Namn: _____ Datum: _____ Poäng: _____

Vad är en VPN Arbetsblad

Praktiska övningar i nätverksprotokoll, tunnling och säkerhetskontroller.

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 begreppet datatunnling och inkapsling.
- Identifiera vanliga protokollkonfigurationer och krypteringsmetoder.
- Analysera servrars och IP-maskerings roll i virtuella privata nätverk.
- Förstå hur ISP:er spårar surfande och hur ett VPN förhindrar det.
- Skilj mellan de operativa gränserna för virtuell nätverkstopologi.

INSTRUKTIONER FÖR GUIDEN VAD ÄR EN VPN

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om verkliga scenarier i avsnittet med fallstudier. Avsluta med bonusaktiviteten Tänk snabbt.

VAD ÄR EN VPN? (INTRODUKTION)

Ett virtuellt privat nätverk är mer än bara en integritetsknapp. Det är en krypterad tunnel som dirigerar din internettrafik via en fjärrserver. Det döljer din IP-adress, hindrar din internetleverantör från att föra loggar över dina onlineaktiviteter och skyddar dina data i offentliga nätverk. Att förstå terminologin är avgörande för att hålla sig digitalt säker.

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

Kontrollpunkt 1: Utmaning med flerval

1. Vad är den främsta funktionen hos ett virtuellt privat nätverk (VPN)?

- A. Att öka webbläsarens renderingshastighet
- B. För att kryptera datapaket och dölja din offentliga IP-adress
- C. Att lagra webbplatsens cookiedatabaser lokalt
- D. För att ersätta din fysiska datorhårdvara

2. Vad är nätverkstunnelering i samband med en VPN?

- A. Att ta bort dubbla nätverksloggfiler
- B. Att installera lokala lagringsfiler för databaser
- C. Att dela filer med andra lokala datorer
- D. Att kapsla in ett nätverkspaket i ett annat säkert paket

3. Vilken krypteringsstandard används ofta för att skydda VPN-trafik?

- A. Äldre DES-kryptering
- B. Moderna standarden AES-256
- C. Klartextkodning med base64
- D. Vanlig chiffrering med rot13

4. Vilken del av din nätverkstrafik krypteras av en VPN?

- A. Endast utskriftsjobb i den lokala enhetens nätverk
- B. Ethernetkabelns fysiska dragning
- C. Hela datanyttolasten i nätverkspaketet
- D. Endast dina sökhistoriker i webbläsaren

5. Vad betyder begreppet ”kryptering” i nätverk?

- A. Att omvandla klartextdata till oläsbar chiffertext
- B. Att radera gamla kommunikationsposter
- C. Att öka dina lokala gränser för bandbreddshastighet
- D. Att dela nycklar till databasåtkomst offentligt

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Ett VPN krypterar din trafik för att förhindra lokal avlyssning på offentligt Wi-Fi.

○ Sant ○ Falskt

7 Fråga 7

7. Ett VPN ändrar fysiskt hårdvarukonfigurationen på din router.

○ Sant ○ Falskt

8 Fråga 8

8. Tunnelprotokoll lägger datapaket i ett krypterat transportlager.

○ Sant ○ Falskt

9 Fråga 9

9. Symmetrisk kryptering använder samma nyckel för att kryptera och dekryptera trafik.

○ Sant ○ Falskt

10 Fråga 10

10. Att använda ett VPN gör din internetanslutning fysiskt immun mot alla offline-strömavbrott.

○ Sant ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. För att skydda din trafik kapslar VPN in dina datapaket i ett annat protokoll, en process som kallas _____ .

2. Om du får långsamma nedladdningar vid streaming kan det bero på nätverkets begränsade _____ .

3. En streamingtjänst som bara finns tillgänglig i ett visst land använder _____ för att begränsa användare i resten av världen.

