget enskilt relä vet både vem du är och vart du går. [1]

Q7: Vad avslöjar min IP-adress?

Din publika IP-adress avslöjar vanligtvis din internetleverantör och en ungefärlig plats, till exempel ditt land eller din stad. Webbplatser kan också använda den för att koppla ihop dina besök och tillämpa geoblockering.

Q8: Hur kontrollerar jag att det är dolt?

Anslut till din VPN, besök sedan en webbplats som kontrollerar IP-adresser och kör DNS- och WebRTC-läckagetest. IP-adressen och DNS-servrarna som visas ska tillhöra VPN:en, inte din ISP. Om din verkliga IP-adress syns, aktivera läckageskydd.

Q9: Kan jag använda ett VPN på min mobil och smart-TV?

Ja. Moderna VPN-leverantörer erbjuder egna appar för iOS, Android, macOS, Windows, Linux och smart-TV, samt routerlösningar som skyddar alla enheter i ditt hemnätverk.

Q10: Vad är en Kill Switch?

En kill switch är en säkerhetsfunktion som automatiskt kopplar bort din enhet från internet om VPN-anslutningen bryts. Det förhindrar att din okrypterade data eller verkliga IP-adress läcker ut.

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

Utforska tekniska och strukturella aspekter av virtuella privata nätverk och säkra tunnelprotokoll.

Q1: Varför kan webbplatser fortfarande spåra mig efter att jag dolt min IP-adress?

Att dölja din IP-adress stoppar inte webbläsarens fingeravtryck. Spårare kan kombinera uppgifter som din skärmupplösning, installerade typsnitt och webbläsarinställningar till en identifierare, och cookies eller inloggade konton kan också identifiera dig, så använd även en integritetsfokuserad webbläsare. [3]

Q2: Vad är dubbel VPN- eller multihop-routning?

Multi-hop dirigerar din trafik genom två eller flera VPN-servrar i följd. Det lägger till ett andra lager av kryptering och hjälper till att hålla din riktiga IP-adress dold för det andra hoppet om en server komprometteras.

Q3: Vad läcker WebRTC och hur förhindrar ett VPN det?

WebRTC är ett webbläsarprotokoll som kan avslöja dina verkliga lokala och offentliga IP-adresser även när en VPN är aktiv. Premium-VPN-tjänster blockerar eller förfalskar WebRTC-förfrågningar i sina appar för dator och mobil samt i webbläsartilläggen.

Q4: Kan IPv6-trafik läcka min verkliga IP-adress?

Ja, om ditt VPN bara tunnlar IPv4. Din enhet kan då skicka IPv6-trafik utanför tunneln och avslöja en adress som tilldelats av din internetleverantör. Använd ett VPN som tunnlar eller blockerar IPv6 och bekräfta det med ett IPv6-läckagetest.

Q5: Hur kringgår obfuskering VPN-blockeringar?

Obfuskering (eller "stealth-VPN") förklär VPN-trafikens paket så att de ser ut som vanlig HTTPS-webbtrafik (port 443). Det hjälper till att ta sig förbi djup paketinspektion (DPI) som regeringar eller skol- och kontorsnätverk använder för att blockera VPN.

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

Utforska tekniska och strukturella aspekter av virtuella privata nätverk och säkra tunnelprotokoll.

Q6: Avslöjar delad tunnel (split tunneling) min verkliga IP-adress?

Ja, för de appar du undantar. Trafik som skickas utanför tunneln använder din riktiga IP-adress, och RFC 8828 anger att WebRTC kan avslöja internetleverantörens adress under ett VPN med delad tunnel om inte webbläsaren begränsar det. [2]

Q7: Vad är en delad IP-adress och hur hjälper den integriteten?

Med en delad IP-adress syns många VPN-användare online med samma adress samtidigt. Det gör det mycket svårare för en webbplats att koppla ett enskilt besök till dig än med en dedikerad IP-adress som bara du använder.

Q8: Kan min internetleverantör se att jag använder ett VPN för att dölja min IP-adress?

Vanligtvis ja. Din ISP kan se att du ansluter till en VPN-servers IP-adress, när du ansluter och hur mycket data du skickar, men inte vilka webbplatser du besöker eller innehållet inuti den krypterade tunneln.

Q9: Vad är skydd mot DNS-läckor?

DNS-läckskydd tvingar din enhet att skicka webbplatsers uppslagsfrågor (DNS-frågor) via VPN-tjänstens privata, krypterade DNS-servrar i stället för din ISP:s servrar. Det hindrar din ISP från att spåra vilka webbplatser du besöker.

Q10: Är en proxy eller ett VPN bättre för att dölja min IP-adress?

Ett VPN är oftast bättre. Det döljer din IP-adress för varje app på enheten och krypterar trafiken, medan en webbproxy vanligtvis bara täcker webbläsaren och ofta saknar kryptering.

Del 11: 10 intressanta fakta om VPN och insikter från verkligheten

Gå igenom dessa mycket värdefulla, verkliga fakta och insikter om VPN-teknikens historia, marknad och teknik.

