Navn: _____ Dato: _____ Poeng: _____

# VPN for bedrifter

Innføring av Zero Trust-nettverkstilgang, dedikerte gateway-noder og sentraliserte administratorkontroller for bedriften.

## LÆRINGSOVERSIKT: VPN-NETTVERK FOR BEDRIFTER

**ELEV**
**STUDENTSTATUS**
Spor for nettverksforsvarere

**SIKKER**
**TILKOBLINGSSTATUS**
Beskytte datapakker

**AKTIV**
**LEKKASJEBESKYTTELSE**
DNS- og IPv6-lekkasjebeskyttelse

**Velkommen!** Dette aktivitetsheftet veileder deg gjennom VPN-nettverk for bedrifter. Du utforsker Zero Trust-arkitekturer, dedikerte gatewayer med statisk IP, administratorkonsoller, klargjøring og IPsec-tunneler mellom nettsteder.

**KONTROLLPUNKTER I ARBEIDSARKET**

- [ ] **Del 1-4: Behersk VPN- og nettverkssikkerhetskonfigurasjoner.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

**Åpne VPN.coms veiledning om de beste VPN-ene**

URL: https://www.vpn.com/no/vpn/beste-vpn-for-bedrifter/enterprise/

# Din læringsveiledning for VPN-nettverk i bedrifter

- Innfør rammeverk for Zero Trust Network Access (ZTNA).
- Konfigurer dedikerte IP-adresser for servergatewayer til hvitelistefiltre.
- Administrere sentraliserte administrasjonspaneler for bedrifter og lister over brukerlisenser.
- Revider tilgangslogger for nettverket og brukernes tilkoblingshistorikk.
- Konfigurer regler for enkel pålogging (SSO) og flerfaktorautentisering.
- Sett opp site-to-site IPsec-tunneler mellom avdelinger.

## INSTRUKSJONER FOR VPN-NETTVERK FOR BEDRIFTER

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på Zero Trust og IPsec mellom nettsteder (site-to-site). Avslutt med bonusaktiviteten Tenk raskt.

## ZERO TRUST-ARKITEKTURER OG DEDIKERTE GATEWAYER (INNLEDNING)

VPN-er for bedrifter sikrer virksomhetens eiendeler ved å gå over til rammeverk for Zero Trust Network Access (ZTNA) og hviteliste dedikerte, statiske IP-gatewayer. IT-sjefer bruker sentraliserte administrasjonskonsoller til å orkestrere site-to-site IPsec-tunneler og lenker for enkel pålogging (SSO).

**LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.**

## Kontrollpunkt 1: Flervalgsutfordring

1. **1. Hvilken sikkerhetsmodell erstatter eldre VPN-er for bedrifter?**
   - A) Zero Trust
   - B) Multi-hop
   - C) Peer-to-peer
   - D) Én enkelt gateway

2. **2. Hvilken funksjon kreves for å begrense databasetilgang til bedriftens servere?**
   - A) Dedikert IP
   - B) Dynamisk ruting
   - C) Delt tunnel
   - D) DNS-proxy

3. **3. Hvilken protokoll er standarden for tunneler mellom bedriftsnettverk (site-to-site)?**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **4. Hvilket sentralt verktøy lar administratorer styre ansattes lisensplasser?**
   - A) Administratorkonsoll
   - B) Registernøkkel
   - C) Ruterfirmware
   - D) Systemlogg

5. **5. Hvilken autentiseringsstandard gjør det mulig å logge inn via Okta eller Microsoft Entra ID?**
   - A) Single Sign-On
   - B) Delt hemmelighet
   - C) EPP-autentisering
   - D) WEP-nøkkel

