Navn: _____ Dato: _____ Poeng: _____

VPN for ekstern tilgang

Sikring av endepunkter for eksterne ansatte, flerfaktorautentisering og konfigurasjon av IPsec-tunneler.

LÆRINGSOVERSIKT OM FJERNTILGANGS-VPN-ER

ELEV
STUDENTSTATUS
Spor for nettverksforsvarere

SIKKER
TILKOBLINGSSTATUS
Beskytte datapakker

AKTIV
LEKKASJEBESKYTTELSE
DNS- og IPv6-lekkasjebeskyttelse

Velkommen! Dette aktivitetsheftet veileder deg gjennom VPN-nettverk for fjerntilgang. Du utforsker tunneler fra klient til nettsted, flerfaktorinnlogginger, tilstandskontroller av endepunkter, båndbreddegrenser og sikkerhetsrevisjon med syslog.

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/fjerntilgang/

Din læringsveiledning for VPN for fjerntilgang

- Sikre endepunkter for eksterne ansatte som får tilgang til lokale nettverksnoder.
- Konfigurer policyer for flerfaktorautentisering for fjernpåloggінger.
- Sett opp IPsec- og OpenVPN-konfigurasjoner fra klient til nettsted.
- Revider logger over eksterne tilkoblinger for brudd på tilgangskontroll.
- Innfør kontroller av enhetens sikkerhetstilstand før nettverkstilkoblinger gis.
- Optimaliser serverens gjennomstrømming for å unngå flaskehals i båndbredden ved fjernarbeid.

INSTRUKSJONER FOR FJERNTILGANGS-VPN-ER

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på sikkerhetssjekker av enheten og flerfaktorpåloggінger. Avslutt med bonusaktiviteten Tenk raskt.

KLIENT-TIL-NETTSTED-TUNNELER OG ENDEPUNKTOVERHOLDELSE (INNLEDNING)

VPN for ekstern tilgang oppretter sikre tunneler mellom klient og nettsted for ansatte utenfor kontoret. For å sikre disse tilkoblingene må du håndheve innlogging med flerfaktorautentisering (MFA), utføre samsvarskontroller av endepunktenes sikkerhetstilstand og revidere logger via sentrale syslog-innsamlere.

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

Kontrollpunkt 1: Flervalgsutfordring

1. **1. Hvilken autentiseringsstandard bør portaler for VPN med ekstern tilgang kreve?**
   - A) Flerfaktor
   - B) Enkeltfaktor
   - C) Ukryptert
   - D) Lokal gjest

2. **2. Hvilken protokoll er standarden for å sikre klient-til-nettverk-tilkoblinger for fjernarbeid?**
   - A) OpenVPN
   - B) SOCKS5
   - C) PPTP
   - D) FTP

3. **3. Hvilken kontroll validerer om en ekstern bærbar PC er ren før den kobler til?**
   - A) Tilstandskontroll
   - B) Hastighetstest
   - C) Ping-test
   - D) Minnemengde

4. **4. Hvor lagres tilkoblingslogger for eksterne medarbeidere for sikkerhetsrevisjon?**
   - A) Syslog-server
   - B) Registernøkkel
   - C) Klientminne
   - D) Nettleser

5. **5. Hvilket problem oppstår når antallet eksterne ansatte overstiger gatewayens båndbreddekapasitet?**
   - A) Båndbreddestrupe
   - B) DNS-lekkasje
   - C) Håndtrykk bestått
   - D) Eksponering av IP-adresse

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Flerfaktorautentisering legger til et sekundært valideringstoken for å sikre eksterne påloggінger.