4. De anslutningsregler som definierar kryptering och anslutningsparametrar kallas VPN:ets _____ .

5. Din dator använder en lokal _____ för att övervaka nätverkstrafik och blockera osäkra anslutningar.

6. När du ansluter till ett VPN dirigeras dina data via en extern _____ för att dölja din publika IP-adress.

ORDBANK

BANDBREDD BRANDVÄGG GEOBLOCKERING INTEGRITET PROTOKOLL SERVER TELEOPERATOR TUNNELERING

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av nätverksbegrepp

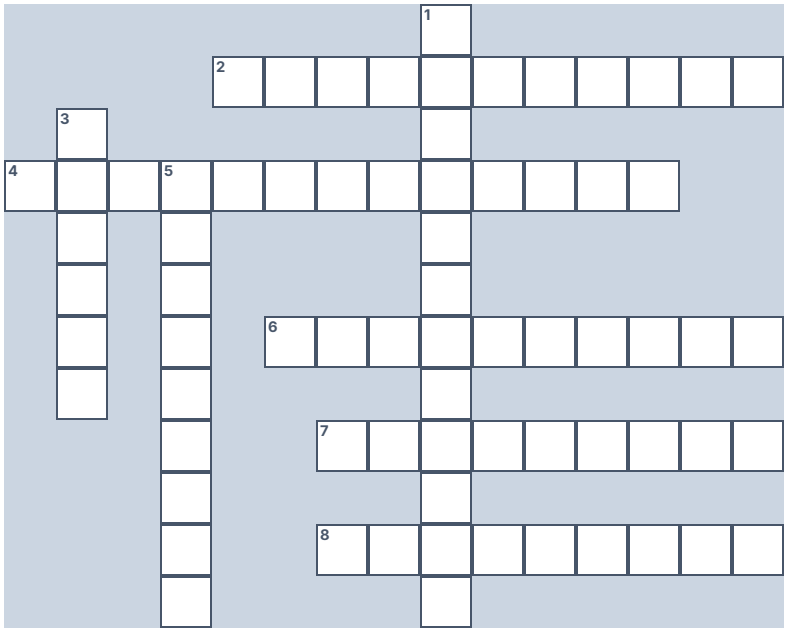
MATCHNING AV DEFINITIONER

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

☐	1. Tunnelering	**A**	En fjärrdator som dirigerar din trafik och döljer din IP-adress.
☐	2. Protokoll	**B**	Internetleverantör som bär din trafik och kan se okrypterad aktivitet.
☐	3. Bandbredd	**C**	En begränsning som hindrar webbåtkomst baserat på fysisk plats.
☐	4. Server	**D**	Ett säkerhetssystem som övervakar och blockerar obehörig trafik.
☐	5. Geospärr	**E**	En uppsättning regler som avgör hur data överförs över nätverket.
☐	6. Brandvägg	**F**	Tillståndet att vara fri från spårning eller offentlig övervakning.
☐	7. Integritet	**G**	Den maximala dataöverföringshastigheten över en anslutning.
☐	8. Internetleverantör	**H**	Att omsluta datapaket i ett annat paket för säker transport.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

2. Inkapsling av datapaket i ett annat paket för säker överföring (11)

4. En begränsning som hindrar webbåtkomst utifrån fysisk plats (13)

6. Tillståndet att vara fri från spårning eller offentlig övervakning (10)

7. Ett säkerhetssystem som övervakar och blockerar obehörig trafik (9)

8. Uppsättning regler som avgör hur data överförs över nätverket (9)

LODRÄTT

1. Internetleverantör (ISP), som loggar din trafik om den inte är krypterad (12)

3. En fjärrdator som dirigerar din trafik och döljer din IP-adress (6)

5. Den högsta hastigheten för dataöverföring över en anslutning (9)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

2 vågrätt: Inkapsling av datapaket i ett annat paket för säker överföring (11 bokstäver):

4 vågrätt: En begränsning som hindrar webbåtkomst utifrån fysisk plats (13 bokstäver):

6 vågrätt: Tillståndet att vara fri från spårning eller offentlig övervakning (10 bokstäver):

7 vågrätt: Ett säkerhetssystem som övervakar och blockerar obehörig trafik (9 bokstäver):

8 vågrätt: Uppsättning regler som avgör hur data överförs över nätverket (9 bokstäver):

LODRÄTT

1 lodrätt: Internetleverantör (ISP), som loggar din trafik om den inte är krypterad (12 bokstäver):

3 lodrätt: En fjärrdator som dirigerar din trafik och döljer din IP-adress (6 bokstäver):

5 lodrätt: Den högsta hastigheten för dataöverföring över en anslutning (9 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

