Namn: _____ Datum: _____ Poäng: _____

VPN för företag

Införa Zero Trust-nätverksåtkomst, dedikerade gateway-noder och centraliserade administratörskontroller för företaget.

INLÄRNINGSÖVERSIKT OM VPN-NÄTVERK FÖR FÖRETAG

ELEV

STUDENTSTATUS

Nätverksförsvararspåret

SÄKER

ANSLUTNINGSSTATUS

Skydda datapaket

AKTIV

LÄCKSKYDD

Skydd mot DNS- och IPv6-läckor

Välkommen! Det här aktivitetshäftet guidar dig genom VPN-nätverk för företag. Du utforskar Zero Trust-arkitekturer, dedikerade gateways med statiska IP-adresser, administratörskonsoler, provisionering och IPsec-tunnlar mellan platser.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska konfigurationer för VPN och nätverkssäkerhet.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

Öppna VPN.com:s guide till de bästa VPN-tjänsterna

URL: https://www.vpn.com/sv/vpn/basta-vpn-foretag/enterprise/

Din inlärningsplan för VPN-nätverk i företag

- Inför ramverk för Zero Trust Network Access (ZTNA).
- Konfigurera dedikerade IP-adresser för servergateway för vitlistefilter.
- Hantera centraliserade administrationspaneler för företag och listor över användarplatser.
- Granska nätverkets åtkomstloggar och användarnas anslutningshistorik.
- Konfigurera regler för enkel inloggning (SSO) och multifaktorautentisering.
- Ställ in site-to-site-IPsec-tunnlar mellan filialer.

INSTRUKTIONER OM VPN-NÄTVERK FÖR FÖRETAG

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

ZERO TRUST-ARKITEKTURER OCH DEDIKERADE GATEWAYS (INTRODUKTION)

VPN för företag skyddar företagets tillgångar genom att övergå till ramverk för Zero Trust Network Access (ZTNA) och vitlista dedikerade statiska IP-gateways. IT-chefer använder centraliserade administrationskonsoler för att orkestrera site-to-site IPsec-tunnlar och länkar för enkel inloggning (SSO).

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

Kontrollpunkt 1: Utmaning med flerval

1. Vilken säkerhetsmodell ersätter äldre VPN-lösningar i företag?

- A) Zero Trust
- B) Multi-hop
- C) Peer-to-peer
- D) Enda gateway

2. Vilken funktion krävs för att begränsa databasåtkomsten till företagets servrar?

- A) Dedikerad IP
- B) Dynamisk routing
- C) Delad tunnel
- D) DNS-proxy

3. Vilket protokoll är standard för tunnlar mellan företagets olika platser?

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

4. Vilket centralt verktyg låter administratörer hantera anställdas licenser?

- A) Adminkonsol
- B) Registernyckel
- C) Routerns firmware
- D) Systemlogg

5. Vilken autentiseringsstandard gör det möjligt att logga in via Okta eller Microsoft Entra ID?

- A) Single Sign-On
- B) Delad hemlighet
- C) EPP-autentisering
- D) WEP-nyckel

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Zero Trust Network Access ger nätverksåtkomst först efter att enhetens förtroende kontinuerligt har verifierats.

- ○ Sant
- ○ Falskt

7 Fråga 7

7. Gateways med dedikerad IP dirigerar de anställdas trafik tillsammans med slumpmässiga offentliga konsumentanvändare.

- ○ Sant
- ○ Falskt

8 Fråga 8

8. Centraliserade administratörskonsoler gör att IT-chefer omedelbart kan återkalla enskilda anställdas platser.

- ○ Sant
- ○ Falskt

9 Fråga 9

9. IPsec är ett lättviktigt protokoll som inte stöder nätverkstunnlar mellan platser (site-to-site).

- ○ Sant
- ○ Falskt

10 Fråga 10

10. Single Sign-On möjliggör säker autentisering av anställda via företagets identitetsleverantörer.

- ○ Sant
- ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Moderna säkerhetsarkitekturer ersätter äldre tunnlar med _____ -åtkomst.
2. För att begränsa åtkomsten till databaser konfigurerar företag en _____ som gateway-adress.
3. Filialkontor ansluts säkert med _____ -tunnlar mellan platser.
4. IT-administratörer tilldelar användarlicenser till anställda i den centrala _____ .
5. Okta-integration gör att anställda kan autentisera sig via företagets _____ .
6. För att skydda inloggningar kräver företagsportaler _____ autentisering.

