Navn: _____ Dato: _____ Point: _____

VPN til store virksomheder

Implementering af Zero Trust-netværksadgang, dedikerede gateway-noder og central administration for virksomheden.

OVERBLIK OVER VPN-NETVÆRK I STORE VIRKSOMHEDER

ELEV
ELEVSTATUS
Netværksforsvarer-spor

SIKKER
FORBINDELSESSTATUS
Beskytter datapakker

AKTIV
LÆKAGEBESKYTTELSE
DNS- og IPv6-lækagebeskyttelse

Velkommen! Dette opgavehæfte guider dig gennem VPN-netværk i store virksomheder. Du vil udforske Zero Trust-arkitektur, dedikerede statiske IP-gateways, administratorkonsoller, tildeling af licenser og site-til-site-IPsec-tunneler.

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.**
- [ ] **Bonus: Tænk hurtigt-udfordring.**

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

URL: https://www.vpn.com/vpn/best-vpn-for-business/enterprise/

Din læringsplan for VPN-netværk i store virksomheder

- Implementér rammeværk for Zero Trust-netværksadgang (ZTNA).
- Konfigurér dedikerede IP-adresser til gateways, så de kan hvidlistes.
- Administrér centrale firmapaneler og lister over brugerpladser.
- Gennemgå logfiler over netværksadgang og brugernes forbindelseshistorik.
- Opsæt regler for Single Sign-On (SSO) og flerfaktorgodkendelse.
- Opsæt site-til-site-IPsec-tunneler mellem filialer.

VEJLEDNING TIL VPN-NETVÆRK I STORE VIRKSOMHEDER

Besvar flervalgs- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden på Zero Trust og site-til-site-IPsec. Slut af med bonusaktiviteten Tænk hurtigt.

ZERO TRUST-ARKITEKTUR OG DEDIKEREDE GATEWAYS (INTRODUKTION)

VPN i store virksomheder beskytter firmaets aktiver ved at skifte til Zero Trust-netværksadgang (ZTNA) og hvidliste dedikerede statiske IP-gateways. IT-ansvarlige bruger centrale administrationskonsoller til at styre site-til-site-IPsec-tunneler og single sign-on (SSO).

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

Kontrolpunkt 1: Flervalgsopgave

1. **1. Hvilken sikkerhedsmodel afløser ældre virksomheds-VPN'er?**
   - A) Zero Trust
   - B) Multi-hop
   - C) Peer-to-peer
   - D) Én enkelt gateway

2. **2. Hvilken funktion kræves for at begrænse databaseadgang til firmaets servere?**
   - A) Dedikeret IP
   - B) Dynamisk routing
   - C) Split tunnel
   - D) DNS-proxy

3. **3. Hvilken protokol er standard for site-til-site-tunneler i virksomheder?**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **4. Hvilket centralt værktøj lader administratorer styre medarbejderpladser?**
   - A) Administrationskonsol
   - B) Registreringsnøgle
   - C) Routerens firmware
   - D) Systemlog

5. **5. Hvilken godkendelsesstandard gør det muligt at logge ind via Okta eller Microsoft Entra ID?**
   - A) Single Sign-On
   - B) Delt hemmelighed
   - C) EPP-godkendelse
   - D) WEP-nøgle

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Zero Trust-netværksadgang giver kun adgang, når enhedens tillid løbende er bekræftet.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. Dedikerede IP-gateways sender medarbejdernes trafik sammen med tilfældige forbrugere.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. Centrale administrationskonsoller lader IT-ansvarlige straks fjerne enkelte medarbejderpladser.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. IPsec er en letvægtsprotokol, der ikke understøtter site-til-site-tunneler.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. Single Sign-On giver sikker godkendelse af medarbejdere via firmaets identitetsudbydere.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. Moderne sikkerhedsarkitektur erstatter ældre tunneler med _____ adgang.
2. For at begrænse databaseadgang opsætter firmaer en _____ gateway-adresse.
3. Filialkontorer forbindes sikkert med site-til-site- _____ -tunneler.
4. IT-administratorer tildeler brugerlicenser i den centrale _____ .
5. Integration med Okta lader medarbejdere godkende sig via firmaets _____ .
6. For at beskytte login kræver virksomhedsportaler _____ godkendelse.