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

ORDLISTA

TUNNELERING PROTOKOLL BANDBREDD SERVER GEOBLOCKERING
BRANDVÄGG INTEGRITET TELEOPERATOR

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. TUNNELERING**
- **B. PROTOKOLL**
- **C. BANDBREDD**
- **D. SERVER**
- **E. GEOBLOCKERING**
- **F. BRANDVÄGG**
- **G. INTEGRITET**
- **H. TELEOPERATOR**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Uppsättning regler som avgör hur data överförs över nätverket. ____
2. En begränsning som hindrar webbåtkomst utifrån fysisk plats. ____
3. Ett säkerhetssystem som övervakar och blockerar obehörig trafik. ____
4. Tillståndet att vara fri från spårning eller offentlig övervakning. ____
5. Internetleverantör (ISP), som loggar din trafik om den inte är krypterad. ____
6. Inkapsling av datapaket i ett annat paket för säker överföring. ____
7. En fjärrdator som dirigerar din trafik och döljer din IP-adress. ____
8. Den högsta hastigheten för dataöverföring över en anslutning. ____

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. EENULRTINGN
2. DBDDAREBN
3. EGKRENGOCL OIB
4. REGTETIINT
5. OORLKTPLO
6. EVSRRE
7. VBGGÄNRDA
8. RLOTERTPEO AE

Bonusaktivitet: Tänk snabbt

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

1	Saker som en IP-adress kan avslöja			
2	Myter om VPN			
3	Saker som färdas över internet			
4	Löften som en bra VPN-leverantör ger			
5	Hemligheter som du skulle kryptera			
6	Saker som ett VPN inte kan skydda dig från			
7	Sätt att upptäcka ett falskt wifi-nätverk			
8	Ord som hör ihop med integritet			
9	Enheter som kan använda ett VPN			
10	Saker som händer när du trycker på "Anslut"			
11	Platser där du skulle använda ett VPN			
12	Skäl till att använda ett VPN under resor			
13	Saker i verkligheten som liknar en tunnel			
14	Ord från det här arbetsbladet som du vill komma ihåg			
15	Ord för att förklara ett VPN för ett barn			

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

Ett VPN krypterar din trafik för att skydda den. Använd bokstav-till-siffra-nyckeln nedan för att avkoda det cybersäkerhetsrelaterade 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	11	25	4	4	1		4	9	14		9	14	20	5	7	18	9	20	5	20
13	5	4		5	14		19	28	11	5	18		20	21	14	14	5	12		

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: Gör ett VPN min internethastighet långsammare?

Ja, något. Krypteringsprocessen och det fysiska avståndet till VPN-servern ger ökad latens och extra belastning. Påverkan varierar med leverantör, protokoll, serveravstånd, enhet och nätverksförhållanden.

Q5: Är det lagligt att använda ett VPN?

Användning av VPN är lagligt i många länder, men vissa jurisdiktioner begränsar, reglerar eller blockerar VPN-tjänster. Användare bör kontrollera aktuella lokala lagar före användning. Mer information finns i guiderna om laglighet på VPN.com.

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: Kan jag använda ett gratis-VPN?

Gratis-VPN kan förlita sig på reklam, begränsade funktioner, användaranalys, datatak eller andra intäktsmodeller. Användare bör granska leverantörens integritetspolicy, ägarskap, granskningar och affärsmodell innan de använder tjänsten.

Q7: Vad är en policy om "inga loggar"?

En policy om ingen loggning beskriver vilken aktivitets- och anslutningsdata en leverantör uppger att den inte sparar. Den exakta omfattningen varierar, så läsare bör granska policyn och oberoende granskningsresultat.

Q8: Hur väljer jag det bästa VPN:et?

Leta efter granskade no-logs-policyer, starka protokoll (WireGuard, OpenVPN), säkra serverplatser, hög hastighet, servrar som bara använder RAM, en kill switch-funktion och en jurisdiktion utanför underrättelsedelande allianser (som 5/9/14 Eyes).

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: Vad är skillnaden mellan WireGuard, OpenVPN och IKEv2?

WireGuard är ett modernt, lättviktigt protokoll (bara cirka 4 000 kodrader) med hög hastighet och snabba anslutningstider. OpenVPN är ett mycket säkert, beprövat protokoll med öppen källkod. IKEv2 är utmärkt för mobila enheter tack vare att det snabbt kan återansluta när man byter nätverk. [4]

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: Vad är servrar som bara använder RAM och varför spelar de roll?

Traditionella servrar skriver data till hårddiskar, som kan beslagtas eller komprometteras. RAM-only-servrar (utan disk) körs helt i flyktigt minne (RAM). När servern startas om eller stängs av raderas data i minnet.

Q5: Hur kringgår obfuskering VPN-blockeringar?

