Namn: _____ Datum: _____ Poäng: _____

Guide till den säkraste VPN:en

Teknisk analys av högsäker VPN-design, servrar med enbart flyktigt RAM-minne, Zero Trust-åtkomstsäkerhet, skydd mot läckor via privat krypterad DNS och granskade WireGuard-konfigurationer.

INLÄRNINGSÖVERSIKT: GUIDE TILL DEN SÄKRASTE VPN:EN

ELEV
STUDENTSTATUS
Nätverksförsvararspåret

SÄKER
ANSLUTNINGSSTATUS
Skydda datapaket

AKTIV
LÄCKSKYDD
Skydd mot DNS- och IPv6-läckor

Välkommen! Det här aktivitetshäftet guidar dig genom tekniska standarder för mycket säkra VPN. Du utforskar serverhårdvara med enbart RAM, Zero Trust-åtkomstsäkerhet, privata krypterade DNS-resolvrar och granskade WireGuard-konfigurationer.

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/sakraste-vpn/

Din inlärningsplan för det säkraste VPN:et

- Analysera den tekniska arkitekturen och krypteringsstandarderna i Most Secure VPN Guide.
- Konfigurera klientinställningar för att förhindra läckor av IP-, DNS- och WebRTC-trafik.
- Jämför proprietära tunnelprotokoll med standardimplementeringar.

INSTRUKTIONER: GUIDE TILL DEN SÄKRASTE VPN:EN

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

INFRASTRUKTUR MED ENBART RAM OCH ZERO TRUST-NÄTVERK (INTRODUKTION)

Ett verkligt säkert VPN bygger på ett zero trust-ramverk, servrar med enbart RAM som hindrar att diskbeslag avslöjar loggar, privata krypterade DNS-resolvrar och granskade protokoll som WireGuard. Dessa kontroller tillsammans skyddar digitala tillgångar med högt värde mot avlyssningshot.

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

Kontrollpunkt 1: Utmaning med flerval

1. **1. Vilken arkitektur är avgörande för att säkerställa högsta säkerhet i moderna VPN-servrar?**
   - A) Serverinfrastruktur med enbart RAM
   - B) Disklagring
   - C) Dynamisk DNS-routing
   - D) Aktivering av portvidarebefordran

2. **2. Vilket protokoll rekommenderas ofta för de säkraste och modernaste VPN-konfigurationerna?**
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. **3. Vilket säkerhetsramverk kräver att varje anslutning verifieras kontinuerligt utan undantag?**
   - A) Zero Trust-arkitektur
   - B) Perimeterbrandväggar
   - C) Dynamisk routing
   - D) Delade hemliga nycklar

4. **4. Vad är den främsta uppgiften för en VPN-klients skydd mot DNS-läckor?**
   - A) Dirigera alla DNS-förfrågningar via privata krypterade resolvrar
   - B) Obfuskera IP-paket
   - C) Cacha DNS-förfrågningar lokalt
   - D) Inaktivera namnservrar

5. **5. Hur ökar multihop-routning den övergripande säkerheten i en VPN-tunnel?**
   - A) Dirigerar data genom två separata servrar i följd
   - B) Ökar komprimeringshastigheten
   - C) Krypterar data med chiffer med låg säkerhet
   - D) Kringgår brandväggar

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Servrar som bara använder RAM lagrar loggfiler i flyktigt minne som raderas vid omstart.

○ Sant ○ Falskt

7 Fråga 7

7. WireGuard använder moderna kryptografiska algoritmer som är mindre känsliga för hastighetsflaskhalsar.

○ Sant ○ Falskt

8 Fråga 8

8. En VPN-kill switch fungerar genom att blockera all nätverkstrafik om tunneln faller.

○ Sant ○ Falskt

9 Fråga 9

9. Oberoende granskningar av tredje part är irrelevanta för att verifiera säkerhetsåtaganden.

○ Sant ○ Falskt

10 Fråga 10

10. Zero Trust-modeller utgår från att alla interna nätverksanslutningar är säkra som standard.

○ Sant ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Administratörer upprätthåller säkerheten genom att införa ett strikt ramverk för _____ .