## Kontrollpunkt 2: Utfordring med sant eller usant

**6 Spørsmål 6**

6. Zero Trust Network Access gir bare nettverkstilgang etter at kontinuerlig tillit til enheten er verifisert.

○ Sant ○ Usant

**7 Spørsmål 7**

7. Gatewayer med dedikert IP ruter ansattes trafikk side om side med tilfeldige offentlige forbrukerbrukere.

○ Sant ○ Usant

**8 Spørsmål 8**

8. Sentraliserte administratorkonsoller lar IT-ledere umiddelbart trekke tilbake enkeltansattes plasser.

○ Sant ○ Usant

**9 Spørsmål 9**

9. IPsec er en lettvektsprotokoll som ikke støtter site-to-site-nettverkstunneler.

○ Sant ○ Usant

**10 Spørsmål 10**

10. Single Sign-On gir sikker autentisering av ansatte via bedriftens identitetsleverandører.

○ Sant ○ Usant

## Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. Moderne sikkerhetsarkitekturer erstatter eldre tunneler med _____ -tilgang.
2. For å begrense databasetilgang setter bedrifter opp en gateway-adresse med _____ .
3. Filialkontorer kobles sikkert sammen med tunneler av typen _____ mellom steder.
4. IT-administratorer tildeler brukerlisenser til ansatte i den sentrale _____ .
5. Okta-integrasjon lar ansatte autentisere seg via bedriftens _____ .
6. For å beskytte påloggінger krever bedriftsportaler _____ -autentisering.

**ORDBANK**

ADMIN-KONSOLL | DEDIKERT IP | ENKEL PÅLOGGING | FLERFAKTOR | INNGANGSNODE | IPSEC | NULLTILLIT | PROVISJONERING

**Skriv svarene dine her:**

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

# Kontrollpunkt 4: Koble nøkkelbegreper

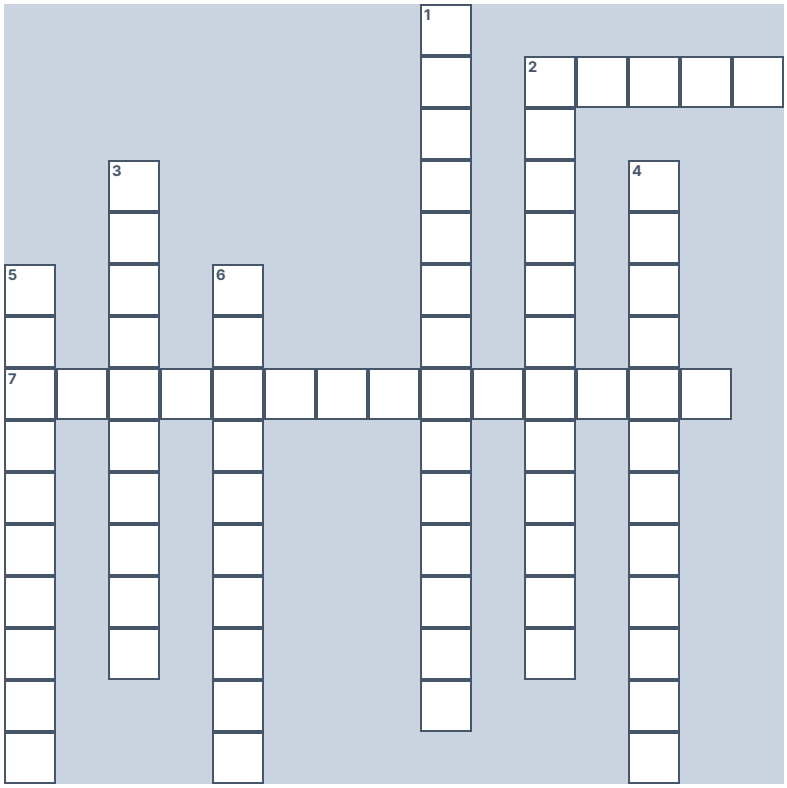
**KOBLE DEFINISJONER**

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

| | | | |
|---|---|---|---|
| ☐ | 1. ZERO TRUST | A | Tildeling av VPN-tilgangslisenser til ansatte. |
| ☐ | 2. DEDIKERT IP | B | Identitetskoblingen til Okta og Entra ID. |
| ☐ | 3. IPSEC | C | Påloggingssikkerhet som krever ekstra tokener. |
| ☐ | 4. ADMINCONSOLE | D | Statisk hviteliste-gatewayadresse. |
| ☐ | 5. SINGLE SIGN-ON | E | Standard for site-to-site-tunneler. |
| ☐ | 6. FLERFAKTOR | F | Rutingnode for inngang til nettverket. |
| ☐ | 7. GATEWAY | G | Sentral portal for IT-lederens plasser. |
| ☐ | 8. PROVISJONERING | H | Rammeverk for kontinuerlig verifisering av tillit. |

## Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.




