

Navn: _____

Dato: _____

Point: _____

Guide til den mest sikre VPN

Teknisk analyse af højsikker VPN-arkitektur og flygtig RAM-only-hukommelse

OVERBLIK OVER GUIDEN TIL DEN MEST SIKRE VPN

ELEV

ELEVSTATUS

Netværksforsvarer-spor

SIKKER

FORBINDELSSTATUS

Beskytter datapakker

100%

LÆKAGEFORSVAR

DNS- og IPv6-lækagebeskyttelse

Velkommen! Dette opgavehæfte guider dig gennem de tekniske standarder for højsikre VPN'er. Du vil udforske RAM-only-serverhardware, Zero Trust-adgangssikkerhed, private krypterede DNS-resolvere og reviderede WireGuard-konfigurationer.

OPGAVEARKETS KONTROLPUNKTER

- ☐ Del 1-4: Lær VPN- og netværkssikkerhedskonfigurationer.
- ☐ Del 5-7: Løs kryds og tværs samt ordjagt.
- ☐ Del 8-9: Løs casestudier og chifferudfordring.
- ☐ Del 10: Gennemgå grundlæggende og avanceret FAQ.
- ☐ Del 11: Udforsk 10 interessante fakta fra virkeligheden.

Åbn VPN.com's guide til de bedste VPN'er

URL: <https://www.vpn.com/vpn/most-secure-vpn/>

Din læringsplan for den mest sikre VPN

- Analysér den tekniske arkitektur og krypteringsstandarderne i guiden om den mest sikre VPN.
- Konfigurer klientindstillinger, så IP-, DNS- og WebRTC-trafik ikke lækker.
- Sammenlign proprietære tunneleringsprotokoller med standardimplementeringer.

VEJLEDNING TIL GUIDEN OM DEN MEST SIKRE VPN

Besvar multiple choice- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden på RAM-only-serverhardware og Zero Trust-systemer.

RAM-ONLY-INFRASTRUKTUR OG ZERO TRUST-NETVÆRK (INTRODUKTION)

En virkelig sikker VPN bygger på et zero trust-princip, RAM-only-servere så beslaglagte diske ikke kan afsløre logfiler, private krypterede DNS-resolvere og reviderede protokoller som WireGuard. Tilsammen beskytter disse kontroller værdifulde digitale aktiver mod aflytning.

LÆS HVERT KONTROLPUNKT GRUNDIGT, OG VÆLG ELLER SKRIV DET RIGTIGE SVAR.

Kontrolpunkt 1: Multiple choice-udfordring

- 1** 1. Hvilken arkitektur er afgørende for den højeste sikkerhed i moderne VPN-servere?

 - ☐ A) RAM-only-serverinfrastruktur
 - ☐ B) Disklagring
 - ☐ C) Dynamisk DNS-routing
 - ☐ D) Aktivering af portviderestilling
- 2** 2. Hvilken protokol anbefales bredt til de mest sikre og moderne VPN-konfigurationer?

 - ☐ A) WireGuard
 - ☐ B) PPTP
 - ☐ C) L2TP/IPSec
 - ☐ D) SSTP
- 3** 3. Hvilket sikkerhedsprincip kræver, at hver forbindelse verificeres løbende uden undtagelse?

 - ☐ A) Zero Trust-arkitektur
 - ☐ B) Perimeterfirewalls
 - ☐ C) Dynamisk routing
 - ☐ D) Delte hemmelige nøgler
- 4** 4. Hvad er hovedformålet med DNS-lækagebeskyttelse i en VPN-klient?

 - ☐ A) At sende alle DNS-forespørgsler gennem private krypterede resolvere
 - ☐ B) At obfuskerer IP-pakker
 - ☐ C) At cache DNS-forespørgsler lokalt
 - ☐ D) At deaktivere navneservere
- 5** 5. Hvordan øger multi-hop-routing sikkerheden i en VPN-tunnel?