ORDBANK MED FAGUDTRYK

ADMINKONSOL DEDIKERET IP FLERFAKTOR GATEWAY IPSEC SINGLE SIGN-ON TILDELING ZERO TRUST

Skriv dine svar her:

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

Kontrolpunkt 4: Match fagbegreber

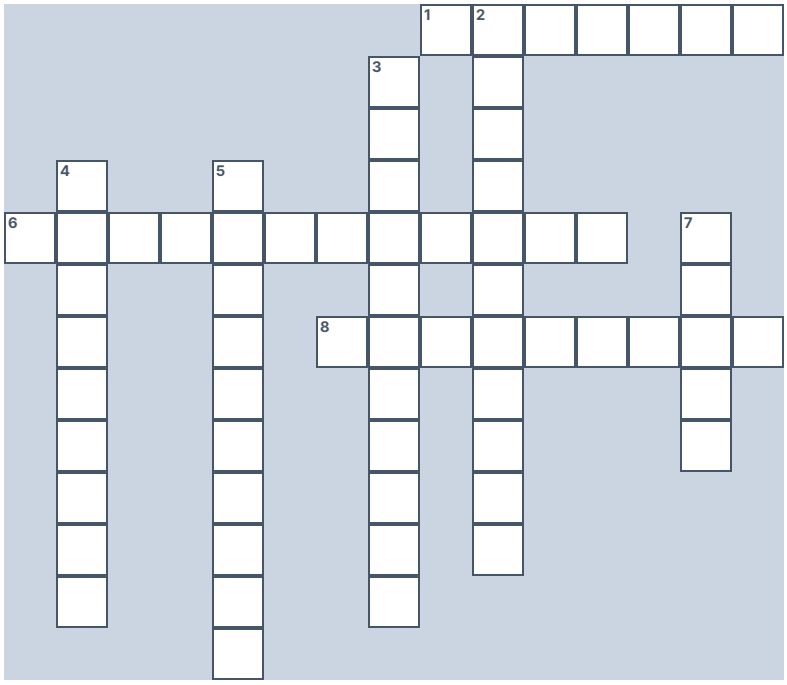
MATCH BEGREBER OG DEFINITIONER

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

☐	1. ZERO TRUST	A	Tildeling af VPN-licenser til medarbejdere.
☐	2. DEDIKERET IP	B	Identitetsforbindelse til Okta og Entra ID.
☐	3. IPSEC	C	Loginsikkerhed der kræver ekstra koder.
☐	4. ADMINKONSOL	D	Statisk gateway-adresse til hvidlistning.
☐	5. SINGLE SIGN-ON	E	Standard for site-til-site-tunneler.
☐	6. FLERFAKTOR	F	Knudepunkt der router indgangen til netværket.
☐	7. GATEWAY	G	Central portal til IT-styring af pladser.
☐	8. TILDELING	H	Rammeværk med løbende verifikation af tillid.

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

1. Knudepunkt, der router indgangen til netværket (7)

6. Identitetskobling til Okta og Entra ID (12)

8. Rammeværk med løbende verifikation af tillid (9)

LODRETTE NØGLER

2. Central portal, hvor IT-administratoren styrer pladser (11)

3. Statisk gateway-adresse til hvidlistning (11)

4. Fordeling af VPN-adgangslicenser til medarbejdere (9)

5. Loginsikkerhed, der kræver ekstra koder (10)

7. Standard for site-til-site-tunneler (5)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

1 vandret: Knudepunkt, der router indgangen til netværket (7 bogstaver):

6 vandret: Identitetskobling til Okta og Entra ID (12 bogstaver):