2. Att dirigera paket via flera ingångspunkter kräver en säker konfiguration av typen _____ .

3. För att förhindra dataläckor från stulna diskar använder vi en design baserad på en _____ .

4. ISP-kapning motverkas genom att konfigurera inbyggda funktioner för _____ .

5. För att blockera trafik vid anslutningsfel aktiverar du mekanismen _____ .

6. För att minimera lagrade databasloggar väljer du en leverantör med ett helt _____ .

ORDBANK

DNS-SKYDD | GRANSKAT SYSTEM | KILL SWITCH | KRYPTERING | MULTIHOP | PROTOKOLL | RAM-SERVER | ZERO TRUST

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av VPN- och nätverksbegrepp

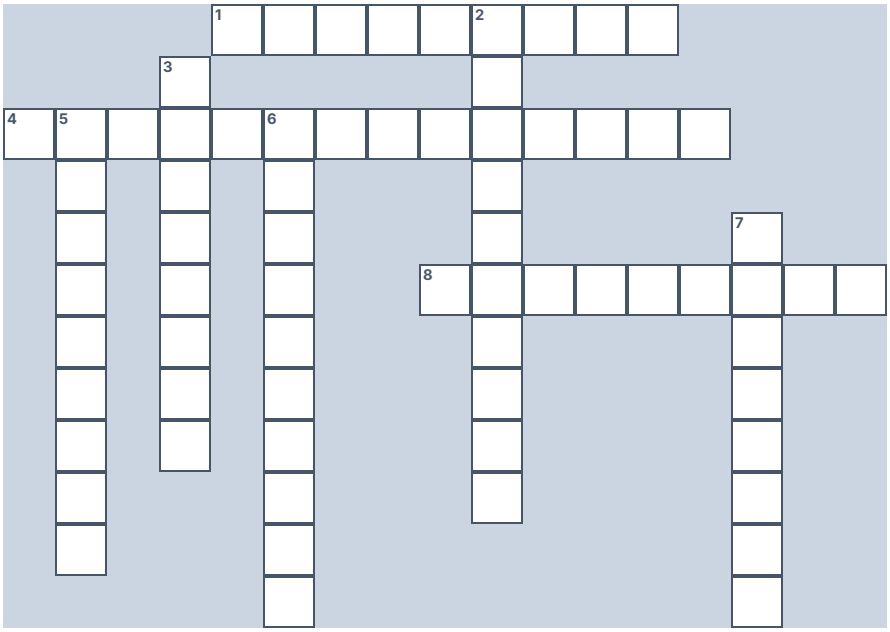
MATCHNING AV DEFINITIONER

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

☐	1. Zero Trust	A	Oberoende granskad uppsättning som bekräftar att inga loggar lagras.
☐	2. Multi-hop	B	Kryptografisk förvrängning av datanyttolaster för att skydda överföringen.
☐	3. Server med enbart RAM	C	Säkerhetsramverk som kräver kontinuerlig autentisering av alla användare.
☐	4. DNS-skydd	D	Uppsättning tekniska regler som avgör hur data paketeras och skickas.
☐	5. Kill switch	E	Kaskadkopplad VPN-routing som kedjar ihop två servernoder.
☐	6. Granskat system	F	Serverarkitektur som använder flyktigt minne för att lagra datanyttolaster.
☐	7. Kryptering	G	Att tillämpa privata DNS-frågor för att skydda namnserveruppslagningar.
☐	8. Protokoll	H	Felsäker mekanism som blockerar trafik om VPN faller.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

1. Uppsättning tekniska regler som avgör hur data paketeras och skickas (9)

4. Oberoende granskad uppsättning som bekräftar att inga loggar lagras (14)

8. Säkerhetsramverk som kräver kontinuerlig autentisering av alla användare (9)

LODRÄTT

2. Kryptografisk omkodning av data för att skydda den under överföring (10)

3. Att tillämpa privata DNS-förfrågningar för att skydda uppslagningar hos namnservrar (8)

5. Serverarkitektur som använder flyktigt minne för att lagra data (9)

6. Skyddsmekanism som blockerar trafiken om VPN-anslutningen faller (10)

7. Kaskadkopplad VPN-routing som länkar ihop två servernoder (8)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

1 vågrätt: Uppsättning tekniska regler som avgör hur data paketeras och skickas (9 bokstäver):

4 vågrätt: Oberoende granskad uppsättning som bekräftar att inga loggar lagras (14 bokstäver):

8 vågrätt: Säkerhetsramverk som kräver kontinuerlig autentisering av alla användare (9 bokstäver):

LODRÄTT

2 lodrätt: Kryptografisk omkodning av data för att skydda den under överföring (10 bokstäver):

3 lodrätt: Att tillämpa privata DNS-förfrågningar för att skydda uppslagningar hos namnservrar (8 bokstäver):

5 lodrätt: Serverarkitektur som använder flyktigt minne för att lagra data (9 bokstäver):

6 lodrätt: Skyddsmekanism som blockerar trafiken om VPN-anslutningen faller (10 bokstäver):