1. FÖRSTA VPN-PROTOKOLLET

PPTP (Point-to-Point Tunneling Protocol), ett tidigt VPN-protokoll från en Microsoft-ledd grupp på 1990-talet, anses nu osäkert, så moderna VPN-tjänster använder WireGuard eller OpenVPN.

2. FINGERAVTRYCKSTAGNING

Att dölja din IP-adress stoppar inte webbläsarens fingeravtryck, som kan identifiera dig utifrån uppgifter som skärmupplösning och installerade typsnitt. [3]

3. WIREGUARD-REVOLUTIONEN

WireGuard har en mycket strömlinjeformad kodbas som är utformad för effektivitet, vilket gör det lättare att granska för säkerhetsbrister än traditionella protokoll.

4. EXPONERING AV WEBRTC-ADRESS

RFC 8828 varnar för att WebRTC kan avslöja både ett VPN:s publika adress och den internetleverantörsadress som VPN:et körs över, om inte webbläsaren begränsar det. [2]

5. 5 EYES-ALLIANSENS URSPRUNG

Underrättelsesamarbetet Five Eyes mellan USA, Storbritannien, Kanada, Australien och Nya Zeeland växte fram ur de allierades samarbete kring signalspaning under andra världskriget.

6. DJUP PAKETINSPEKTION

Avancerade brandväggar använder Deep Packet Inspection (DPI) för att analysera nätverkspakets metadata och blockera typiska kännetecken hos VPN-anslutningar.

7. ÅTERANVÄNDNING AV TOR-KRETS

Tor återanvänder samma krets i ungefär tio minuter och bygger sedan en ny, vilket gör det svårare att koppla ihop din surfaktivitet. [1]

8. DECENTRALISERADE VPN

Decentraliserade VPN (dVPN) fördelar trafiken över ett nätverk av noder som drivs av andra användare, vilket minskar beroendet av en enda central leverantör.

9. ANONYMITET MED TOR MOT VPN

Ett VPN tunnlar trafiken genom en enda leverantör, medan Tor (The Onion Router) skickar trafiken genom tre frivilliga reläer (guard, middle, exit) för att maximera integriteten. [1]

10. PROXYER VS. VPN-TUNNLAR

En webbproxy ändrar den IP-adress som en webbplats ser för din webbläsartrafik, men till skillnad från ett VPN krypterar den vanligtvis inte trafiken och täcker inte andra appar på din enhet. [5]

Tekniska referenser och källor

Citerade publikationer, kryptografiska specifikationer och officiella dokumentstandarder som används i detta arbetsblad.

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[1] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

Facit: Dölja IP-adresser, platsmaskering, proxy, Tor och förhindra DNS-/WebRTC-läckor

1 Fråga 1

Rätt svar: B

ANTECKNING FÖR LÄRAREN

Vad avslöjar en enhets offentliga IP-adress för de webbplatser du besöker? → Din ungefärliga plats och namnet på din internetleverantör

2 VPN-systemkryptering LATENS

Rätt svar: C

ANTECKNING FÖR LÄRAREN

Till skillnad från proxyer som bara omdirigerar webbläsartrafik skapar ett VPN en krypterad tunnel för hela systemet och skyddar bakgrundsprogram, spel och operativsystemets förfrågningar. Källa: Tor Project Relays, W3C WebRTC API.

3 Proxyers brist på kryptering WI-FI-SÄKERHET

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Webbproxyer vidarebefordrar bara webbläsartrafik utan att kryptera paketens innehåll, vilket innebär att nätverksoperatören eller din internetleverantör fortfarande kan spåra ditt innehåll. Källa: IETF Proxy Vulnerabilities.

4 Fråga 4

Rätt svar: B

ANTECKNING FÖR LÄRAREN

Hur ger nätverket Tor hög anonymitet åt användare? → Genom att dirigera trafiken via tre reläns som drivs av frivilliga

5 DNS-tunnelläckor INTEGRITET

Rätt svar: B

ANTECKNING FÖR LÄRAREN

En DNS-läcka uppstår när domännamnsförfrågningar kringgår VPN-tunneln och går direkt till din internetleverantörs resolvrar, vilket avslöjar poster över besökta domäner. Källhänvisning: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Detaljer om proxyns begränsningar** IP-MASKERING **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Proxyer fungerar på applikationslagret och saknar den systemomfattande integrationen med nätverksdrivrutiner som en VPN-tunnel har. Källa: IETF Proxy Vulnerabilities.

7 **Fråga 7** **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Att vidarebefordra trafik via tre relän som drivs av frivilliga med lagerkryptering ger högre latens, så Tor är vanligtvis långsammare än en direkt anslutning.

8 **Fråga 8** **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

WebRTC kan avslöja lokala adresser och, med vissa VPN-konfigurationer, den offentliga IP-adress som internetleverantören tilldelat under tunneln (RFC 8828).