8 vandret: Rammeværk med løbende verifikation af tillid (9 bogstaver):

LODRETTE NØGLER

2 lodret: Central portal, hvor IT-administratoren styrer pladser (11 bogstaver):

3 lodret: Statisk gateway-adresse til hvidlistning (11 bogstaver):

4 lodret: Fordeling af VPN-adgangslicenser til medarbejdere (9 bogstaver):

5 lodret: Loginsikkerhed, der kræver ekstra koder (10 bogstaver):

7 lodret: Standard for site-til-site-tunneler (5 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

ZEROTRUST DEDIKERETIP IPSEC ADMINKONSOL SINGLESIGNON FLERFAKTOR GATEWAY TILDELING

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. ZEROTRUST
B. DEDIKERETIP
C. IPSEC
D. ADMINKONSOL
E. SINGLESIGNON
F. FLERFAKTOR
G. GATEWAY
H. TILDELING

DEFINITIONER OG MATCHFELTER
[ ] 1. Statisk gateway-adresse til hvidlistning.
[ ] 2. Knudepunkt, der router indgangen til netværket.
[ ] 3. Fordeling af VPN-adgangslicenser til medarbejdere.
[ ] 4. Loginsikkerhed, der kræver ekstra koder.
[ ] 5. Standard for site-til-site-tunneler.
[ ] 6. Rammeværk med løbende verifikation af tillid.
[ ] 7. Identitetskobling til Okta og Entra ID.
[ ] 8. Central portal, hvor IT-administratoren styrer pladser.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige fagbegreber fra opgavearket. Skriv dine svar i indtastningsfelterne.

1. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. YAWEAGT
5. TEERDPKEDII
6. NLKNOSADOMI
7. LRFKATORFE
8. GENTDILIL

Bonusaktivitet: Tænk hurtigt

3 SVAR I HVER KATEGORI. DEN FØRSTE, DER UDFYLDER HELE LISTEN, VINDER.

1	Værktøjer, som et firma bruger hver dag			
2	Ting, en VPN kan skjule			
3	Roller i en IT-afdeling			
4	Ord, der beskriver Zero Trust			
5	Måder at logge sikkert ind			
6	Grunde til at give medarbejdere VPN			
7	Ting at gøre ved et sikkerhedsbrud			
8	Grunde til at bruge en VPN på rejsen			
9	Regler for sikker fjernarbejde			
10	Data, et firma skal beskytte			
11	Ting, der kan forsinke et videomøde			
12	Enheder, der kan bruge en VPN			
13	Kontorprogrammer, du kender			
14	Steder, hvor medarbejdere arbejder fra			
15	Enheder, en medarbejder kan have			

Kontrolpunkt 8: Casestudier om VPN og netværk

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

CASESTUDIE 1: OVERGANG TIL ZERO TRUST

👷

Scenarie: En virksomhed vil sikre sine lokale servere ved løbende at kontrollere enhedernes certifikater, firewallstatus og brugerens placering frem for at stole på alle inde i netværket.

Diskussion: Hvilket rammeværk bør IT-sikkerhedschefen indføre for at nå dette mål?

CASESTUDIE 2: BEGRÆNSNING AF GATEWAY

👷

Scenarie: En virksomhed har private finansdatabaser i skyen. De vil blokere al offentlig adgang til administrationspanelerne og kun tillade login fra verificerede firmaenheder.

Diskussion: Hvilken netværkskonfiguration bør databaseadministratoren opsætte i skyens firewall?

Kontrolpunkt 9: 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.

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 Æ=27 Ø=28 Å=29

22	5	18	9	6	9	3	5	18		8	22	5	18		5	14	8	5	4
6	28	18		4	21		7	9	22	5	18		1	4	7	1	14	7	

Afkodet besked:

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z, 27 = Æ, 28 = Ø, 29 = Å).

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del A)

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

Q1: Hvad er en VPN til store virksomheder?