7 lodrätt: Kaskadkopplad VPN-routing som länkar ihop två servernoder (8 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

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

ORDLISTA

ZEROTRUST MULTIHOP RAMSERVER DNSSKYDD KILLSWITCH
GRANSKATSYSTEM KRYPTERING PROTOKOLL

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. ZEROTRUST**
- **B. MULTIHOP**
- **C. RAMSERVER**
- **D. DNSSKYDD**
- **E. KILLSWITCH**
- **F. GRANSKATSYSTEM**
- **G. KRYPTERING**
- **H. PROTOKOLL**

DEFINITIONER OCH MATCHNINGSFÄLT

_____ 1. Skyddsmekanism som blockerar trafiken om VPN-anslutningen faller.

_____ 2. Att tillämpa privata DNS-förfrågningar för att skydda uppslagningar hos namnservrar.

_____ 3. Kaskadkopplad VPN-routing som länkar ihop två servernoder.

_____ 4. Uppsättning tekniska regler som avgör hur data paketeras och skickas.

_____ 5. Kryptografisk omkodning av data för att skydda den under överföring.

_____ 6. Serverarkitektur som använder flyktigt minne för att lagra data.

_____ 7. Oberoende granskad uppsättning som bekräftar att inga loggar lagras.

_____ 8. Säkerhetsramverk som kräver kontinuerlig autentisering av alla användare.

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. RTOEZUSTR
2. RRESARVEM
3. KWCIISHLTL
4. ENTGPIRKRY
5. IHUPTMOL
6. DDSYDKNS
7. SEYGSRAMKT TNAS
8. LOLPTRKOO

Bonusaktivitet: Tänk snabbt

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

1	Lås eller nycklar du använder varje dag			
2	Saker som ett VPN kan dölja			
3	Saker som gör ett VPN säkert			
4	Myter om VPN			
5	Skäl till att använda ett VPN under resor			
6	Säkra platser i verkligheten			
7	Ord som betyder "skyddad"			
8	Löften som en bra VPN-leverantör ger			
9	Ord som hör ihop med integritet			
10	Typer av granskning eller inspektion			
11	Ord från det här arbetsbladet som du vill komma ihåg			
12	Saker som en hackare vill stjäla			
13	Sätt att upptäcka ett falskt wifi-nätverk			
14	Platser där du skulle använda ett VPN			
15	Saker som din internetleverantör kan se			

Kontrollpunkt 8: Fallstudier om VPN och nätverk

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

FALLSTUDIE 1: HÄRDA FÖRETAGSINFRASTRUKTUR



Scenario: En företagsbank utformar om sin topologi för fjärråtkomst. De kräver en Zero Trust-arkitektur som länkar alla klientenheter till säkra servrar.

Diskussionsfråga: Vad är den främsta fördelen med mikrosegmentering av nätverket i en Zero Trust VPN-modell?

FALLSTUDIE 2: SKYDD FÖR SERVRAR MED ENDAST RAM



Scenario: En VPN-leverantör med fokus på säkerhet uppgraderar sina servrar för att förhindra att ett fysiskt beslag av servrar avslöjar användarnas loggar.

Diskussionsfråga: Förklara hur maskinvarukonfigurationer med enbart RAM förhindrar att data utvinns med kriminaltekniska metoder vid fysiska serverbeslag.

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	28	11	18	1		22	16	14		19	11	25	4	4	1	18

4	9	7	9	20	1	12	1		20	9	12	12	7	27	14	7	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 gör ett VPN 'mest säkert'?

En kombination av Zero Trust, servrar med enbart RAM och granskade protokoll.

Q2: Vad är servrar med enbart RAM?

Servrar som körs i flyktigt minne och är utformade för att inte lagra några loggar på disk.

Q3: Vad är ett Zero Trust-VPN?

Ett ramverk som kontinuerligt verifierar varje åtkomstförfrågan och anslutning.

Q4: Varför anses WireGuard vara säkert?

Den har en liten, lättgranskad kodbas och använder moderna chiffer.

Q5: Hur förhindrar säkra VPN DNS-läckor?

Genom att dirigera alla förfrågningar via privata, krypterade DNS-resolvrar.

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

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

Q6: Kräver ett säkert VPN granskningar?

Ja, oberoende granskningar verifierar påståenden om noll loggar och kodens säkerhet.

Q7: Vilken roll har en kill switch?

Den stoppar omedelbart nätverkstrafiken om VPN-anslutningen bryts.

Q8: Vilken kryptering används i säkra VPN?

AES-256 och ChaCha20 är branschstandarder för kryptering.