ORDBANK

ADMINKONSOL DEDIKERAD IP FLERFAKTOR GATEWAY IPSEC SINGLE SIGN-ON TILLDELNING ZERO TRUST

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av nyckelbegrepp

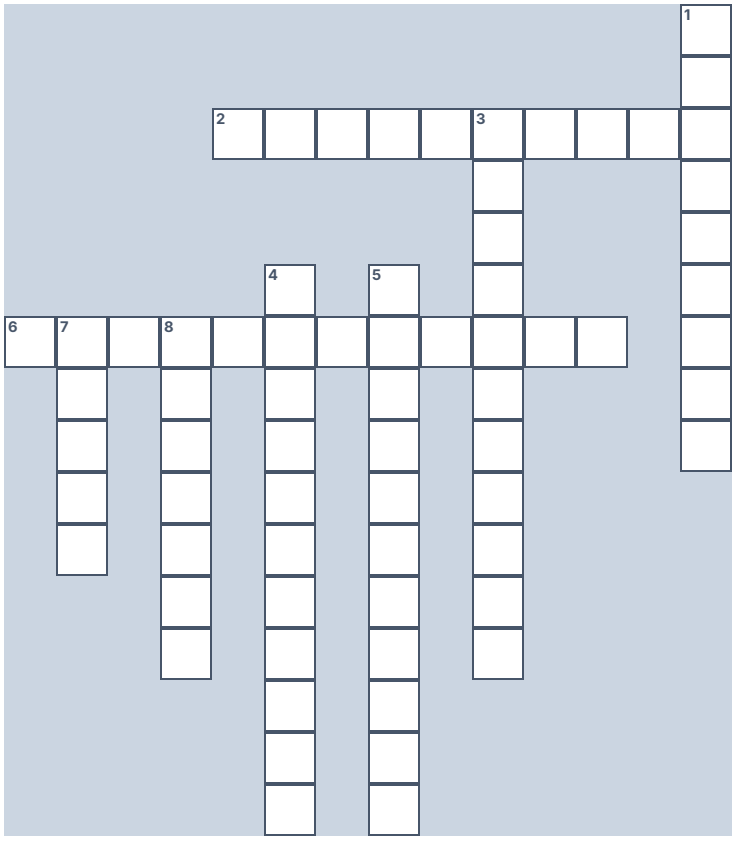
MATCHNING AV DEFINITIONER

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

☐	1. ZERO TRUST	A	Tilldelning av VPN-åtkomstlicenser till anställda.
☐	2. DEDIKERAD IP	B	Länken mellan Okta och Entra ID för identitet.
☐	3. IPSEC	C	Inloggningssäkerhet som kräver extra token.
☐	4. ADMINKONSOL	D	Statisk gateway-adress i vitlistan.
☐	5. ENKEL INLOGGNING	E	Standard för tunnel mellan platser.
☐	6. MULTIFAKTOR	F	Nätverkets ingångsnod för routing.
☐	7. GATEWAY	G	Central portal för IT-chefens platser.
☐	8. TILLHANDAHÅLLA	H	Ramverk för kontinuerlig tillitsverifiering.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

2. Inloggningsskydd som kräver extra tokens (10)

6. Identitetskoppling till Okta och Entra ID (12)

LODRÄTT

1. Ramverk för kontinuerlig verifiering av förtroende (9)

3. Central portal för IT-ansvariga (11)

4. Statisk adress till en vitlistad gateway (11)

5. Utdelning av VPN-licenser till anställda (11)

7. Standard för tunnlar mellan platser (5)

8. Nätverkets ingångsnod för dirigering (7)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

2 vågrätt: Inloggningsskydd som kräver extra tokens (10 bokstäver):

6 vågrätt: Identitetskoppling till Okta och Entra ID (12 bokstäver):

LODRÄTT

1 lodrätt: Ramverk för kontinuerlig verifiering av förtroende (9 bokstäver):

3 lodrätt: Central portal för IT-ansvariga (11 bokstäver):

4 lodrätt: Statisk adress till en vitlistad gateway (11 bokstäver):

5 lodrätt: Utdelning av VPN-licenser till anställda (11 bokstäver):

7 lodrätt: Standard för tunnlar mellan platser (5 bokstäver):

8 lodrätt: Nätverkets ingångsnod för dirigering (7 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

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

ORDLISTA

ZEROTRUST, DEDIKERADIP, IPSEC, ADMINKONSOL, SINGLESIGNON, FLERFAKTOR, GATEWAY, TILLDELNING

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

ORDLISTA

- **A. ZEROTRUST**
- **B. DEDIKERADIP**
- **C. IPSEC**
- **D. ADMINKONSOL**
- **E. SINGLESIGNON**
- **F. FLERFAKTOR**
- **G. GATEWAY**
- **H. TILLDELNING**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Statisk adress till en vitlistad gateway.
2. Nätverkets ingångsnod för dirigering.
3. Utdelning av VPN-licenser till anställda.
4. Inloggningsskydd som kräver extra tokens.
5. Standard för tunnlar mellan platser.
6. Ramverk för kontinuerlig verifiering av förtroende.
7. Identitetskoppling till Okta och Entra ID.
8. Central portal för IT-ansvariga.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga begrepp i detta arbetsblad. Skriv dina svar i rutorna.

1. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. YAWEAGT
5. DEARDPKEDII
6. NLKNOSADOMI
7. LRFKATORFE
8. ILGELTDINNL

Bonusaktivitet: Tänk snabbt

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

1	Verktyg som ett företag använder varje dag			
2	Saker som ett VPN kan dölja			
3	Roller på en IT-avdelning			
4	Ord som beskriver Zero Trust			
5	Sätt att logga in säkert			
6	Skäl till att ge anställda ett VPN			
7	Saker att göra efter ett säkerhetsintrång			
8	Skäl till att använda ett VPN under resor			
9	Regler för säkert distansarbete			
10	Data som ett företag måste skydda			
11	Saker som kan störa ett videomöte			
12	Enheter som kan använda ett VPN			
13	Kontorsprogram du känner till			
14	Platser som anställda arbetar från			
15	Enheter som en anställd kan ha			

Kontrollpunkt 8: Fallstudier om VPN och nätverk

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

FALLSTUDIE 1: MIGRERING TILL NOLLTILLIT

👷

Scenario: Ett företag vill skydda sina lokala servrar genom att fortlöpande verifiera enheters efterlevnadscertifikat, brandväggsstatus och användarens plats i stället för att lita på alla som finns inne i nätverket.

Diskussionsfråga: Vilket ramverk bör IT-säkerhetschefen införa för att uppnå detta?

FALLSTUDIE 2: BEGRÄNSNING AV GATEWAY

👷

Scenario: Ett företag har privata finansdatabaser i molnet. De vill blockera all offentlig internetåtkomst till adminpanelerna och bara tillåta inloggningar från verifierade slutpunkter i företaget.

Diskussionsfråga: Vilken nätverkskonfiguration bör databasadministratören ställa in i molnbrandväggen?

Kontrollpunkt 9: Knäck chiffret

En nätverksingenjör skyddar dirigeringskanaler och klienttunnlar. Använd bokstav-till-siffra-nyckeln nedan för att avkoda meddelandet genom att skriva de matchande bokstäverna på de tomma raderna.

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10
K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20
U=21 V=22 W=23 X=24 Y=25 Z=26 Å=27 Ä=28 Ö=29

26	5	18	15		20	18	21	19	20		22	5	18	9	6	9	5	18	1	18

22	1	18	10	5		1	14	19	12	21	20	5	14		5	14	8	5	20

Avkodat meddelande:

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

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

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

Q1: Vad är ett VPN för storföretag (enterprise)?

En säker nätverkstunnel utformad för företag, som låter distansarbetare komma åt företagsnätverk med central hantering.

Q2: Hur skiljer sig Zero Trust från traditionella VPN?

Traditionella VPN litar på alla inuti tunneln, medan Zero Trust kontinuerligt verifierar varje enhets- och användaranslutning.

Q3: Vad är en dedikerad IP-adress i VPN för företag?

En statisk IP-adress som är reserverad enbart för ditt företag, så att du kan vitlista den för säker åtkomst till molndatabaser.

Q4: Varför är SSO viktigt för VPN för företag?

Single Sign-On låter anställda använda sina företagsuppgifter (som Okta eller Microsoft Entra ID) för att logga in på ett säkert sätt.

Q5: Vad är ett plats-till-plats-VPN?

En tunnel som kopplar samman två fysiska kontor (som ett filialkontor och huvudkontoret) över det offentliga internet med IPsec.

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

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

Q6: Vilken funktion har en administrationskonsol?

En instrumentpanel för IT-administratörer för att lägga till eller ta bort anställdas platser, tilldela gateways och övervaka aktiva anslutningar.

Q7: Hur skyddar MFA VPN för företag?

Genom att kräva en sekundär kod (som en token från en autentiseringsapp) för att förhindra obehörigt intrång via komprometterade lösenord.

Q8: Kan jag granska de anställdas anslutningshistorik?

Ja, VPN-tjänster för företag loggar tidsstämplar för anslutningar, varaktighet och tilldelade IP-adresser för efterlevnadsgranskning.