### VANNRETT

**2. Standard for tunneler mellom steder (5)**

**7. Identitetskobling mot Okta og Entra ID (14)**

### LODDRETT

**1. Tildeling av VPN-tilgangslisenser til ansatte (14)**

**2. Rutingnode ved nettverkets inngang (12)**

**3. Statisk hvitelistet gateway-adresse (10)**

**4. Sentral portal der IT-ansvarlige styrer brukerplasser (12)**

**5. Påloggingssikkerhet som krever ekstra tokens (10)**

**6. Rammeverk for kontinuerlig verifisering av tillit (10)**

# Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

## VANNRETT

**2 vannrett: Standard for tunneler mellom steder (5 bokstaver):**

**7 vannrett: Identitetskobling mot Okta og Entra ID (14 bokstaver):**

## LODDRETT

**1 loddrett: Tildeling av VPN-tilgangslisenser til ansatte (14 bokstaver):**

**2 loddrett: Rutingnode ved nettverkets inngang (12 bokstaver):**

**3 loddrett: Statisk hvitelistet gateway-adresse (10 bokstaver):**

**4 loddrett: Sentral portal der IT-ansvarlige styrer brukerplasser (12 bokstaver):**

**5 loddrett: Påloggingssikkerhet som krever ekstra tokens (10 bokstaver):**

**6 loddrett: Rammeverk for kontinuerlig verifisering av tillit (10 bokstaver):**

## Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

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

**ORDLISTE**

NULLTILLIT DEDIKERTIP IPSEC ADMINKONSOLL ENKELPÅLOGGING
FLERFAKTOR INNGANGSNODE PROVISJONERING

## Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

| BEGREPER |
| --- |
| A. NULLTILLIT |
| B. DEDIKERTIP |
| C. IPSEC |
| D. ADMINKONSOLL |
| E. ENKELPÅLOGGING |
| F. FLERFAKTOR |
| G. INNGANGSNODE |
| H. PROVISJONERING |

| DEFINISJONER OG TILHØRENDE FELT |
| --- |
| [ ] 1. Statisk hvitelistet gateway-adresse. |
| [ ] 2. Rutingnode ved nettverkets inngang. |
| [ ] 3. Tildeling av VPN-tilgangslisenser til ansatte. |
| [ ] 4. Påloggingssikkerhet som krever ekstra tokens. |
| [ ] 5. Standard for tunneler mellom steder. |
| [ ] 6. Rammeverk for kontinuerlig verifisering av tillit. |
| [ ] 7. Identitetskobling mot Okta og Entra ID. |
| [ ] 8. Sentral portal der IT-ansvarlige styrer brukerplasser. |

## Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper fra dette arbeidsarket. Skriv svarene dine i svarboksene.

1. ILITUNLTLL
2. ICESP
3. EONNLGGGKÅ LPIE
4. DSANGENONI NG
5. TEPEIRKDID
6. LNSOKLNADO MI
7. LRFKATORFE
8. VOISNERGPJ ONRI

# Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

| | | | | |
|---|---|---|---|---|
| 1 | Verktøy et selskap bruker hver dag | | | |
| 2 | Ting en VPN kan skjule | | | |
| 3 | Roller i en IT-avdeling | | | |
| 4 | Ord som beskriver Zero Trust | | | |
| 5 | Måter å logge inn sikkert på | | | |
| 6 | Grunner til å gi ansatte en VPN | | | |
| 7 | Ting å gjøre etter et sikkerhetsbrudd | | | |
| 8 | Grunner til å bruke en VPN på reise | | | |
| 9 | Regler for sikkert hjemmekontor | | | |
| 10 | Data et selskap må beskytte | | | |
| 11 | Ting som kan forstyrre et videomøte | | | |
| 12 | Enheter som kan bruke en VPN | | | |
| 13 | Kontorprogrammer du kjenner til | | | |
| 14 | Steder ansatte jobber fra | | | |
| 15 | Enheter en ansatt kan ha | | | |

# Kontrollpunkt 8: Casestudier om VPN og nettverk

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

### CASESTUDIE 1: MIGRERING TIL NULLTILLIT

👷

**Scenario:** En bedrift vil sikre de lokale serverne sine ved fortløpende å kontrollere enhetenes samsvarssertifikater, brannmurstatus og brukerens plassering, i stedet for å stole på alle som er inne i nettverket.