Q9: Är Multi-Hop-routning säker?

Ja, den kedjar ihop två eller fler servrar för att förhindra trafikanalys.

Q10: Hur hjälper offshore-jurisdiktion?

Det kan begränsa vilka lagar som gäller, men ger ingen absolut immunitet.

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 förhindrar servrar som bara använder RAM risken för beslag av data?

Eftersom de körs i RAM raderas data i minnet när strömmen dras.

Q2: Hur ersätter Zero Trust traditionellt perimeterskydd?

Den behandlar varje klient som fientlig och kräver kontinuerlig autentisering.

Q3: Vad gör att WireGuards kodbas är lättare att granska?

Dess Linux-kod är under 4 000 rader, mycket mindre än typiska VPN-stackar. [4]

Q4: Hur skyddar DNSSEC DNS-frågor?

Den signerar DNS-poster så att resolvrar kan upptäcka förfalskade eller manipulerade svar.

Q5: Hur försvårar Multi-Hop korrelation av trafik?

Genom att separera inkommande och utgående IP-adresser hos olika webbhotell.

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

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

Q6: Varför är jurisdiktioner inom Five Eyes riskfyllda för VPN?

Medlemsstater delar underrättelser och kan använda rättsliga beslut för att begära användardata.

Q7: Hur implementeras en kill switch på kärnnivå?

Den använder systemets brandväggsregler (som iptables eller WFP) för att blockera utgående trafik.

Q8: Vad är forward secrecy i VPN-handskakningar?

Den genererar unika sessionsnycklar så att tidigare sessioner inte kan dekrypteras.

Q9: Hur minskar säkra VPN WebRTC-läckor?

Genom att blockera WebRTC-förfrågningar eller dirigera dem genom tunneln.

Q10: Hur säkerställer oberoende granskningar efterlevnad av integritetskrav?

Granskare utför penetrationstester och inspekterar serverkonfigurationer.

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

Servrar som bara använder RAM läser in sitt operativsystem i minnet vid start, så ingenting finns kvar på disk efter en omstart.

2. VPN-INSIKT

WireGuard använder ramverket Noise med Curve25519, ChaCha20, Poly1305, BLAKE2s och HKDF. [3]

3. VPN-INSIKT

Zero Trust ger åtkomst per resurs och ger inget underförstått förtroende baserat på nätverksplats (NIST SP 800-207). [1]

4. VPN-INSIKT

Underrättelsealliansen Five Eyes omfattar USA, Storbritannien, Kanada, Australien och Nya Zeeland.

5. VPN-INSIKT

WebRTC-läckor uppstår när webbläsare avslöjar klientens verkliga offentliga IP-adress genom STUN-förfrågningar.

6. VPN-INSIKT

Perfect forward secrecy (PFS) säkerställer att en komprometterad långtidsnyckel inte avslöjar tidigare sessionsnycklar. [3]

7. VPN-INSIKT

Cure53, ett säkerhetsföretag i Berlin, har publicerat granskningar av flera VPN-leverantörer.

8. VPN-INSIKT

DNS-läckor uppstår när DNS-frågor går förbi VPN-tunneln och skickas till den lokala ISP:ns namnservrar.

9. VPN-INSIKT

Flyktiga RAM-kretsar behöver ständig elförsörjning för att behålla data och förlorar innehållet när strömmen stängs av.

10. VPN-INSIKT

Zero Trust-system i företag tillämpar kontroller av enhetens säkerhetsläge innan anslutning till säkra resurser tillåts. [1]

Tekniska referenser och källor

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

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Facit: Kontrollpunkt 1 – Flerval

1 **Server med enbart RAM** ENBART RAM — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Servrar som bara använder RAM lagrar inga loggar på disk och raderar data vid omstart. Källa: Most Secure VPN.

2 **Fråga 2** — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

WireGuard kombinerar en liten kodbas som går att granska med moderna chiffer.

3 **Zero Trust-modellen** ZERO TRUST — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Zero Trust-modeller verifierar kontinuerligt enhetens efterlevnad innan åtkomst ges. Källhänvisning: Most Secure VPN.

4 **DNS-skydd** DNS-SKYDD — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

DNS-läckskydd dirigerar uppslagsfrågor via privata resolvrar. Källa: Most Secure VPN.

5 **Multi-hop-tunnlar** MULTI-HOP — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Multi-hop-routing kedjar ihop två separata servernoder i serie. Källa: Most Secure VPN.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Server med enbart RAM** ENBART RAM — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Serverhårdvara som bara använder RAM skriver inga data till disk och raderas vid omstart. Källa: Most Secure VPN.