○ Sant ○ Usant

7 Spørsmål 7

7. Sikkerhetstilstandskontroller lar eksterne enheter med deaktiverte brannmurer få tilgang til private servere.

○ Sant ○ Usant

8 Spørsmål 8

8. Logger fra VPN for ekstern tilgang er avgjørende for å spore uautorisert tilgang til bedriftsnettverket.

○ Sant ○ Usant

9 Spørsmål 9

9. OpenVPN og IPsec er eldre protokoller som ikke krypterer nyttelasten til eksterne klienter.

○ Sant ○ Usant

10 Spørsmål 10

10. Flaskehals i gatewayens båndbredde oppstår når trafikk fra eksterne brukere overstiger kapasiteten til tilkoblingskortet.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. For å beskytte bedriftsportaler må eksterne påloggingerkreve _____ -autentisering.
2. Eksterne klienter krypterer tunnelens nyttelast med standardprotokollen _____ .
3. Enheter må bestå en sikkerhetskontroll av _____ før de får nettverkstilkobling.
4. Reviderbare tilgangslogger sendes kontinuerlig til en sentral _____ -server.
5. Tung trafikk i arbeidstiden kan føre til overbelastning av gatewayens _____ .
6. Drivere for virtuelle adaptere håndterer _____ mellom klient og nettsted under Windows og macOS.

ORDBANK

BRANNMUR BÅNDBREDDE FLERFAKTOR HELSESTATUS KRYPTERING
OPENVPN SYSLOG TUNNELERING

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble nøkkelbegreper

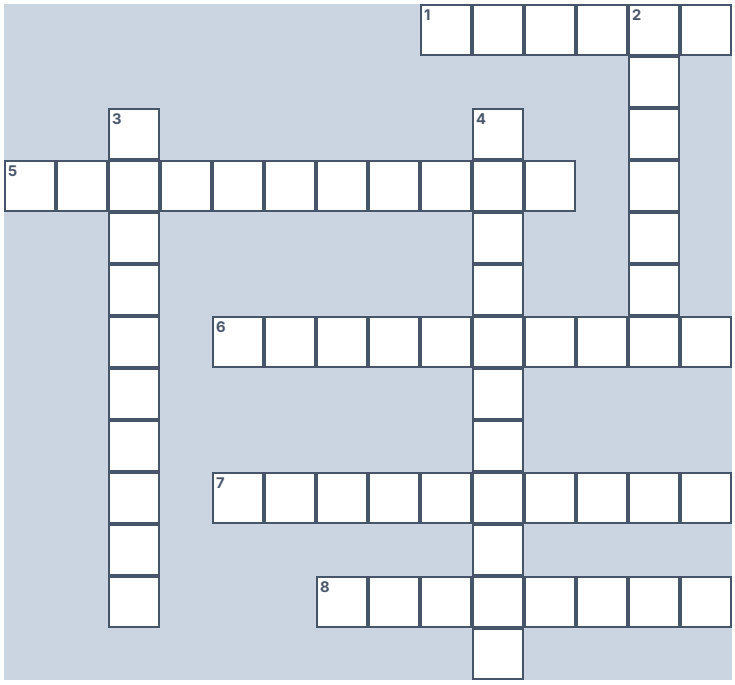
KOBLE DEFINISJONER

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

☐	1. FLERFAKTOR	A	Innkapsling av data i en sikker bane.
☐	2. OPENVPN	B	Sentral innsamler av sikkerhetslogger.
☐	3. SIKKERHETSTILSTAND	C	Grense for nettverkets datakapasitet.
☐	4. SYSLOG	D	Standard protokoll fra klient til nettsted.
☐	5. BÅNDBREDDE	E	Validering av ekstern enhets helsetilstand.
☐	6. KRYPTERING	F	Regler for trafikkfiltreringssystemet.
☐	7. TUNNELERING	G	Kryptografisk omblanding av pakker.
☐	8. BRANNMUR	H	Påloggingssikkerhet som krever ekstra tokener.