9 **Fråga 9** **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Utan DNS- eller WebRTC-läckor ser internetleverantören bara krypterad trafik till VPN-servern, inte de webbplatser du besöker.

10 **Begränsningar för fingeravtryck** INGA LOGGAR **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Fingeravtryck riktar sig mot mått på enhetens konfiguration (skärmupplösning, teckensnitt, tillägg) som förblir synliga även när IP-adressen är dold. Källa: EFF Tracking Evasion.

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

D 1. IP-adress	A 2. VPN-tunnel	B 3. Tor-nätverket	E 4. Webbproxy
G 5. DNS-läcka	H 6. WebRTC-API	C 7. Platsmaskering	F 8. Spårning från internetleverantören

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 DNS-LÄCKA	2 WEBRTC	3 WEBBPROXY	4 TOR
5 IP-ADRESS	6 MASKERING		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 D – WEBBPROXY	2 G – MASKERING	3 F – WEBRTCAPI	4 A – IPADRESS
5 C – TORNÄTVERK	6 H – ISPSPÅRNING	7 E – DNSLÄCKA	8 B – VPNTUNNEL

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara IP-adress, VPN-tunnel och Tor-nätverket med egna ord och ge ett exempel på varje.

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

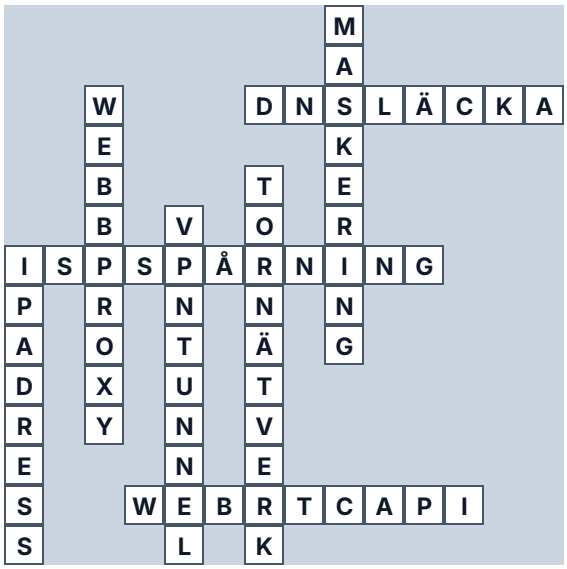
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

3 vågrätt: DNSLÄCKA Förfrågningar som löses utanför VPN-tunneln och avslöjar besökta domäner för internetleverantören (8 bokstäver)

6 vågrätt: ISPSPÅRNING Teleoperatörens loggning av mål för okrypterad internettrafik (11 bokstäver)

7 vågrätt: WEBRTCAPI Webbläsarfunktion för röst och video som kan kringgå tunnlar och avslöja verkliga IP-adresser (9 bokstäver)

LODRÄTT

1 lodrätt: MASKERING Att dirigera anslutningen via en server i ett annat land för att kringgå geoblockeringar (9 bokstäver)

2 lodrätt: WEBBPROXY Omdirigerar webbläsartrafik på applikationsnivå utan kryptering av systemet (9 bokstäver)

4 lodrätt: TORNÄTVERK Dirigerar data via tre frivilliga servrar och krypterar lager för lager i varje steg (10 bokstäver)

5 lodrätt: VPNTUNNEL Krypterar all trafik från en enhet och dirigerar den via en VPN-server (9 bokstäver)

6 lodrätt: IPADRESS Unik numerisk etikett som identifierar en enhets gränssnitt på internet (8 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. SDRIEPSA	IPADRESS	5. NUPLNTVEN	VPNTUNNEL
2. RNTOÄKVETR	TORNÄTVERK	6. XBEORWPYB	WEBBPROXY
3. LNDÄCAKS	DNSLÄCKA	7. CWPIARETB	WEBRTCAPI
4. EGNKIRMAS	MASKERING	8. IRGÅPIPSNNS	ISPSPÅRNING

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"DOLJ DIN ADRESS MED ETT DOLT SYSTEM"

Facit till fallstudierna

A Scenario A: Säkerhet i offentliga nätverk

SNIFFNING OCH KRYPTERING | Sarahs dilemma

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Risker: Paketsniffning, avlyssning av data och man-in-the-middle-attacker. Någon på samma kafénätverk kan fånga hennes inloggningsuppgifter eller läxfil.
- VPN-skydd: Krypterar nyttolasten i nätverkspaketen, så att avlyssnad tunneltrafik blir oläslig för passiva snokare i det lokala nätverket när VPN är korrekt konfigurerat.

B Scenario B: Åtkomst till blockerade resurser

GEOBLOCKERING OCH IP-ADRESSER | Alex dilemma

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Varför blockerad: Streamingvärden använder geoblockering, som kopplar den resandes lokala IP-adress till hans fysiska land och blockerar den utifrån territoriella licenser.
- Så hjälper VPN: Genom att dölja hans verkliga plats genom att routa trafiken via en server i hans hemland. Webbplatsen ser hemlandets IP-adress, vilket ger åtkomst.