 - ☐ A) Den sender data gennem to separate servere i serie
 - ☐ B) Den øger komprimeringshastigheden
 - ☐ C) Den krypterer data med svage algoritmer
 - ☐ D) Den omgår firewalls

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. RAM-only-servere gemmer logfiler i flygtig hukommelse, som slettes ved genstart.

☐

Sandt

☐

Falsk

7 Spørgsmål 7

7. WireGuard bruger moderne kryptografiske algoritmer, der er mindre udsatte for hastighedsflaskehalse.

☐

Sandt

☐

Falsk

8 Spørgsmål 8

8. En VPN-kill switch fungerer ved at blokere al netværkstrafik, hvis tunnelen falder ud.

☐

Sandt

☐

Falsk

9 Spørgsmål 9

9. Uafhængige tredjepartsrevisioner er irrelevante, når sikkerhedsløfter skal verificeres.

☐

Sandt

☐

Falsk

10 Spørgsmål 10

10. Zero Trust-modeller antager, at alle interne netværksforbindelser som udgangspunkt er sikre.

☐

Sandt

☐

Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

Læs hver sætning nedenfor, og udfyld det tomme felt med det rigtige ord fra ordbanken.

1. Administratorer styrker sikkerheden ved at indføre et strengt _____ princip.
2. At sende pakker gennem flere indgangspunkter kræver en sikker _____ konfiguration.
3. For at undgå data-læk fra stjålne diske bruger vi et _____ design.
4. Kapring fra udbyderen mindskes ved at konfigurere indbygget _____ funktioner.
5. For at blokere trafik ved forbindelsesfejl aktiveres _____ mekanismen.
6. For at sikre at der ikke findes logdatabaser, vælges en fuldt _____ udbyder.

ORDBANK MED FAGUDTRYK

DNSBESKYTTELSE

KILLSWITCH
RAMONLYKRYPTERING
REVISIONMULTIHOP
ZEROTRUST

PROTOKOL

Skriv dine svar her:

1.

2.

3.

4.

5.

6.

Kontrolpunkt 4: Match VPN- og netværksbegreber

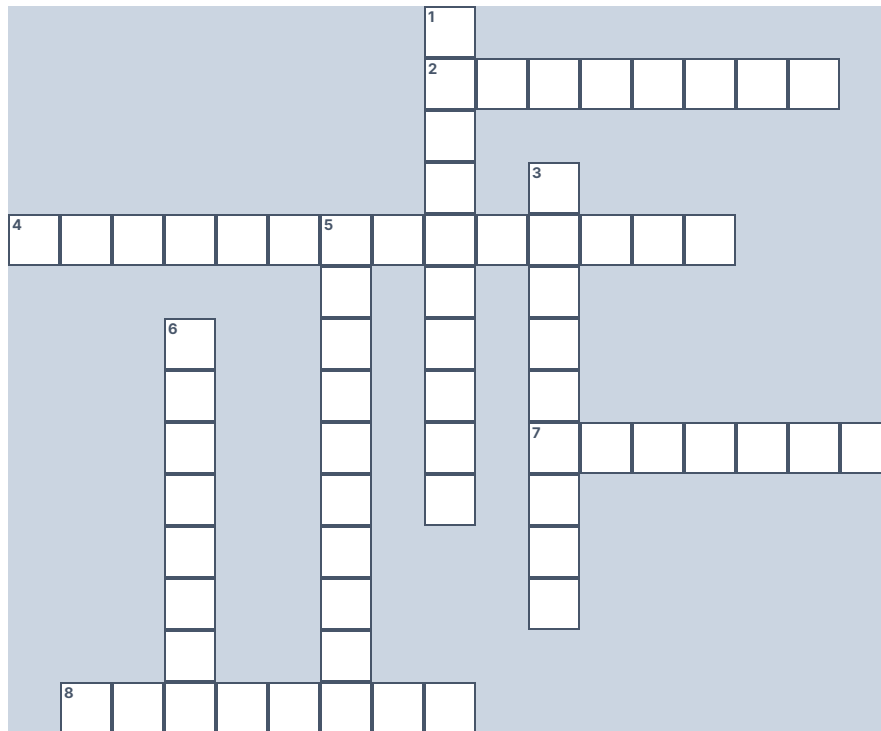
MATCH DEFINITIONER

Match hvert fagudtryk til venstre med den rigtige definition til højre ved at skrive det tilhørende bogstav (A-H) i indtastningsfeltet.

