Namn: _____ Datum: _____ Poäng: _____

VPN för fjärråtkomst

Skydda slutpunkter för distansanställda, multifaktorsautentisering och konfiguration av IPsec-tunnlar.

LÄROÖVERSIKT OM VPN FÖR FJÄRRÅTKOMST

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 fjärråtkomst. Du utforskar tunnlar mellan klient och plats, flerfaktorsinloggningar, kontroller av enhetens status, bandbreddsgränser och säkerhetsgranskning med syslog.

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-for-foretag/fjarratkomst/

Din inlärningsplan för VPN för fjärråtkomst

- Säkra slutpunkter för distansanställda som når lokala nätverksnoder.
- Konfigurera policyer för multifaktorautentisering vid fjärrinloggningar.
- Ställ in IPsec- och OpenVPN-konfigurationer för klient till plats.
- Granska loggar över fjärranslutningar för brott mot åtkomstkontroll.
- Inför kontroller av enhetens status innan nätverksanslutningar beviljas.
- Optimera serverns genomströmning för att undvika att bandbredden strypts vid distansarbete.

ANVISNINGAR FÖR VPN FÖR FJÄRRÅTKOMST

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om säkerhetskontroller av enheter och inloggning med flera faktorer. Avsluta med bonusaktiviteten Tänk snabbt.

KLIENT-TILL-PLATS-TUNNLAR OCH EFTERLEVNAD PÅ SLUTPUNKTER (INLEDNING)

VPN för fjärråtkomst upprättar säkra tunnlar mellan klient och plats för anställda utanför kontoret. Att säkra dessa anslutningar kräver inloggning med multifaktorautentisering (MFA), kontroller av slutpunkters säkerhetsstatus och granskning av loggar via centrala syslog-insamlare.

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

Kontrollpunkt 1: Utmaning med flerval

1 **1. Vilken autentiseringsstandard bör portaler för VPN med fjärråtkomst kräva?**

- A) Flerfaktor
- B) Enfaktorsautentisering
- C) Okrypterat
- D) Lokal gäst

2 **2. Vilket protokoll är standard för att skydda anslutningar mellan klient och plats vid distansarbete?**

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3 **3. Vilken kontroll validerar att en bärbar dator på distans är ren innan den ansluter?**

- A) Hälsokontroll av enheten
- B) Hastighetstest
- C) Pingtest
- D) Minnesantal

4 **4. Var lagras anslutningsloggar för anställda på distans för säkerhetsgranskning?**

- A) Syslog-server
- B) Registernyckel
- C) Klientminne
- D) Webbläsare

5 **5. Vilket problem uppstår när antalet medarbetare på distans överstiger gatewayens bandbreddskapacitet?**

- A) Bandbreddsstrypning
- B) DNS-läcka
- C) Handskakningspass
- D) Exponering av IP-adress

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Multifaktorautentisering lägger till en andra valideringstoken för att säkra fjärrinloggningar.

○ Sant ○ Falskt

7 Fråga 7

7. Kontroller av säkerhetsstatus tillåter fjärrenheter med avstängda brandväggar att komma åt privata servrar.

○ Sant ○ Falskt

8 Fråga 8

8. Loggar från VPN för fjärråtkomst är avgörande för att spåra obehörig åtkomst till företagsnätverket.

○ Sant ○ Falskt

9 Fråga 9

9. OpenVPN och IPsec är äldre protokoll som inte krypterar fjärrklienternas data.

○ Sant ○ Falskt

10 Fråga 10

10. Flaskhals i gatewayens bandbredd uppstår när fjärrtrafiken överstiger anslutningskortets kapacitet.

○ Sant ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. För att skydda företagsportaler måste fjärrinloggningar kräva _____ autentisering.
2. Fjärrklienter krypterar tunnelns nyttolast med standardprotokoll som _____ .
3. Enheter måste klara en säkerhets _____ innan de får nätverksanslutning.
4. Granskningsbara inloggningsloggar skickas kontinuerligt till en central _____ -server.
5. Tung trafik under kontorstid kan leda till överbelastning av gatewayens _____ .
6. Drivrutiner för virtuella adaptrar hanterar _____ mellan klient och plats i Windows och macOS.