Kontrollpunkt 5: Kryssord

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



VANNRETT

1. Sentral innsamler av sikkerhetslogger (6)

5. Validering av en fjernenhets helsetilstand (11)

6. Kryptografisk sammenblanding av pakker (10)

7. Grense for nettverkets datakapasitet (10)

8. Regler for systemer som filtrerer trafikk (8)

LODDRETT

2. Standard protokoll mellom klient og nettsted (7)

3. Påloggingssikkerhet som krever ekstra tokens (10)

4. Innkapsling av data i en sikker bane (11)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

1 vannrett: Sentral innsamler av sikkerhetslogger (6 bokstaver):

5 vannrett: Validering av en fjernenhets helsetilstand (11 bokstaver):

6 vannrett: Kryptografisk sammenblanding av pakker (10 bokstaver):

7 vannrett: Grense for nettverkets datakapasitet (10 bokstaver):

8 vannrett: Regler for systemer som filtrerer trafikk (8 bokstaver):

LODDRETT

2 loddrett: Standard protokoll mellom klient og nettsted (7 bokstaver):

3 loddrett: Påloggingssikkerhet som krever ekstra tokens (10 bokstaver):

4 loddrett: Innkapsling av data i en sikker bane (11 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

FLERFAKTOR
OPENVPN
HELSESTATUS
SYSLOG
BÅNDBREDDE
KRYPTERING
TUNNELERING
BRANNMUR

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. FLERFAKTOR
B. OPENVPN
C. HELSESTATUS
D. SYSLOG
E. BÅNDBREDDE
F. KRYPTERING
G. TUNNELERING
H. BRANNMUR

DEFINISJONER OG TILHØRENDE FELT
[ ] 1. Sentral innsamler av sikkerhetslogger.
[ ] 2. Regler for systemer som filtrerer trafikk.
[ ] 3. Innkapsling av data i en sikker bane.
[ ] 4. Kryptografisk sammenblanding av pakker.
[ ] 5. Standard protokoll mellom klient og nettsted.
[ ] 6. Grense for nettverkets datakapasitet.
[ ] 7. Validering av en fjernenhets helsetilstand.
[ ] 8. Påloggingssikkerhet som krever ekstra tokens.

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. **OKAFLFTRRE** _____
2. **ESEHUSLTATS** _____
3. **BRDEÅBEDDN** _____
4. **ENGLNEIRTUN** _____
5. **VNNEOPP** _____
6. **OLSSGY** _____
7. **RPKREINGTY** _____
8. **NRNRBUMA** _____

Bonusaktivitet: Tenk raskt

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

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

Kontrollpunkt 8: Casestudier om VPN og nettverk

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

CASESTUDIE 1: HÅNDHEVING AV MFA

👮

Scenario: En forretningsanalytiker prøver å logge inn i selskapets database mens vedkommende jobber eksternt. Vedkommende skriver inn riktig brukernavn og passord, men VPN-portalen blokkerer tilgangen og krever en kode fra en fysisk token.

Diskusjonsspørsmål: Hvilken sikkerhetspolicy håndhever dette doble verifiseringstrinnet?

CASESTUDIE 2: OVERHOLDELSE AV SIKKERHETSTILSTAND

👮

Scenario: En konsulent kobler den private bærbare datamaskinen sin til selskapets eksterne nettverk. VPN-klienten kobler umiddelbart fra og varsler brukeren om at antivirusdefinisjonene er utdaterte.

Diskusjonsspørsmål: Hvilken spesialisert kontroll i VPN-gatewayen blokkerte dette tilkoblingsforsøket?

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

22	16	14		2	5	19	11	25	20	20	5	18		5	14	8	5	20	5	18
			13	5	4		6	10	5	18	14	20	9	12	7	1	14	7		

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 VPN for ekstern tilgang?

En sikker tilkoblingsmetode som lar ansatte som jobber utenfor kontoret, koble seg direkte til private bedriftsservere.

Q2: Hvorfor er klient-til-nettsted annerledes enn nettsted-til-nettsted?