Zero Trust	E	Fejlsikker mekanisme, der blokerer trafik, hvis VPN'en svigter.
Multi-Hop	F	Uafhængigt kontrolleret opsætning, der bekræfter, at ingen logfiler gemmes.
RAM-only-server	G	Kryptografisk omformning af dataindhold, så transporten sikres.
DNS-beskyttelse	C	Serverarkitektur, der bruger flygtig hukommelse til at opbevare data.
Kill switch	B	Kaskaderet VPN-routing, der kæder to serverknodepunkter sammen.
Revideret system	A	Sikkerhedsprincip, der kræver løbende godkendelse af alle brugere.
Kryptering	H	Sæt af tekniske regler for, hvordan data pakkes og sendes.
Protokol	D	Håndhævelse af private DNS-forespørgsler for at beskytte navneserveropslag.

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

- 2. Uafhængig kontrol der bekræfter nul logfiler (8)
- 4. Sikrer at navneopslag går gennem krypterede resolve (14)
- 7. Serverhardware med flygtig hukommelse der slettes ved genstart (7)
- 8. Routing der kæder to servere sammen i serie (8)

LODRETTE NØGLER

- 1. Kryptografisk omformning der beskytter dataindhold (10)
- 3. Princip der kræver løbende godkendelse af hver forbindelse (9)
- 5. Fejlsikker afbryder der blokerer trafik ved udfald (10)
- 6. Tekniske regler for hvordan data pakkes og sendes (8)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

Brugere af skærmlæser og tastatur kan skrive krydsordssvarene direkte i tekstfelterne nedenfor.

VANDRETTE NØGLER

2 vandret: Uafhængig kontrol der bekræfter nul logfiler (8 bogstaver):

4 vandret: Sikrer at navneopslag går gennem krypterede resolve (14 bogstaver):

7 vandret: Serverhardware med flygtig hukommelse der slettes ved genstart (7 bogstaver):

8 vandret: Routing der kæder to servere sammen i serie (8 bogstaver):

LODRETTE NØGLER

1 lodret: Kryptografisk omformning der beskytter dataindhold (10 bogstaver):

3 lodret: Princip der kræver løbende godkendelse af hver forbindelse (9 bogstaver):

5 lodret: Fejlsikker afbryder der blokerer trafik ved udfald (10 bogstaver):

6 lodret: Tekniske regler for hvordan data pakkes og sendes (8 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

Find de 8 vigtige fagudtryk, der er skjult i gitteret nedenfor. Ordene kan stå vandret, lodret eller diagonalt.

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

ORDLISTE MED FAGUDTRYK

ZEROTRUST

MULTIHOP

RAMONLY
KRYPTERINGDNSBESKYTTELSE
PROTOKOL

KILLSWITCH

REVISION

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK

- A. Zero Trust
- B. Multi-Hop
- C. RAM-only-server
- D. DNS-beskyttelse
- E. Kill switch
- F. Revideret system
- G. Kryptering
- H. Protokol

DEFINITIONER OG MATCHFELTER

- 1. Sikkerhedsprincip med løbende verifikation af adgang.
- 2. Routing gennem to servere i serie.
- 3. Serverhardware med flygtig hukommelse, der gemmer nul logfiler.
- 4. Lækagebeskyttelse via krypteret DNS-resolver.
- 5. Fejlsikker kill switch, der stopper datalæk ved udfald.
- 6. Tredjepartsrevideret no-logs-privatlivsniveau.
- 7. Kryptografisk omformning, der beskytter pakkernes indhold.
- 8. Tekniske protokolregler for pakning af data under transport.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige begreber om virtuelle private netværk (VPN). Skriv dine svar i indtastningsfelterne.