**Diskusjonsspørsmål:** Hvilket rammeverk bør IT-sikkerhetssjefen innføre for å oppnå dette?

### CASESTUDIE 2: BEGRENSNING VED GATEWAY

👷

**Scenario:** Et selskap har private finansdatabaser i skyen. Det vil blokkere all offentlig internetttilgang til administrasjonspanelene og kun tillate innlogging fra verifiserte selskapsenheter.

**Diskusjonsspørsmål:** Hvilken nettverkskonfigurasjon bør databaseadministratoren sette opp i skybrannmuren?

# Kontrollpunkt 9: Knekk chifferet

En nettverksingeniør sikrer rutingkanaler og klienttunneler. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

**NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL**

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

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 21 | 12 | 12 | 20 | 9 | 12 | 12 | 9 | 20 | | 19 | 10 | 5 | 11 | 11 | 5 | 18 |
| | | | | | | | | | | | | | | | | |
| 8 | 22 | 5 | 18 | | 5 | 14 | 8 | 5 | 20 | | 16 | 29 | | | | |
| | | | | | | | | | | | | | | | | |
| 14 | 5 | 20 | 20 | 22 | 5 | 18 | 11 | 5 | 20 | | | | | | | |
| | | | | | | | | | | | | | | | | |

**Dekodet melding:**

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

# Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del A)

Gå gjennom de vanligste spørsmålene og svarene om virtuelle private nettverk (VPN-er) og tunnelering.

### Q1: Hva er en VPN for store virksomheter (enterprise)?

En sikker nettverkstunnel utformet for bedrifter som lar fjernarbeidere få tilgang til bedriftsnettverk med sentralisert administrasjon.

### Q2: Hvordan skiller Zero Trust seg fra tradisjonelle VPN-er?

Tradisjonelle VPN-er stoler på alle inne i tunnelen, mens Zero Trust kontinuerlig verifiserer hver enhet og hver brukertilkobling.

### Q3: Hva er en dedikert IP-adresse i bedrifts-VPN-er?

En statisk IP-adresse reservert utelukkende for virksomheten din, slik at du kan hviteliste den for sikker tilgang til skydatabaser.

### Q4: Hvorfor er SSO viktig for bedrifts-VPN-er?

Single Sign-On lar ansatte bruke bedriftspåloggingene sine (som Okta eller Microsoft Entra ID) til å logge inn på en sikker måte.

### Q5: Hva er en nettsted-til-nettsted-VPN?

En tunnel som kobler sammen to fysiske kontorer (som et avdelingskontor og hovedkontoret) over det offentlige internett ved hjelp av IPsec.

# Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del B)

Gå gjennom de vanligste spørsmålene og svarene om virtuelle private nettverk (VPN-er) og tunnelering.

### Q6: Hva er funksjonen til en administratorkonsoll?

Et dashbord for IT-administratorer for å legge til eller fjerne ansattplasser, tildele gatewayer og overvåke aktive tilkoblinger.

### Q7: Hvordan sikrer MFA bedrifts-VPN-er?

Ved å kreve en sekundær kode (som et token fra en autentiseringsapp) for å hindre uautorisert tilgang fra kompromitterte passord.

### Q8: Kan jeg revidere ansattes tilkoblingshistorikk?

Ja, bedrifts-VPN-er logger tidspunkter for tilkobling, varighet og tildelte IP-adresser for samsvarsrevisjon.

### Q9: Hva er ZTNA?

Zero Trust Network Access, en sikkerhetsmodell som bare gir tilgang til bestemte applikasjoner i stedet for hele nettverket.

### Q10: Hva er rollen til gatewaynoder?

De fungerer som sikre inngangspunkter for fjerntrafikk og ruter data direkte til private bedriftsservere.

# Kontrollpunkt 10: Avanserte vanlige spørsmål om VPN (Del C)

Utforsk avanserte tekniske sider ved VPN-tunnelprotokoller, integrering av mobilklienter og utrulling i bedrifter.