Klient-til-nettsted kobler sammen enkeltbrukeres enheter, mens nettsted-til-nettsted kobler sammen hele fysiske kontorlokasjoner.

Q3: Hva er en enhetssjekk av sikkerhetstilstand (device posture check)?

En skanning som kontrollerer sikkerhetsstatusen til en ekstern enhet (antivirus, OS-oppdateringsnivå) før tilgang gis.

Q4: Hvorfor brukes OpenVPN til fjerntilgang?

På grunn av den sterke sikkerhetsprotokollen, kompatibilitet på tvers av plattformer og evnen til å håndtere enkeltforbindelser.

Q5: Hvordan beskytter MFA fjerntilgang?

Den legger til et sekundært verifiseringstoken, slik at tilgang hindres selv om ansattes passord lekkes eller stjeles.

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 en syslog-server?

Et sentralisert loggregister som lagrer tilkoblingshendelser, innlogginger og systemvarsler for samsvarsrevisjoner.

Q7: Hva forårsaker flaskehals i båndbredden?

Når de samlede båndbreddebehovene til eksterne ansatte overstiger hastighetsgrensen for internettilgangen i bedriftens gateway.

Q8: Kan jeg koble hjemmedatamaskinen min til en jobb-VPN?

Bare hvis enheten består revisjoner av bedriftens sikkerhetskontroll og er godkjent av IT-administratorer.

Q9: Hva er nettverksinnkapsling?

Innpakkingen av datapakker under transport inne i krypterte protokollhoder for å sikre overføringen.

Q10: Hvordan optimaliserer delt tunnelering (split tunneling) ekstern tilgang?

Den lar ansatte bruke den lokale internettleverandøren til vanlig surfing mens arbeidsrelaterte filer rutes via VPN-en.

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 styrker sertifikatbasert autentisering ekstern tilgang?

Den knytter tilkoblingstillatelser til forhåndsinstallerte lokale digitale sertifikater og blokkerer uadministrerte eller uautoriserte enheter.

Q2: Hva er sikkerhetsrisikoen ved delt tunnelering (split tunneling) for fjernarbeid?

Den skaper en potensiell bro der en kompromittert lokal enhet kan rute eksterne trusler inn i det private nettverket.

Q3: Hvordan inspiserer holdningssjekker (posture checks) registerinnstillinger?

VPN-klienten kjører lokale skript som spør etter registerstier for å kontrollere om bedriftens sikkerhetsprogramvare kjører aktivt.

Q4: Hvorfor bruker syslog UDP-port 514 som standard?

For å overføre logger raskt med minimal overhead, selv om sikre oppsett nå krever TLS-innkapsling over TCP.

Q5: Hvordan løser selskaper flaskehalser i gatewayens båndbredde?

Ved å innføre lastbalansere og fordele ekstern trafikk mellom regionale servernoder.

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

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

Q6: Hva er funksjonen til virtuelle TAP/TUN-adaptere på eksterne klienter?

De fungerer som virtuelle nettverkskort og ruter TCP/IP-trafikk på enhetsnivå direkte inn i den krypterte VPN-tunnelen.

Q7: Hvordan støtter IKEv2 MOBIKE mobiliteten til ansatte som jobber eksternt?

Den oppdaterer dynamisk bindingene til IP-adresser, slik at VPN-en forblir aktiv når brukeren beveger seg mellom Wi-Fi og mobildata.

Q8: Hva er forskjellen mellom delt og full tunnelruting?

Full ruting tvinger all internettrafikk fra enheten gjennom VPN-en, mens delt ruting bare sender trafikk til bedriftens IP-adresser.

Q9: Hvordan håndterer NAT-enheter eksterne VPN-tilkoblinger?

Ved å kartlegge lokale portområder til offentlige gateway-IP-adresser for å rute returnerende krypterte datapakker.

Q10: Hvilke etterlevelsesstandarder krever revisjon av ekstern tilgang?