1. **R T O E Z U S T R**

5. **I H U P T M O L**

2. **R M Y L N O A**

6. **S K E E S L Y S T D
N T E B**

3. **K W C I I S H L T L**

7. **R N S I O E I V**

4. **E N T G P I R K R Y**

8. **T R O L P O K O**

Kontrolpunkt 8: VPN- og netværkscasestudier

Anvend de begreber, du har lært, til at løse de virkelige scenarier nedenfor.

CASESTUDIE 1: HÆRDNING AF VIRKSOMHEDENS INFRASTRUKTUR



Scenarie: En bank omlægger sin fjernadgang. De har brug for en zero trust-arkitektur, der forbinder alle klientenheder til sikre servere.

Diskussion: Hvad er den største fordel ved mikrosegmentering under en Zero Trust-VPN-model?

CASESTUDIE 2: BESKYTTELSE MED RAM-ONLY-SERVERE



Scenarie: En sikker VPN-udbyder opgraderer sine servere for at undgå, at fysisk beslaglæggelse af servere afslører brugernes loghistorik.

Diskussion: Forklar hvordan RAM-only-hardware forhindrer forensisk dataudtræk ved fysisk beslaglæggelse af servere.

Sidste udfordring: Afkod chifferet

En netværksingeniør sikrer routingkanaler og klienttunneler. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter. Afkodet cybersikkerhedsbesked:

BOGSTAV-TIL-TAL-KRYPTERINGSNØGLE

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

Afkodet cybersikkerhedsbesked:

	19	9	11	18	5		22	16	14	5	18		19	9	11	18	5	18	
22	1	5	18	4	9	6	21	12	4	5		4	9	7	9	20	1	12	5
							1	11	20	9	22	5	18						

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z).

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del A)

Gennemgå de mest almindelige spørgsmål og svar om virtuelle private netværk (VPN'er) og tunnelering.

Q1: Hvad gør en VPN til den "mest sikre"?

En kombination af Zero Trust, RAM-only-servere og reviderede protokoller.

Q2: Hvad er RAM-only-servere?

Servere der udelukkende kører i flygtig hukommelse og gemmer nul logfiler på disken.

Q3: Hvad er en Zero Trust-VPN?

Et princip, der løbende verificerer hver adgangsmodning og forbindelse.

Q4: Hvorfor betragtes WireGuard som sikker?

Den har en lille, let reviderbar kodebase og bruger moderne algoritmer.

Q5: Hvordan forhindrer sikre VPN'er DNS-lækager?

Ved at sende alle forespørgsler gennem private, krypterede DNS-resolvere.

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del B)

Gennemgå de mest almindelige spørgsmål og svar om virtuelle private netværk (VPN'er) og tunnelering.

Q6: Kræver en sikker VPN revisioner?

Ja, uafhængige revisioner verificerer no-logs-påstande og kodesikkerhed.

Q7: Hvilken rolle spiller en kill switch?

Den stopper øjeblikkeligt netværkstrafikken, hvis VPN-forbindelsen falder ud.

Q8: Hvilken kryptering bruges i sikre VPN'er?

AES-256 og ChaCha20 er branchestandarderne for kryptering.

Q9: Er multi-hop-routing sikker?

Ja, den kæder to eller flere servere sammen for at forhindre trafikanalyse.

Q10: Hvordan hjælper en jurisdiktion i udlandet?

Den beskytter VPN-udbyderen mod retskendelser og anmodninger om data.

Kontrolpunkt 11: Avanceret VPN-FAQ (del A)

Udforsk avancerede tekniske aspekter af VPN-tunneleringsprotokoller, mobile klientintegrationer og virksomhedsudrulning.

Q1: Hvordan forhindrer RAM-only-servere risikoen ved beslaglæggelse?