### Q1: Hvordan beskytter IPsec kommunikasjon mellom bedriftens nettsteder?

IPsec krypterer trafikk på nettverkslaget ved hjelp av Encapsulating Security Payload (ESP) for å sikre datas konfidensialitet og integritet.

### Q2: Hvorfor svikter tradisjonell perimeterbasert sikkerhet for ansatte som jobber eksternt?

Fordi ansatte får tilgang til data fra flere steder og enheter, noe som gjør en enkelt nettverksbrannmur som perimeter foreldet.

### Q3: Hvordan implementerer IT-ledere automatisert klargjøring?

Ved å kartlegge SCIM-protokoller mellom identitetsleverandører (Okta) og VPN-administrasjonskonsollen for å synkronisere brukerkataloger.

### Q4: Hva er fordelen med split tunneling i bedriftsmiljøer?

Den ruter lokal SaaS-trafikk (som Microsoft 365) utenfor VPN-tunnelen og sparer bedriftens gateway-båndbredde til private databaser.

### Q5: Hvordan validerer enhetssjekker av sikkerhetstilstand (device posture checks) sikkerheten til endepunkter?

VPN-klienten skanner enheten før tilkobling for å kontrollere at brannmuren er aktiv, at antivirusprogrammet kjører og at operativsystemet har siste oppdateringer.

# Kontrollpunkt 10: Avanserte vanlige spørsmål om VPN (Del D)

Utforsk avanserte tekniske sider ved VPN-tunnelprotokoller, integrering av mobilklienter og utrulling i bedrifter.

### Q6: Hvilken rolle spiller NAT traversal i oppsett av bedrifts-VPN?

NAT-T kapsler inn IPsec-pakker i UDP slik at de kan passere hjemmerutere og brannmurer uten at tilkoblingen faller ut.

### Q7: Hvordan forhindrer virksomheter flaskehals i gatewayens båndbredde?

Ved å sette opp flere regionale gateway-noder og fordele innkommende brukertrafikk mellom dem med lastbalansere.

### Q8: Hvorfor foretrekkes hvitelister med statiske IP-adresser framfor dynamiske?

Statiske hvitelister hindrer uautoriserte eksterne IP-adresser i å forsøke tilkoblingshåndtrykk og reduserer angrepsflaten dramatisk.

### Q9: Hvilken rolle spiller sertifikatbasert autentisering i bedrifts-VPN-er?

Den validerer unike digitale sertifikater som er installert på bedriftsadministrerte enheter, og blokkerer uadministrerte personlige datamaskiner.

### Q10: Hvordan reduserer ZTNA risikoen for lateral bevegelse?

Ved å isolere brukerøkter til bestemte autoriserte ressurser, slik at hackere ikke kan bevege seg gjennom nettverket hvis én node brytes.

# Del 11: 10 fakta om VPN fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om VPN-krypteringshastigheter, protokollrevisjoner, mobiltilkobling og fjernarbeid i bedrifter.

**1. VPN-INNSIKT**

Zero Trust-arkitekturer verifiserer kontinuerlig sikkerhetstilstanden til hver enhet som forsøker å koble til et nettverk.

**2. VPN-INNSIKT**

Gatewayer med dedikert IP gjør det mulig for bedrifter å låse ned skydatabaser ved å hviteliste statiske adresser.

**3. VPN-INNSIKT**

IPsec er bransjestandarden for å konfigurere sikre site-to-site-tunneler mellom kontornettverk.

**4. VPN-INNSIKT**

Administratorkonsoller lar IT-avdelinger tildele, administrere og revidere ansattes VPN-tilgangsplasser.

**5. VPN-INNSIKT**

Single Sign-On integrerer VPN-tilgang med bedriftens identitetsleverandører som Okta og Entra ID.

**6. VPN-INNSIKT**

Flerfaktorautentisering blokkerer uautoriserte tilkoblingsforsøk som stammer fra stjålne passordnøkler.

**7. VPN-INNSIKT**

Split tunneling optimaliserer bedriftens båndbredde ved å utelate offentlig SaaS-trafikk fra den krypterte tunnelen.

**8. VPN-INNSIKT**

Kontroller av enhetens sikkerhetstilstand verifiserer lokale sikkerhetsinnstillinger før det gis tilgang til bedriftsservere.