Standarder som HIPAA, SOC 2 og PCI DSS krever logging og overvåking av alle eksterne tilkoblingsøkter.

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

VPN for ekstern tilgang oppretter sikre tunneler mellom klient og nettsted for arbeidstakere utenfor kontoret.

2. VPN-INNSIKT

Flerfaktorautentisering kreves av samsvarsregler for å beskytte eksterne bedriftsportaler.

3. VPN-INNSIKT

Sikkerhetstilstandskontroller verifiserer sikkerhetsinnstillingene på den lokale klienten før de gir tilgang til det private nettverket.

4. VPN-INNSIKT

Syslog-servere samler tilkoblingslogger for å revidere og oppdage uautoriserte tilgangsforsøk.

5. VPN-INNSIKT

Flaskehalser i gatewayens båndbredde oppstår når samlet ekstern trafikk overstiger serverens internettgrenser.

6. VPN-INNSIKT

Virtuelle nettverksadaptere kapsler inn nettverksspørringer fra operativsystemet i sikre protokoller.

7. VPN-INNSIKT

MOBIKE-støtte lar eksterne klienter bytte nettverk uten at VPN-tunnelen faller ut.

8. VPN-INNSIKT

Full tunnelruting sikrer all internettrafikk fra de ansatte, men øker belastningen på bedriftens gateway.

9. VPN-INNSIKT

Sertifikatautentisering knytter autorisasjon av VPN-tilkoblingen direkte til maskinvare som administreres av bedriften.

10. VPN-INNSIKT

Rammeverk som SOC 2 og PCI DSS forventer logging og overvåking av økter med fjerntilgang.

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/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).

https://www.rfc-editor.org/rfc/rfc4555

Fasit: Kontrollpunkt 1 – flervalg

1 **Innloggingstokener** MFA-SIKKERHET — Riktig svar: A

MERKNAD TIL LÆREREN

Flerfaktorautentisering krever sekundær verifisering ved pålogging.

2 **OpenVPN-tunnel** KLIENT-TIL-NETTSTED — Riktig svar: A

MERKNAD TIL LÆREREN

OpenVPN er en standardprotokoll for å sikre tunneler fra klient til nettsted.

3 **Revisjoner av sikkerhetstilstand** ENHETSSJEKK — Riktig svar: A

MERKNAD TIL LÆREREN

Sikkerhetstilstandskontroller skanner endepunkter etter aktive brannmurer og antivirusverktøy.

4 **Loggaggregator** SYSLOG-SERVER — Riktig svar: A

MERKNAD TIL LÆREREN

Syslog-servere samler sikkerhetshendelseslogger for å overvåke brudd på tilgang.

5 **Kortoverflyt** FLASKEHALS I GATEWAYEN — Riktig svar: A

MERKNAD TIL LÆREREN

Flaskehals i gatewayens båndbredde oppstår når brukertrafikken overstiger serverens grenser.

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Innloggingstokener** MFA-KONTROLLER **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Flerfaktorautentisering krever sekundær verifisering ved pålogging.

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

MERKNAD TIL LÆREREN

Tilstandskontroller (posture checks) blokkerer enheter der brannmuren eller antivirusprogrammet er slått av, så slike enheter nektes tilgang.

8 **Loggaggregator** SYSLOG-SERVER **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Syslog-servere samler sikkerhetshendelseslogger for å overvåke brudd på tilgang.

9 **Spørsmål 9** **Riktig svar: Usant**

MERKNAD TIL LÆREREN

OpenVPN og IPsec er gjeldende protokoller som krypterer trafikken fra eksterne klienter.

10 **Kortoverflyt** FLASKEHALS I GATEWAYEN **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Flaskehals i gatewayens båndbredde oppstår når brukertrafikken overstiger serverens grenser.