Fordi de kører i RAM, slettes alle data øjeblikkeligt, når strømmen afbrydes.

Q2: Hvordan erstatter Zero Trust almindelig perimetersikkerhed?

Den behandler enhver klient som fjendtlig og kræver løbende godkendelse.

Q3: Hvad gør WireGuards kodebase lettere at revidere?

Den indeholder under 4.000 linjer kode mod OpenVPN's over 100.000.

Q4: Hvordan beskytter DNSSEC DNS-forespørgsler?

Den signerer DNS-forespørgsler kryptografisk for at forhindre spoofing og kapring.

Q5: Hvordan vanskeliggør multi-hop trafikkorrelation?

Ved at adskille indgående og udgående IP-adresser hos forskellige hostingudbydere.

Kontrolpunkt 11: Avanceret VPN-FAQ (del B)

Udforsk avancerede tekniske aspekter af VPN-tunneleringsprotokoller, mobile klientintegrationer og virksomhedsudrulning.

Q6: Hvorfor er Five Eyes-jurisdiktioner risikable for VPN'er?

Fordi efterretningstjenester kan tvinge udbydere til hemmeligt at indsamle data.

Q7: Hvordan implementeres en kill switch på kerneniveau?

Den bruger systemets firewallregler (som iptables eller WFP) til at blokere udgående trafik.

Q8: Hvad er forward secrecy i VPN-handshakes?

Den genererer unikke sessionsnøgler, så tidligere sessioner ikke kan dekrypteres.

Q9: Hvordan afbøder sikre VPN'er WebRTC-lækager?

Ved at blokere WebRTC-forespørgsler eller sende dem gennem tunnelen.

Q10: Hvordan sikrer uafhængige revisioner overholdelse af privatlivsregler?

Revisorer udfører penetrationstest og gennemgår serverkonfigurationer.

Del 11: 10 VPN-fakta og indsigter fra virkeligheden

Gennemgå virkelige fakta om VPN-krypteringshastigheder, protokolrevisioner, mobil forbindelse og fjernarbejde i virksomheder.

1. VPN-INDSIGT

RAM-only-serverarkitekturer henter konfigurationsfiler fra sikre, krypterede netværksdrev ved opstart.

2. VPN-INDSIGT

WireGuard bruger Noise-protokolrammen samt algoritmerne Curve25519, ChaCha20, Poly1305 og BLAKE2.

3. VPN-INDSIGT

Zero Trust-netværksadgang (ZTNA) erstatter hurtigt ældre klient-til-site-VPN'er i virksomheder.

4. VPN-INDSIGT

Efterretningsalliancen Five Eyes omfatter USA, Storbritannien, Canada, Australien og New Zealand.

5. VPN-INDSIGT

WebRTC-lækager opstår, når browsere afslører klientens rigtige offentlige IP-adresse via STUN-forespørgsler.

6. VPN-INDSIGT

Perfect forward secrecy (PFS) sikrer, at kompromittering af en langtidsnøgle ikke kompromitterer tidligere nøgler.

7. VPN-INDSIGT

Cure53 er et af de mest fremtrædende cybersikkerhedsfirmaer, der reviderer VPN-udbydere globalt.

8. VPN-INDSIGT

DNS-lækager opstår, når DNS-forespørgsler går uden om VPN-tunnelen til den lokale udbyders navneservere.

9. VPN-INDSIGT

Flygtige RAM-chips kræver konstant strøm for at bevare data og slettes helt, når strømmen afbrydes.

10. VPN-INDSIGT

Virksomheders Zero Trust-systemer kontrollerer enhedens tilstand, før der gives adgang til sikre ressourcer.

Tekniske referencer og kilder

Studieguiden og de interaktive opgaver er sammensat ud fra globale tekniske standarder, specifikationer og lovgivningsmæssige rammer.

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[1] VPN.com. (2026). Sammenligning og købsguide til de mest sikre VPN'er.