Obfuskering (eller "stealth-VPN") förklär VPN-trafik så att den ser ut som vanlig HTTPS-trafik (port 443). Det kan hjälpa den 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: Vad är delad tunnel (split tunneling) och när ska jag använda den?

Delad tunnling låter dig välja vilka appar som routas genom den krypterade VPN-tunneln och vilka som ansluter direkt till internet. Använd den för att routa känsliga bankappar genom VPN-tjänsten medan lokala spel ansluter direkt, så att du undviker den fördröjning som VPN-tjänsten lägger till.

Q7: Hur fungerar Forward Secrecy (Perfect Forward Secrecy)?

PFS ser till att en unik, tillfällig krypteringsnyckel genereras för varje enskild session. Även om en privat nyckel skulle kompromitteras i framtiden kan den inte användas för att dekryptera tidigare eller framtida sessioner, eftersom de använde oberoende nycklar.

Q8: Vad är allianserna 5/9/14 Eyes och varför ska jag bry mig?

Jurisdiktion kan påverka den rättsliga process som en leverantör kan ställas inför, men den praktiska integritetsrisken beror också på vilka data leverantören behåller, dess tekniska arkitektur, ägarskap, transparensrapportering och granskningshistorik.

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: Kan ett VPN kringgå strypning av internet från internetleverantören?

Ibland. En VPN-tjänst kan hjälpa när en internetleverantör selektivt saktar ned identifierbara aktiviteter, men den löser inte överbelastning, datatak, hastighetsgränser på kontonivå eller dålig nätverkskvalitet.

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) utvecklades av en leverantörsgrupp som bland annat omfattade Microsoft och publicerades som RFC 2637 i juli 1999 för att stödja VPN för fjärråtkomst. [6]

2. MARKNADSVÄRDERING

Den globala VPN-marknaden har vuxit snabbt, drivet av ökande krav på distansarbete och företagens säkerhetsbehov.

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]

4. STRIKTA GRANSKNINGSSTANDARDER

Ledande VPN-leverantörer anlitar externa granskare (som Cure53 eller PwC) för att göra oberoende kodgranskningar och verifiera att de inte loggar någon användaraktivitet.

5. 5 EYES-ALLIANSENS URSPRUNG

Alliansen Five Eyes växte fram ur UKUSA-avtalet från 1946 om signalspaning mellan USA och Storbritannien, som senare utökades med Kanada, Australien och Nya Zeeland.

6. DJUP PAKETINSPEKTION

Djup paketinspektion (DPI) undersöker paketens innehåll och trafikmönster, inte bara huvuden, och vissa brandväggar använder den för att upptäcka och blockera vanliga VPN-protokoll.

7. FÖRETAGSANVÄNDNING

En stor andel av företagsanställda globalt använder säkra VPN för att logga in på interna databaser, vilket gör det till en viktig säkerhetsstandard.

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 och exit) så att inget enskilt relä känner till båda ändarna.

10. KOSTNADEN FÖR DATAINTRÅNG

Att använda en säker åtkomstmodell enligt zero trust med ett VPN hjälper organisationer att skydda immateriella rättigheter och mildra den ekonomiska effekten av dataintrång.

Tekniska referenser och källor

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

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

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

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

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

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Facit: Arbetsblad om vad ett VPN är

1 **Primär funktion** PROTOKOLL — Rätt svar: B

ANTECKNING FÖR LÄRAREN

Ett VPN:s huvuduppgift är att upprätta en krypterad tunnel som skyddar paketens nyttolast och döljer användarens publika IP-adress. Källhänvisning: IETF Tunnel RFC.

2 **Nätverkstunnling** LATENS — Rätt svar: D

ANTECKNING FÖR LÄRAREN

Tunnelprotokoll kapslar in ursprungliga datapaket i yttre bärarpaket för att säkert ta sig över publika nätverk. Källa: IETF Tunnel RFC.

3 **Fråga 3** — Rätt svar: B

ANTECKNING FÖR LÄRAREN

Vilken krypteringsstandard används ofta för att skydda VPN-trafik? → Moderna standarden AES-256

4 **Krypterade komponenter** ROUTNINGSKONTROLLER — Rätt svar: C

ANTECKNING FÖR LÄRAREN

Ett VPN krypterar hela nyttolastsegmentet i IP-datapaket och håller överföringens innehåll konfidentiellt. Källhänvisning: IETF Tunnel RFC.