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. FLERFAKTOR	D 2. OPENVPN	E 3. SIKKERHETSTILSTAND	B 4. SYSLOG
C 5. BÅNDBREDDE	G 6. KRYPTERING	A 7. TUNNELERING	F 8. BRANNMUR

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 FLERFAKTOR	2 OPENVPN	3 HELSESTATUS	4 SYSLOG
5 BÅNDBREDDE	6 TUNNELERING		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 D – SYSLOG	2 H – BRANNMUR	3 G – TUNNELERING	4 F – KRYPTERING
5 B – OPENVPN	6 E – BÅNDBREDDE	7 C – HELSESTATUS	8 A – FLERFAKTOR

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare FLERFAKTOR, OPENVPN og SIKKERHETSTILSTAND med egne ord og gi et eksempel på hvert.

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

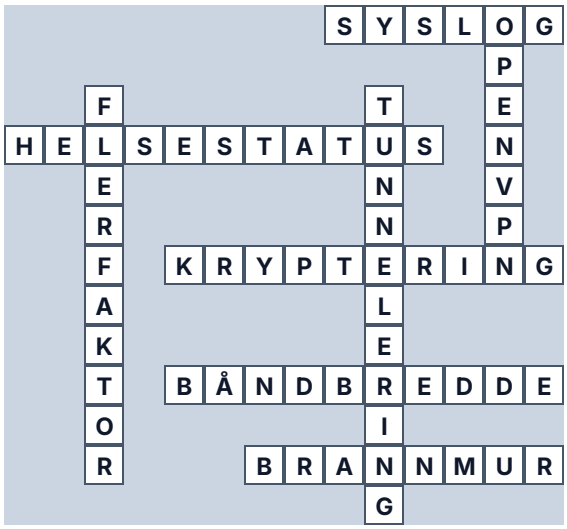
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

1 vannrett: SYSLOG Sentral innsamler av sikkerhetslogger (6 bokstaver)

5 vannrett: HELSESTATUS Validering av en fjernenhets helsetilstand (11 bokstaver)

6 vannrett: KRYPTERING Kryptografisk sammenblanding av pakker (10 bokstaver)

7 vannrett: BÅNDBREDDE Grense for nettverkets datakapasitet (10 bokstaver)

8 vannrett: BRANNMUR Regler for systemer som filtrerer trafikk (8 bokstaver)

LODDRETT

2 loddrett: OPENVPN Standard protokoll mellom klient og nettsted (7 bokstaver)

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

4 loddrett: TUNNELERING Innkapsling av data i en sikker bane (11 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1.	O K A F L F T R R E	FLERFAKTOR	5.	V N N E O P P	OPENVPN
2.	E S E H U S L T A T S	HELSESTATUS	6.	O L S S G Y	SYSLOG
3.	B R D E Å B E D D N	BÅNDBREDDE	7.	R P K R E I N G T Y	KRYPTERING
4.	E N G L N E I R T U N	TUNNELERING	8.	N R N R B U M A	BRANNMUR

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"VPN BESKYTTER ENHETER MED FJERNTILGANG"

Fasit til casestudiene

A Casestudie 1: Håndheving av MFA

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En forretningsanalytiker prøver å logge inn i bedriftens database mens vedkommende jobber eksternt. Vedkommende skriver inn riktig brukernavn og passord, men VPN-portalen blokkerer tilgangen og krever en fysisk tokenkode.
- Anbefalt strategi og løsning: Bedriftens VPN-portal håndhever en streng policy for flerfaktorautentisering (MFA) for å sikre eksterne innlogginger.

B Casestudie 2: Overholdelse av sikkerhetstilstand

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En innleid konsulent kobler sin private bærbare datamaskin til bedriftens eksterne nettverk. VPN-klienten kobler umiddelbart fra og varsler brukeren om at antivirusdefinisjonene er utdaterte.
- Anbefalt strategi og løsning: Gatewayen for ekstern tilgang utførte en kontroll av endepunktets sikkerhetstilstand og blokkerte enheten på grunn av utdaterte sikkerhetskonfigurasjoner.