7 **WireGuard-hastighet** WIREGUARD — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

WireGuard använder modern kryptografi som undviker flaskhalsar i bearbetningen. Källa: Most Secure VPN.

8 **Kill switch** FELSÄKER BRYTARE — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

En kill switch blockerar all trafik om VPN-anslutningen bryts. Källhänvisning: Most Secure VPN.

9 **Granskningar av tredje part** GRANSKNINGAR ÄR VIKTIGA — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Granskningar av tredje part är nödvändiga för att verifiera företags påståenden om integritet. Källa: Most Secure VPN.

10 **Fråga 10** — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Zero Trust ger inget underförstått förtroende baserat på nätverksplats. [1]

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. Zero Trust	E 2. Multi-hop	F 3. Server med enbart RAM	G 4. DNS-skydd
H 5. Kill switch	A 6. Granskat system	B 7. Kryptering	D 8. Protokoll

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 ZERO TRUST	2 MULTIHOP	3 RAM-SERVER	4 DNS-SKYDD
5 KILL SWITCH	6 GRANSKAT SYSTEM		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 E – KILLSWITCH	2 D – DNSSKYDD	3 B – MULTIHOP	4 H – PROTOKOLL
5 G – KRYPTERING	6 C – RAMSERVER	7 F – GRANSKATSYSTEM	8 A – ZEROTRUST

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara Zero Trust, Multi-hop och Server med enbart RAM 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

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

LÖSNING PÅ KORSORDET

			P	R	O	T	O	K	O	L	L			
			D					R						
G	R	A	N	S	K	A	T	S	Y	S	T	E	M	
	A		S		I			P						
	M		S		L			T					M	
	S		K		L		Z	E	R	O	T	R	U	S	T
	E		Y		S			R					L	
	R		D		W			I					T	
	V		D		I			N					I	
	E				T			G					H	
	R				C								O	
					H								P	

LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

1 vågrätt: PROTOKOLL Uppsättning tekniska regler som avgör hur data paketeras och skickas (9 bokstäver)

4 vågrätt: GRANSKATSYSTEM Oberoende granskad uppsättning som bekräftar att inga loggar lagras (14 bokstäver)

8 vågrätt: ZEROTRUST Säkerhetsramverk som kräver kontinuerlig autentisering av alla användare (9 bokstäver)

LODRÄTT

2 lodrätt: KRYPTERING Kryptografisk omkodning av data för att skydda den under överföring (10 bokstäver)

3 lodrätt: DNSSKYDD Att tillämpa privata DNS-förfrågningar för att skydda uppslagningar hos namnservrar (8 bokstäver)

5 lodrätt: RAMSERVER Serverarkitektur som använder flyktigt minne för att lagra data (9 bokstäver)

6 lodrätt: KILLSWITCH Skyddsmekanism som blockerar trafiken om VPN-anslutningen faller (10 bokstäver)

7 lodrätt: MULTIHOP Kaskadkopplad VPN-routing som länkar ihop två servernoder (8 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. RTOEZUSTR — **ZEROTRUST**
2. RRESARVEM — **RAMSERVER**
3. KWCIISHLTL — **KILLSWITCH**
4. ENTGPIRKRY — **KRYPTERING**
5. IHUPTMOL — **MULTIHOP**
6. DDSYDKNS — **DNSSKYDD**
7. SEYGSRAMKTTNAS — **GRANSKATSYSTEM**
8. LOLPTRKOO — **PROTOKOLL**

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"SÄKRA VPN SKYDDAR DIGITALA TILLGÅNGAR"

Facit till fallstudierna

A FALLSTUDIE 1: HÄRDA FÖRETAGSINFRASTRUKTUR

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En företagsbank utformar om sin topologi för fjärråtkomst. De kräver en zero trust-arkitektur som länkar alla klientenheter till säkra servrar.
- Rekommenderad strategi och lösning: Bedömningsvägledning: Förklara att mikrosegmentering begränsar åtkomsten till specifika resurser och förhindrar att hot rör sig i sidled om en enhet komprometteras.

B FALLSTUDIE 2: SKYDD FÖR SERVRAR MED ENDAST RAM

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En säkerhetsfokuserad VPN-leverantör uppgraderar sina servrar för att förhindra att fysiskt beslag av servrar exponerar användarnas loggar.
- Rekommenderad strategi och lösning: Bedömningsvägledning: Beskriv att RAM-only-servrar saknar fysisk disklagring. Strömavbrott raderar automatiskt alla tillfälliga data i det flyktiga minnet.