ORDBANK

BANDBREDD BRANDVÄGG FLERFAKTOR HÄLSOKONTROLL KRYPTERING
OPENVPN SYSLOG TUNNLING

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av nyckelbegrepp

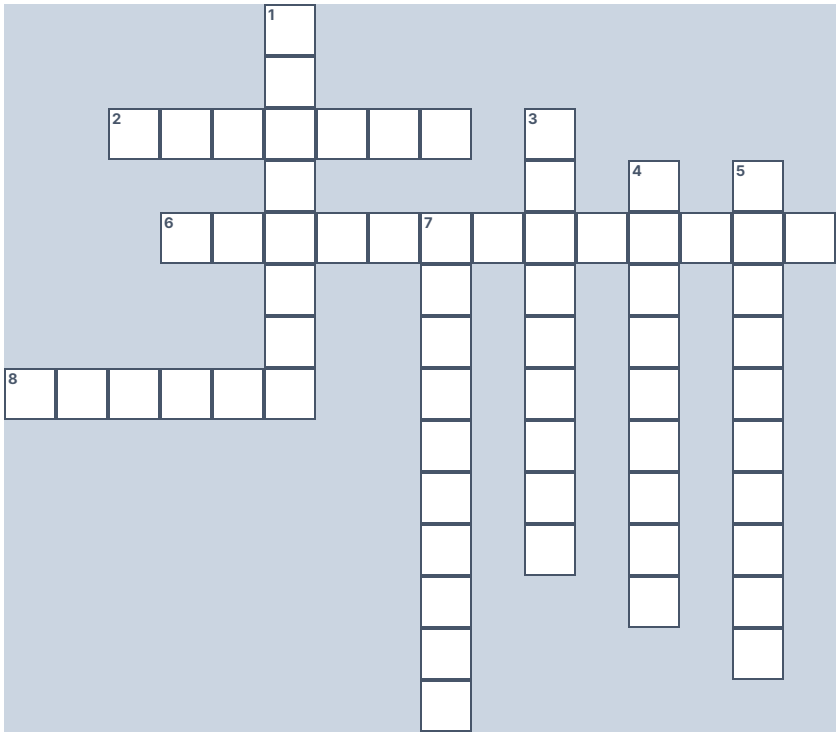
MATCHNING AV DEFINITIONER

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

☐	1. MULTIFAKTOR	A	Att kapsla in data i en säker väg.
☐	2. OPENVPN	B	Central insamlare av säkerhetsloggar.
☐	3. SÄKERHETSLÄGE	C	Gräns för nätverkets datakapacitet.
☐	4. SYSLOG	D	Standardprotokoll för klient till plats.
☐	5. BANDBREDD	E	Validering av fjärrenhetens hälsotillstånd.
☐	6. KRYPTERING	F	Regler för trafikfiltreringssystem.
☐	7. TUNNLING	G	Kryptografisk förvrängning av paket.
☐	8. BRANDVÄGG	H	Inloggningssäkerhet som kräver extra token.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

2. Standardprotokoll mellan klient och plats (7)

6. Validering av fjärrenhetens skick (13)

8. Central insamlare av säkerhetsloggar (6)

LODRÄTT

1. Inkapsling av data i en säker väg (8)

3. Gräns för nätverkets datakapacitet (9)

4. Regler för system som filtrerar trafik (9)

5. Inloggningsskydd som kräver extra tokens (10)

7. Kryptografisk förvrängning av paket (10)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

2 vågrätt: Standardprotokoll mellan klient och plats (7 bokstäver):

6 vågrätt: Validering av fjärrenhetens skick (13 bokstäver):

8 vågrätt: Central insamlare av säkerhetsloggar (6 bokstäver):

LODRÄTT

1 lodrätt: Inkapsling av data i en säker väg (8 bokstäver):

3 lodrätt: Gräns för nätverkets datakapacitet (9 bokstäver):

4 lodrätt: Regler för system som filtrerar trafik (9 bokstäver):

5 lodrätt: Inloggningsskydd som kräver extra tokens (10 bokstäver):

7 lodrätt: Kryptografisk förvrängning av paket (10 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

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

ORDLISTA

FLERFAKTOR OPENVPN HÄLSOKONTROLL SYSLOG BANDBREDD KRYPTERING TUNNLING BRANDVÄGG

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. FLERFAKTOR**
- **B. OPENVPN**
- **C. HÄLSOKONTROLL**
- **D. SYSLOG**
- **E. BANDBREDD**
- **F. KRYPTERING**
- **G. TUNNLING**
- **H. BRANDVÄGG**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Central insamlare av säkerhetsloggar.
2. Regler för system som filtrerar trafik.
3. Inkapsling av data i en säker väg.
4. Kryptografisk förvrängning av paket.
5. Standardprotokoll mellan klient och plats.
6. Gräns för nätverkets datakapacitet.
7. Validering av fjärrenhetens skick.
8. Inloggningsskydd som kräver extra tokens.

Kontrollpunkt 7: Utmaning med blandade ord

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

1. OKAFLFTRRE
2. LOÄKLHOOLT RNS
3. BRBAEDDDN
4. NNGILTUN
5. VNNEOPP
6. OLSSGY
7. RPKREINGTY
8. GDGBNRVÄA

Bonusaktivitet: Tänk snabbt

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

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

Kontrollpunkt 8: Fallstudier om VPN och nätverk

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

FALLSTUDIE 1: TILLÄMPA MFA



Scenario: En affärsanalytiker försöker logga in i företagets databas när hen arbetar på distans. Hen anger rätt användarnamn och lösenord, men VPN-portalen blockerar åtkomsten och kräver en kod från en fysisk token.

Diskussionsfråga: Vilken säkerhetspolicy tillämpar detta steg med dubbel verifiering?