<https://www.vpn.com/vpn/most-secure-vpn/>

[3] Cloudflare. (2026). Hvad er Zero Trust? Implementeringsguide.

<https://www.cloudflare.com/learning/security/what-is-zero-trust/>

[5] WireGuard. (2026). WireGuard: Hurtig, moderne og sikker VPN-tunnel.

<https://www.wireguard.com/>

[7] CISA. (2026). Cybersikkerhedsvejledninger og - anbefalinger.

<https://www.cisa.gov/>

[9] NIST. (2026). Håndhævelse af mindst mulige rettigheder.

<https://csrc.nist.gov/publications/detail/sp/800-207/final>

[2] CISA. (2026). Officiel hjemmeside.

<https://www.cisa.gov/>

[4] NIST. (2026). NIST SP 800-207: Zero Trust-arkitektur.

<https://csrc.nist.gov/publications/detail/sp/800-207/final>

[6] OpenVPN. (2026). Open source-virtuelt privat netværk.

<https://www.openvpn.net>

[8] Cloudflare. (2026). Trusselsforebyggelse og sikker tunnelering.

<https://www.cloudflare.com/learning/security/what-is-zero-trust/>

[10] VPN.com. (2026). Højest bedømte krypterede VPN-udbydere.

<https://www.vpn.com/vpn/most-secure->

Facitliste: Kontrolpunkt 1 – Multiple choice

1 RAM-only-server RAM-ONLY

Rigtigt svar: A

UNDERVISNINGSNOTE

RAM-only-servere gemmer ingen logfiler på disken og slettes ved genstart. Kilde: Most Secure VPN [Ref 4].

RAM-only-servere gemmer ingen logfiler på disken og slettes ved genstart.

2 WireGuard-protokol WIREGUARD

Rigtigt svar: A

UNDERVISNINGSNOTE

WireGuard-protokollen leverer den hurtigste og sikreste moderne kryptografi. Kilde: Most Secure VPN [Ref 5].

WireGuard-protokollen leverer den hurtigste og sikreste moderne kryptografi.

3 Zero Trust-modellen ZERO TRUST

Rigtigt svar: A

UNDERVISNINGSNOTE

Zero Trust-modeller kontrollerer løbende enhedens tilstand før adgang. Kilde: Most Secure VPN [Ref 3].

Zero Trust-modeller kontrollerer løbende enhedens tilstand før adgang.

4 DNS-beskyttelse DNS-BESKYTTELSE

Rigtigt svar: A

UNDERVISNINGSNOTE

DNS-lækagebeskyttelse sender opslag gennem private resolvere. Kilde: Most Secure VPN [Ref 10].

DNS-lækagebeskyttelse sender opslag gennem private resolvere.

5 Multi-hop-tunneler MULTI-HOP

Rigtigt svar: A

UNDERVISNINGSNOTE

Multi-hop-routing kæder to separate serverknodepunkter i serie. Kilde: Most Secure VPN [Ref 10].

Multi-hop-routing kæder to separate serverknodepunkter i serie.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 RAM-only-server RAM-ONLY

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

RAM-only-serverhardware skriver ingen data til disk og slettes ved genstart. Kilde: Most Secure VPN [Ref 4].

RAM-only-serverhardware skriver ingen data til disk og slettes ved genstart.

7 WireGuard-hastighed WIREGUARD

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

WireGuard bruger moderne kryptografi, der undgår flaskehalse i behandlingen. Kilde: Most Secure VPN [Ref 5].

WireGuard bruger moderne kryptografi, der undgår flaskehalse i behandlingen.

8 Kill switch FEJLSIKKER AFBRYDER

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

En kill switch blokerer al trafik, hvis VPN-forbindelsen falder ud. Kilde: Most Secure VPN [Ref 10].

En kill switch blokerer al trafik, hvis VPN-forbindelsen falder ud.

9 Tredjepartsrevisioner REVISIONER ER AFGØRENDE

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Tredjepartsrevisioner er afgørende for at verificere virksomheders privatlivspåstande. Kilde: Most Secure VPN [Ref 10].