En sikker netværkstunnel til virksomheder, der giver fjernmedarbejdere adgang til firmanetværket med central styring.

Q2: Hvordan adskiller Zero Trust sig fra traditionel VPN?

Traditionelle VPN'er stoler på alle i tunnelen, mens Zero Trust løbende verificerer hver enhed og hver brugerforbindelse.

Q3: Hvad er en dedikeret IP i virksomheds-VPN?

En statisk IP-adresse reserveret til din virksomhed, som kan hvidlistes til sikker adgang til databaser i skyen.

Q4: Hvorfor er SSO vigtigt for virksomheds-VPN?

Single Sign-On lader medarbejdere bruge deres virksomhedslogin (fx Okta eller Microsoft Entra ID) til at logge sikkert ind.

Q5: Hvad er en site-til-site-VPN?

En tunnel, der forbinder to fysiske kontorer (fx en filial og hovedkontoret) over internettet ved hjælp af IPsec.

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del B)

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

Q6: Hvad bruges en administrationskonsol til?

Et panel, hvor IT-administratorer tilføjer eller fjerner medarbejderpladser, tildeler gateways og overvåger aktive forbindelser.

Q7: Hvordan sikrer MFA virksomhedens VPN?

Ved at kræve en ekstra kode (fx fra en godkendelsesapp), så stjålne adgangskoder ikke giver adgang.

Q8: Kan man revidere medarbejdernes forbindelseshistorik?

Ja, virksomheds-VPN'er logger tidspunkter, varighed og tildelte IP-adresser til brug for revision.

Q9: Hvad er ZTNA?

Zero Trust Network Access – en sikkerhedsmodel, der kun giver adgang til bestemte programmer, ikke til hele netværket.

Q10: Hvilken rolle spiller gateway-knudepunkter?

De er sikre indgangspunkter for fjerntrafik og sender data direkte videre til firmaets private servere.

Kontrolpunkt 10: Avanceret VPN-FAQ (del C)

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

Q1: Hvordan beskytter IPsec site-til-site-kommunikation?

IPsec krypterer trafikken på netværkslaget med Encapsulating Security Payload (ESP) og sikrer fortrolighed og integritet.

Q2: Hvorfor slår perimetersikkerhed fejl ved fjernarbejde?

Fordi medarbejdere tilgår data fra mange steder og enheder, hvilket gør én samlet firewallgrænse forældet.

Q3: Hvordan indfører IT-ansvarlige automatisk tildeling?

Ved at koble SCIM-protokoller mellem identitetsudbyderen (Okta) og VPN-konsollen, så brugerkataloger synkroniseres.

Q4: Hvad er fordelen ved split tunneling i virksomheder?

Den sender lokal SaaS-trafik (fx Microsoft 365) uden om VPN-tunnelen og sparer dermed virksomhedsgatewayens båndbredde til private databaser.

Q5: Hvordan kontrollerer enhedstjek sikkerheden på klienten?

VPN-klienten scanner enheden før forbindelsen og kontrollerer, at firewallen er aktiv, antivirus kører, og styresystemet er opdateret.

Kontrolpunkt 10: Avanceret VPN-FAQ (del D)

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

Q6: Hvilken rolle spiller NAT-traversal i virksomheds-VPN?

NAT-T pakker IPsec-pakker ind i UDP, så de kan passere hjemmeroutere og firewalls uden afbrydelser.

Q7: Hvordan undgår virksomheder flaskehalse på gatewayen?

Ved at opsætte flere regionale gateway-knudepunkter og fordele trafikken mellem dem med load balancere.

Q8: Hvorfor foretrækkes statiske hvidlister frem for dynamiske?

Statiske hvidlister forhindrer ukendte eksterne IP-adresser i at forsøge at forbinde og mindsker angrebsfladen markant.

Q9: Hvilken rolle spiller certifikatbaseret godkendelse?

Den kontrollerer unikke digitale certifikater på firmaets administrerede enheder og blokerer private computere.