Q9: Vad är ZTNA?

Zero Trust Network Access, en säkerhetsmodell som ger åtkomst endast till specifika program i stället för hela nätverket.

Q10: Vilken roll har gatewaynoder?

De fungerar som säkra ingångspunkter för fjärrtrafik och dirigerar data direkt till privata företagsservrar.

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

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

Q1: Hur skyddar IPsec kommunikation mellan företagets olika platser (site-to-site)?

IPsec krypterar trafik på nätverksnivå med Encapsulating Security Payload (ESP) för att säkerställa datasekretess och dataintegritet.

Q2: Varför fungerar äldre perimeterbaserad säkerhet dåligt för distansarbetande personal?

Eftersom anställda använder data från flera platser och enheter, vilket gör ett enda brandväggsperimeterskydd i nätverket föråldrat.

Q3: Hur genomför IT-chefer automatiserad tilldelning av resurser?

Genom att mappa SCIM-protokoll mellan identitetsleverantörer (Okta) och VPN-adminkonsolen för att synkronisera användarkataloger.

Q4: Vilken fördel har delad tunnel (split tunneling) i företagsmiljöer?

Den routar lokal SaaS-trafik (som Microsoft 365) utanför VPN-tunneln och sparar företagets gatewaybandbredd åt privata databaser.

Q5: Hur validerar enhetshållningskontroller slutpunktens säkerhet?

VPN-klienten skannar enheten innan den ansluter för att kontrollera att brandväggen är aktiv, antiviruset körs och operativsystemets korrigeringar är aktuella.

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

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

Q6: Vilken roll spelar NAT-traversering i VPN-lösningar för företag?

NAT-T kapslar in IPsec-paket i UDP så att de kan passera hemroutrar och brandväggar utan att anslutningen bryts.

Q7: Hur förhindrar företag flaskhalsar i gatewayens bandbredd?

Genom att distribuera flera regionala gatewaynoder och fördela inkommande användartrafik mellan dem med lastbalanserare.

Q8: Varför föredras vitlistor med statiska IP-adresser framför dynamiska?

Statiska vitlistor hindrar obehöriga externa IP-adresser från att försöka genomföra anslutningshandskakningar, vilket minskar attackytan dramatiskt.

Q9: Vilken roll har certifikatbaserad autentisering i VPN för företag?

Den validerar unika digitala certifikat som är installerade på företagshanterade enheter och blockerar ohanterade privata datorer.

Q10: Hur minskar ZTNA risken för lateral förflyttning?

Genom att isolera användarsessioner till specifika behöriga resurser, så att hackare inte kan röra sig i nätverket om en nod kompromitteras.

Del 11: 10 verkliga fakta och insikter om VPN

Gå igenom verkliga fakta om VPN-kryptering och hastigheter, protokollgranskningar, mobil anslutning och distansarbete i företag.

1. VPN-INSIKT

Zero Trust-arkitekturer verifierar kontinuerligt säkerhetsstatusen för varje enhet som försöker ansluta till ett nätverk.

2. VPN-INSIKT

Gateways med dedikerad IP gör det möjligt för företag att låsa ned molndatabaser genom att vitlista statiska adresser.

3. VPN-INSIKT

IPsec är branschstandardens protokoll för att konfigurera säkra nätverkstunnlar mellan kontor (site-to-site).

4. VPN-INSIKT

Adminkonsoler låter IT-avdelningar tilldela, hantera och granska anställdas VPN-åtkomstplatser.

5. VPN-INSIKT

Single Sign-On integrerar VPN-åtkomst med företagets identitetsleverantörer som Okta och Entra ID.

6. VPN-INSIKT

Multifaktorautentisering blockerar obehöriga anslutningsförsök som utgår från stulna lösenordsnycklar.

7. VPN-INSIKT

Delad tunnling optimerar företagets bandbredd genom att utesluta offentlig SaaS-trafik från den krypterade tunneln.

8. VPN-INSIKT

Kontroller av enhetens säkerhetsläge verifierar lokala säkerhetsinställningar innan åtkomst till företagets servrar beviljas.

9. VPN-INSIKT

SCIM-katalogsynkronisering automatiserar åtkomstkontroller vid introduktion och avslut av anställda.

10. VPN-INSIKT

Zero Trust Network Access begränsar användarnas åtkomst till vissa behöriga program och förhindrar lateral förflyttning i nätverket.

Tekniska referenser och källor

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

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[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/

Facit: Kontrollpunkt 1 – Flerval

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

ANTECKNING FÖR LÄRAREN

Zero Trust-modeller verifierar kontinuerligt enhetens efterlevnad innan nätverksåtkomst ges. Källhänvisning: NIST Zero Trust.