**9. VPN-INNSIKT**

SCIM-katalogsynkronisering automatiserer tilgangskontroller ved ansettelse og avslutning av ansatte.

**10. VPN-INNSIKT**

Zero Trust Network Access begrenser brukertilgangen til bestemte godkjente applikasjoner og hindrer lateral bevegelse i nettverket.

# Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale tekniske standarder, spesifikasjoner og regelverk.

## FAGLIGE REFERANSER OG BRANSJEREFERANSER

[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/

## Fasit: Kontrollpunkt 1 – flervalg

**1** **Zero Trust** ZTNA-MODELL **Riktig svar: A**

### MERKNAD TIL LÆREREN

Zero Trust-modeller verifiserer kontinuerlig at enheter oppfyller kravene før de får tilgang til nettverket.

**2** **Dedikert IP** STATISK IP **Riktig svar: A**

### MERKNAD TIL LÆREREN

Dedikerte IP-adresser gjør det mulig å hviteliste gatewayer for å blokkere offentlig trafikk.

**3** **IPsec-standarden** IPSEC-TUNNEL **Riktig svar: A**

### MERKNAD TIL LÆREREN

IPsec er standardprotokollen som brukes til site-to-site-tunneler mellom filialer.

**4** **IT-tildeling** ADMINISTRATORKONSOLL **Riktig svar: A**

### MERKNAD TIL LÆREREN

Sentraliserte administratordashbord lar IT-ledere tildele plasslisenser.

**5** **Spørsmål 5** **Riktig svar: A**

### MERKNAD TIL LÆREREN

Hvilken autentiseringsstandard gjør det mulig å logge inn via Okta eller Microsoft Entra ID? → Single Sign-On

## Fasit: Kontrollpunkt 2 – sant eller usant

**6** **Zero Trust** ZTNA-KONTROLLER **Riktig svar: Sant**

### MERKNAD TIL LÆREREN

Zero Trust-modeller verifiserer kontinuerlig at enheter oppfyller kravene før de får tilgang til nettverket.

**7** **Spørsmål 7** **Riktig svar: Usant**

### MERKNAD TIL LÆREREN

Dedikerte IP-adresser er reservert for én bedrift, så trafikken blandes ikke med andre brukere.

**8** **IT-tildeling** IT-ADMINISTRATORLISENS **Riktig svar: Sant**

### MERKNAD TIL LÆREREN

Sentraliserte administratordashbord lar IT-ledere tildele plasslisenser.

**9** **IPsec-standarden** SITE-TIL-SITE **Riktig svar: Usant**

### MERKNAD TIL LÆREREN

IPsec er standardprotokollen som brukes til site-to-site-tunneler mellom filialer.

**10** **Okta SSO-lenke** SSO-INNLOGGING **Riktig svar: Sant**

### MERKNAD TIL LÆREREN

Single Sign-On integrerer VPN-påloggінger med bedriftskataloger som Okta.

# Fasit for ordforråd og vurderingsmatrise

**Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).**

## KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

| | | | |
|---|---|---|---|
| H 1. ZERO TRUST | D 2. DEDIKERT IP | E 3. IPSEC | G 4. ADMINCONSOLE |
| B 5. SINGLE SIGN-ON | C 6. FLERFAKTOR | F 7. GATEWAY | A 8. PROVISJONERING |

## KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

| | | | |
|---|---|---|---|
| 1 NULLTILLIT | 2 DEDIKERT IP | 3 IPSEC | 4 ADMIN-KONSOLL |
| 5 ENKEL PÅLOGGING | 6 FLERFAKTOR | | |

## KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

| | | | |
|---|---|---|---|
| 1 B – DEDIKERTIP | 2 G – INNGANGSNODE | 3 H – PROVISJONERING | 4 F – FLERFAKTOR |
| 5 C – IPSEC | 6 A – NULLTILLIT | 7 E – ENKELPÅLOGGING | 8 D – ADMINKONSOLL |

## DISKUSJONSNOTATER TIL LÆRERE

**Nøkkelbegreper:**
Kontroller at elevene kan forklare ZERO TRUST, DEDIKERT IP og IPSEC med egne ord og gi et eksempel på hvert.