Tredjepartsrevisioner er afgørende for at verificere virksomheders privatlivspåstande.

10 Zero Trust-modellen INGEN TILLID SOM UDGANGSPUNKT

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Zero Trust-modeller antager, at alle forbindelser er fjendtlige, indtil de er godkendt. Kilde: Most Secure VPN [Ref 3].

Zero Trust-modeller antager, at alle forbindelser er fjendtlige, indtil de er godkendt.

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

- | | | | |
|----------------------|---------------------------|--------------------------|--------------------------|
| A Zero Trust | B Multi-Hop | C RAM-only-server | D DNS-beskyttelse |
| E Kill switch | F Revideret system | G Kryptering | H Protokol |

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

- | | | | |
|----------------------|---------------------------|--------------------------|--------------------------|
| 1 Zero Trust | 2 Multi-Hop | 3 RAM-only-server | 4 DNS-beskyttelse |
| 5 Kill switch | 6 Revideret system | | |

DISKUSSIONSNOTER TIL UNDERVISERE

Vurderingsnøjagtighed:

Kontrollér, at eleverne forstår, hvordan domænelængde, endelse (.com, .ai) og kommerciel søgevolumen påvirker vurderingsprisen.

Deponeringssikkerhed:

Understreg, at midlerne opbevares på licenserede tredjepartskonti, indtil overdragelsen af domænets WHOIS er verificeret.

Anonym repræsentation:

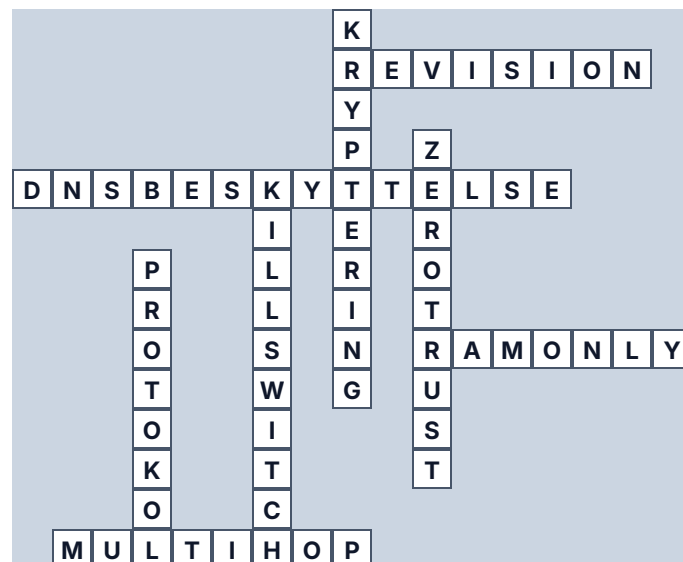
Fremhæv, hvordan fortrolighedsaftaler og tredjepartsrepræsentation forhindrer spekulative prisstigninger under virksomhedsindkøb.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: REVISION Uafhængig kontrol der bekræfter nul logfiler (6,10)

4 vandret: DNSBESKYTTELSE Sikrer at navneopslag går gennem krypterede resolve (9,2)

7 vandret: RAMONLY Serverhardware med flygtig hukommelse der slettes ved genstart (13,12)

8 vandret: MULTIHOP Routing der kæder to servere sammen i serie (18,3)

LODRETTE NØGLER

1 lodret: KRYPTERING Kryptografisk omformning der beskytter dataindhold (5,10)

3 lodret: ZEROTRUST Princip der kræver løbende godkendelse af hver forbindelse (8,12)

5 lodret: KILLSWITCH Fejlsikker afbryder der blokerer trafik ved udfald (9,8)

6 lodret: PROTOKOL Tekniske regler for hvordan data pakkes og sendes (11,5)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

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

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"SIKRE VPNER SIKRER VAERDIFULDE DIGITALE AKTIVER"

Facit til VPN- og netværkscasestudier