2 **Dedikerad IP** STATISK IP **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Dedikerade IP-adresser gör det möjligt att vitlista gateways för att blockera offentlig trafik. Källa: Dedicated IP Guide.

3 **IPsec-standard** IPSEC-TUNNEL **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

IPsec är standardprotokollet som används för site-to-site-tunnlar mellan filialer. Källa: IPsec Tunneling.

4 **IT-tilldelning** ADMINKONSOL **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Centraliserade administratörspaneler gör att IT-chefer kan fördela platslicenser. Källa: CISA Guidelines.

5 **Fråga 5** **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Vilken autentiseringsstandard gör det möjligt att logga in via Okta eller Microsoft Entra ID? → Single Sign-On

Facit: Kontrollpunkt 2 – Sant eller falskt

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

ANTECKNING FÖR LÄRAREN

Zero Trust-modeller verifierar kontinuerligt enhetens efterlevnad innan nätverksåtkomst ges. Källhänvisning: NIST Zero Trust.

7 **Fråga 7** **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Dedikerade IP-adresser är reserverade för ett enda företag, så dess trafik blandas inte med andra användares.

8 **IT-tilldelning** IT-ADMINISTRATÖRSPLATS **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Centraliserade administratörspaneler gör att IT-chefer kan fördela platslicenser. Källa: CISA Guidelines.

9 **IPsec-standard** PLATS TILL PLATS **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

IPsec är standardprotokollet som används för site-to-site-tunnlar mellan filialer. Källa: IPsec Tunneling.

10 **Okta SSO-länk** SSO-INLOGGNING **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Single Sign-On integrerar VPN-inloggningar med företagets kataloger som Okta. Källa: Okta SSO.

Facit för ordförråd och bedömningsmall

Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

H 1. ZERO TRUST	D 2. DEDIKERAD IP	E 3. IPSEC	G 4. ADMINKONSOL
B 5. ENKEL INLOGGNING	C 6. MULTIFAKTOR	F 7. GATEWAY	A 8. TILLHANDAHÅLLA

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

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

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

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

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara ZERO TRUST, DEDIKERAD IP och IPSEC med egna ord och ge ett exempel på varje.

Fallstudier:
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

2 vågrätt: FLERFAKTOR Inloggningsskydd som kräver extra tokens (10 bokstäver)

6 vågrätt: SINGLESIGNON Identitetskoppling till Okta och Entra ID (12 bokstäver)

LODRÄTT

1 lodrätt: ZEROTRUST Ramverk för kontinuerlig verifiering av förtroende (9 bokstäver)

3 lodrätt: ADMINKONSOL Central portal för IT-ansvariga (11 bokstäver)

4 lodrätt: DEDIKERADIP Statisk adress till en vitlistad gateway (11 bokstäver)

5 lodrätt: TILLDELNING Utdelning av VPN-licenser till anställda (11 bokstäver)

7 lodrätt: IPSEC Standard för tunnlar mellan platser (5 bokstäver)

8 lodrätt: GATEWAY Nätverkets ingångsnod för dirigering (7 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. RTOEZUSTR — **ZEROTRUST**
2. ICESP — **IPSEC**
3. SIISOGNENLNG — **SINGLESIGNON**
4. YAWEAGT — **GATEWAY**
5. DEARDPKEDII — **DEDIKERADIP**
6. NLKNOSADOMI — **ADMINKONSOL**
7. LRFKATORFE — **FLERFAKTOR**
8. ILGELTDINNL — **TILLDELNING**

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"ZERO TRUST VERIFIERAR VARJE ANSLUTEN ENHET"

Facit till fallstudierna

A Fallstudie 1: Migrering till nolltillit

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: Ett företag vill skydda sina lokala servrar genom att fortlöpande verifiera enheters efterlevnadscertifikat, brandväggsstatus och användarens plats i stället för att lita på alla som befinner sig inne i nätverket.
- Rekommenderad strategi och lösning: Direktören bör gå över till en modell med Zero Trust Network Access (ZTNA), som tillämpar kontinuerliga kontextbaserade säkerhetskontroller.

B Fallstudie 2: Begränsning av gateway

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: Ett företag har privata finansdatabaser i molnet. De vill blockera all publik internetåtkomst till administratörspanelerna och endast tillåta inloggningar från verifierade slutpunkter i företaget.
- Rekommenderad strategi och lösning: Administratören bör konfigurera en dedikerad IP-gateway på företags-VPN:en och vitlista denna statiska adress i molndatabasens brandvägg.