5 **Fråga 5** — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Kryptering använder en algoritm och en nyckel för att göra klartext till oläslig chiffertext.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Skydd mot avlyssning** IP-MASKERING — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Krypterade tunnlar ser till att paketens nyttolaster förblir oläsliga för aktörer som avlyssnar data på lokala Wi-Fi-nätverk. Källa: Deloitte Advisory.

7 **Hårdvaruändringar** HASTIGHETER — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

VPN är programvarubaserade nätverkstunnlar och ändrar inte fysiskt din gatewayrouters maskinvara. Källa: Cure53 Audit.

8 **Tunnling av paket** RISK FÖR SNIFFNING — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Tunnling fungerar genom att ursprungliga nätverkspaket omsluts av transporthuvuden under överföringen. Källa: IETF Tunnel RFC.

9 **Symmetriska nycklar** BRANDVÄGGAR — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Symmetrisk kryptografi använder en delad nyckel både för att kryptera och dekryptera nätverksströmmar. Källa: WireGuard Project.

10 **Immunitet för strömförsörjning** INGA LOGGAR — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Ett VPN krypterar bara aktiva anslutningssignaler; det kan inte förhindra tjänsteavbrott som orsakas av lokala strömavbrott. Källhänvisning: EDRi Retention Guidelines.

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

H 1. Tunnelering	E 2. Protokoll	G 3. Bandbredd	A 4. Server
C 5. Geospärr	D 6. Brandvägg	F 7. Integritet	B 8. Internetleverantör

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 TUNNELERING	2 BANDBREDD	3 GEOBLOCKERING	4 PROTOKOLL
5 BRANDVÄGG	6 SERVER		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 B – PROTOKOLL	2 E – GEOBLOCKERING	3 F – BRANDVÄGG	4 G – INTEGRITET
5 H – TELEOPERATOR	6 A – TUNNELERING	7 D – SERVER	8 C – BANDBREDD

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara Tunnelering, Protokoll och Bandbredd med egna ord och ge ett exempel på varje.

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

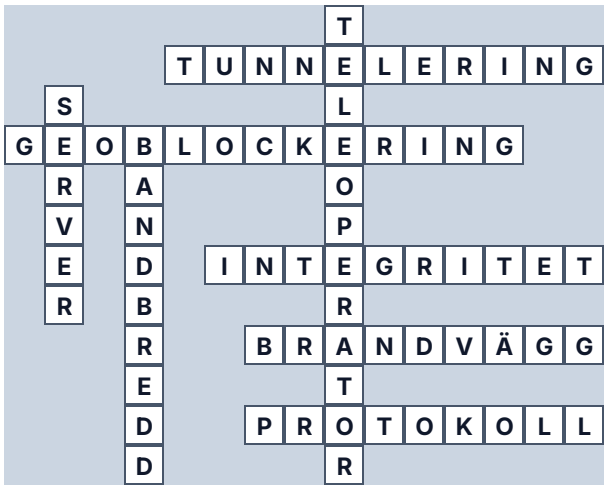
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

2 vågrätt: TUNNELERING Inkapsling av datapaket i ett annat paket för säker överföring (11 bokstäver)

4 vågrätt: GEOBLOCKERING En begränsning som hindrar webbåtkomst utifrån fysisk plats (13 bokstäver)

6 vågrätt: INTEGRITET Tillståndet att vara fri från spårning eller offentlig övervakning (10 bokstäver)

7 vågrätt: BRANDVÄGG Ett säkerhetssystem som övervakar och blockerar obehörig trafik (9 bokstäver)

8 vågrätt: PROTOKOLL Uppsättning regler som avgör hur data överförs över nätverket (9 bokstäver)

LODRÄTT

1 lodrätt: TELEOPERATOR Internetleverantör (ISP), som loggar din trafik om den inte är krypterad (12 bokstäver)

3 lodrätt: SERVER En fjärrdator som dirigerar din trafik och döljer din IP-adress (6 bokstäver)

5 lodrätt: BANDBREDD Den högsta hastigheten för dataöverföring över en anslutning (9 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1.	EENULRTINGN	TUNNELERING	5.	OORLKTPLO	PROTOKOLL
2.	DBDDAREBN	BANDBREDD	6.	EVSRRE	SERVER
3.	EGKRENGOCLOIB	GEOBLOCKERING	7.	VBGGÄNRDA	BRANDVÄGG
4.	REGTETIINT	INTEGRITET	8.	RLOTERTPEOAE	TELEOPERATOR

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"SKYDDA DIN INTEGRITET MED EN SÄKER TUNNEL"

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.