Q10: Hvordan mindsker ZTNA risikoen for sideværts bevægelse?

Ved at begrænse brugersessioner til bestemte godkendte ressourcer, så hackere ikke kan bevæge sig videre i netværket.

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

Zero Trust-arkitektur kontrollerer løbende sikkerhedstilstanden på hver enhed, der forsøger at forbinde.

2. VPN-INDSIGT

Dedikerede IP-gateways lader virksomheder låse databaser i skyen ved at hvidliste statiske adresser.

3. VPN-INDSIGT

IPsec er branchestandarden til opsætning af sikre site-til-site-tunneler mellem kontorer.

4. VPN-INDSIGT

Administrationskonsoller lader IT-afdelingen tildele, styre og revidere medarbejdernes VPN-pladser.

5. VPN-INDSIGT

Single Sign-On integrerer VPN-adgang med virksomhedens identitetsudbydere som Okta og Entra ID.

6. VPN-INDSIGT

Flerfaktorgodkendelse blokerer uautoriserede forbindelsesforsøg med stjålne adgangskoder.

7. VPN-INDSIGT

Split tunneling optimerer firmaets båndbredde ved at holde offentlig SaaS-trafik uden for tunnelen.

8. VPN-INDSIGT

Enhedstjek kontrollerer de lokale sikkerhedsindstillinger, før der gives adgang til firmaets servere.

9. VPN-INDSIGT

SCIM-synkronisering automatiserer adgangsstyring ved ansættelse og fratrædelse.

10. VPN-INDSIGT

Zero Trust-netværksadgang begrænser adgangen til bestemte godkendte programmer og hindrer sideværts bevægelse.

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). Best VPN for Business: Tested & Ranked By Our Experts.

https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.

https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.

https://nordlayer.com/

Facitliste: Kontrolpunkt 1 – Flervalg

1 **Zero Trust** ZTNA-MODEL — Rigtigt svar: A

UNDERVISNINGSNOTE

Zero Trust-modeller kontrollerer løbende enhedens tilstand før adgang til netværket.

2 **Dedikeret IP** STATISK IP — Rigtigt svar: A

UNDERVISNINGSNOTE

Dedikerede IP-adresser gør det muligt at hvidliste gateways og blokere offentlig trafik.

3 **IPsec-standard** IPSEC-TUNNEL — Rigtigt svar: A

UNDERVISNINGSNOTE

IPsec er standardprotokollen til site-til-site-tunneler mellem filialer.

4 **IT-tildeling** ADMINISTRATIONSKONSOL — Rigtigt svar: A

UNDERVISNINGSNOTE

Centrale administrationspaneler lader IT-ansvarlige tildele pladslicenser.

5 **Spørgsmål 5** — Rigtigt svar: A

UNDERVISNINGSNOTE

Hvilken godkendelsesstandard gør det muligt at logge ind via Okta eller Microsoft Entra ID? → Single Sign-On

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Zero Trust** ZTNA-KONTROLLER — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Zero Trust-modeller kontrollerer løbende enhedens tilstand før adgang til netværket.

7 **Spørgsmål 7** — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Dedikerede IP-adresser er forbeholdt én virksomhed, så dens trafik ikke blandes med andre brugeres.

8 **IT-tildeling** IT-ADMINISTRERET PLADS — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Centrale administrationspaneler lader IT-ansvarlige tildele pladslicenser.

9 **IPsec-standard** SITE-TIL-SITE — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

IPsec er standardprotokollen til site-til-site-tunneler mellem filialer.

10 **Okta SSO-kobling** SSO-LOGIN — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Single Sign-On kobler VPN-login sammen med firmakataloger som Okta.