**Casestudier:**
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

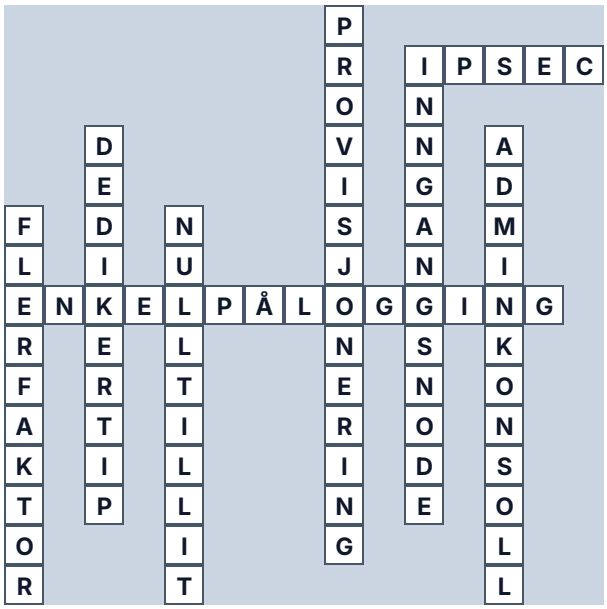
**Kildevurdering:**
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

# Fasit for oppgavene og merknader til læreren

## LØSNING PÅ ORDSØKET

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

## KRYSSORDLØSNING




## LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

### VANNRETT

**2 vannrett: IPSEC** Standard for tunneler mellom steder (5 bokstaver)

**7 vannrett: ENKELPÅLOGGING** Identitetskobling mot Okta og Entra ID (14 bokstaver)

### LODDRETT

**1 loddrett: PROVISJONERING** Tildeling av VPN-tilgangslisenser til ansatte (14 bokstaver)

**2 loddrett: INNGANGSNODE** Rutingnode ved nettverkets inngang (12 bokstaver)

**3 loddrett: DEDIKERTIP** Statisk hvitelistet gateway-adresse (10 bokstaver)

**4 loddrett: ADMINKONSOLL** Sentral portal der IT-ansvarlige styrer brukerplasser (12 bokstaver)

**5 loddrett: FLERFAKTOR** Påloggingssikkerhet som krever ekstra tokens (10 bokstaver)

**6 loddrett: NULLTILLIT** Rammeverk for kontinuerlig verifisering av tillit (10 bokstaver)

# Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

### FASIT: BOKSTAVBLANDING

1. I L I T U N L T L L — **NULLTILLIT**
2. I C E S P — **IPSEC**
3. E O N N L G G G K Å L P I E — **ENKELPÅLOGGING**
4. D S A N G E N O N I N G — **INNGANGSNODE**
5. T E P E I R K D I D — **DEDIKERTIP**
6. L N S O K L N A D O M I — **ADMINKONSOLL**
7. L R F K A T O R F E — **FLERFAKTOR**
8. V O I S N E R G P J O N R I — **PROVISJONERING**

### FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

**"NULLTILLIT SJEKKER HVER ENHET PÅ NETTVERKET"**

# Fasit til casestudiene

## A Casestudie 1: Migrering til nulltillit

Løsning for læreren

### RETTEVEILEDNING

**Elevsvar bør dekke følgende punkter:**

- Scenarioanalyse: En bedrift vil sikre de lokale serverne sine ved å fortløpende verifisere enhetenes samsvarssertifikater, brannmurstatus og brukerens plassering i stedet for å stole på alle som er inne i nettverket.
- Anbefalt strategi og løsning: Direktøren bør gå over til en modell med Zero Trust Network Access (ZTNA), som håndhever kontinuerlige kontekstbaserte sikkerhetskontroller.

## B Casestudie 2: Begrensning ved gateway

Løsning for læreren

### RETTEVEILEDNING

**Elevsvar bør dekke følgende punkter:**

- Scenarioanalyse: Et selskap hoster private finansdatabaser i skyen. Det vil blokkere all offentlig internetttilgang til administrasjonspanelene og bare tillate innlogging fra verifiserte selskapsendepunkter.
- Anbefalt strategi og løsning: Administratoren bør konfigurere en Dedicated IP-gateway på bedriftens VPN og hviteliste denne statiske adressen i brannmuren til skydatabasen.