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

H 1. ZERO TRUST	D 2. DEDIKERET IP	E 3. IPSEC	G 4. ADMINKONSOL
B 5. SINGLE SIGN-ON	C 6. FLERFAKTOR	F 7. GATEWAY	A 8. TILDELING

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 ZERO TRUST	2 DEDIKERET IP	3 IPSEC	4 ADMINKONSOL
5 SINGLE SIGN-ON	6 FLERFAKTOR		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 B – DEDIKERETIP	2 G – GATEWAY	3 H – TILDELING	4 F – FLERFAKTOR
5 C – IPSEC	6 A – ZEROTRUST	7 E – SINGLESIGNON	8 D – ADMINKONSOL

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare ZERO TRUST, DEDIKERET IP og IPSEC med egne ord og give et eksempel på hvert begreb.

Casestudier:
Bed eleverne begrunde deres anbefalinger med fakta fra opgavearket frem for antagelser.

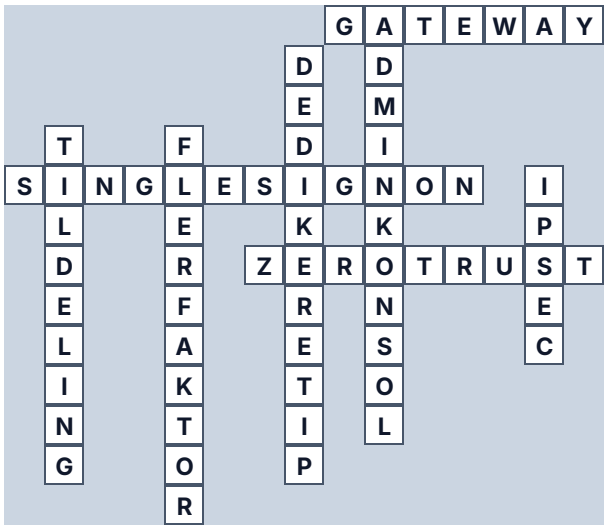
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

1 vandret: GATEWAY Knudepunkt, der router indgangen til netværket (7 bogstaver)

6 vandret: SINGLESIGNON Identitetskobling til Okta og Entra ID (12 bogstaver)

8 vandret: ZEROTRUST Rammeværk med løbende verifikation af tillid (9 bogstaver)

LODRETTE NØGLER

2 lodret: ADMINKONSOL Central portal, hvor IT-administratoren styrer pladser (11 bogstaver)

3 lodret: DEDIKERETIP Statisk gateway-adresse til hvidlistning (11 bogstaver)

4 lodret: TILDELING Fordeling af VPN-adgangslicenser til medarbejdere (9 bogstaver)

5 lodret: FLERFAKTOR Loginsikkerhed, der kræver ekstra koder (10 bogstaver)

7 lodret: IPSEC Standard for site-til-site-tunneler (5 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1.	RTOEZUSTR	ZEROTRUST	5.	TEERDPKEDII	DEDIKERETIP
2.	ICESP	IPSEC	6.	NLKNOSADOMI	ADMINKONSOL
3.	SIISOGNENLNG	SINGLESIGNON	7.	LRFKATORFE	FLERFAKTOR
4.	YAWEAGT	GATEWAY	8.	GENTDILIL	TILDELING

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"VERIFICER HVER ENHED FØR DU GIVER ADGANG"

Facit til casestudier

A Casestudie 1: Overgang til Zero Trust

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En virksomhed vil sikre sine lokale servere ved løbende at kontrollere enhedernes certifikater, firewallstatus og brugerens placering frem for at stole på alle inde i netværket.
- Anbefalet strategi og løsning: Chefen bør skifte til en model med Zero Trust-netværksadgang (ZTNA), der håndhæver løbende, kontekstbaserede sikkerhedstjek.

B Casestudie 2: Begrænsning af gateway

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En virksomhed har private finansdatabaser i skyen. De vil blokere al offentlig adgang til administrationspanelerne og kun tillade login fra verificerede firmaenheder.
- Anbefalet strategi og løsning: Administratoren bør opsætte en gateway med dedikeret IP på virksomhedens VPN og hvidliste denne statiske adresse i skyens databasefirewall.