FALLSTUDIE 2: EFTERLEVNAD AV POSTURE



Scenario: En konsult ansluter sin privata bärbara dator till företagets fjärrnätverk. VPN-klienten avbryter anslutningen omedelbart och meddelar användaren att antivirusdefinitionerna är föråldrade.

Diskussionsfråga: Vilken specialiserad kontroll i VPN-gatewayen blockerade det här anslutningsförsöket?

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

6	10	28	18	18	27	20	11	15	13	19	20		22	9	1		22	16	14

19	11	25	4	4	1	18		19	12	21	20	5	14	8	5	20	5	18

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 VPN för fjärråtkomst?

En säker anslutningsmetod som låter anställda som arbetar utanför kontoret ansluta direkt till privata företagsservrar.

Q2: Varför skiljer sig klient-till-plats från plats-till-plats?

Klient-till-plats kopplar samman enskilda användarenheter, medan plats-till-plats länkar ihop hela fysiska kontorsplatser.

Q3: Vad är en enhetshållningskontroll (device posture check)?

En skanning som kontrollerar en fjärrenhets säkerhetsstatus (antivirus, korrigeringsnivå för operativsystemet) innan åtkomst beviljas.

Q4: Varför används OpenVPN för fjärråtkomst?

På grund av dess starka säkerhetsprotokoll, kompatibilitet mellan plattformar och förmåga att hantera enskilda anslutningar.

Q5: Hur skyddar MFA fjärråtkomst?

Den lägger till en extra verifieringstoken som förhindrar åtkomst även om medarbetares lösenord läcker eller stjäls.

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

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

Q6: Vad är en syslog-server?

Ett centralt loggarkiv som lagrar anslutningshändelser, inloggningar och systemvarningar för efterlevnadsgranskningar.

Q7: Vad orsakar flaskhalsar i bandbredden?

När de sammanlagda bandbreddsbehoven hos anställda på distans överstiger företagets gateway-gräns för internethastighet.

Q8: Kan jag ansluta min hemdator till ett jobb-VPN?

Bara om enheten klarar granskningar av företagets säkerhetsstatus och har godkänts av IT-administratörerna.

Q9: Vad är nätverksinkapsling?

Inkapslingen av datapaket under överföring i krypterade protokollhuvuden för att säkra överföringen.

Q10: Hur optimerar delad tunnel (split tunneling) fjärråtkomst?

Den låter anställda använda sin lokala internetleverantör för vanlig surfning medan arbetsrelaterade filer routas via VPN.

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 förbättrar certifikatbaserad autentisering fjärråtkomst?

Den binder anslutningsbehörigheter till förinstallerade lokala digitala certifikat och blockerar ohanterade eller obehöriga enheter.

Q2: Vilken säkerhetsrisk innebär delad tunnel (split tunneling) för distansarbete?

Den skapar en potentiell brygga där en komprometterad lokal enhet kan routa externa hot in i det privata nätverket.

Q3: Hur granskar hållningskontroller (posture checks) registerinställningar?

VPN-klienten kör lokala skript som frågar registersökvägar för att verifiera om säkerhetsprogram för företag körs aktivt.

Q4: Varför använder syslog UDP-port 514 som standard?

För att överföra loggar snabbt med minimal overhead, även om säkra konfigurationer numera kräver TLS-inkapsling över TCP.

Q5: Hur löser företag flaskhalsar i gatewayens bandbredd?

Genom att införa lastbalanserare och fördela fjärrtrafik mellan regionala servernoder.

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 funktion har virtuella TAP/TUN-adaptrar på fjärrklienter?

De fungerar som virtuella nätverkskort och dirigerar TCP/IP-trafik på enhetsnivå direkt in i den krypterade VPN-tunneln.

Q7: Hur stöder IKEv2 MOBIKE rörlighet för distansarbetande personal?

Den uppdaterar dynamiskt bindningarna av IP-adresser och håller VPN aktivt när användaren rör sig mellan Wi-Fi och mobildata.

Q8: Vad är skillnaden mellan delad och fullständig tunnelroutning?

Full routning tvingar all internettrafik från enheten genom VPN:et, medan delad routning bara skickar IP-adresser till företagets mål.

Q9: Hur hanterar NAT-enheter VPN-anslutningar på distans?

Genom att mappa lokala portintervall till offentliga gateway-IP-adresser för att dirigera tillbaka krypterade datapaket.

Q10: Vilka efterlevnadsstandarder kräver granskning av fjärråtkomst?

Standarder som HIPAA, SOC 2 och PCI DSS kräver loggning och övervakning av alla fjärranslutna sessioner.

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

VPN för fjärråtkomst upprättar säkra tunnlar mellan klient och plats för arbetare utanför kontoret.

2. VPN-INSIKT

Multifaktorautentisering krävs enligt efterlevnadsregler för att skydda företagsportaler för fjärråtkomst.

3. VPN-INSIKT

Kontroller av säkerhetsstatus verifierar klientens lokala säkerhetsinställningar innan åtkomst till det privata nätverket beviljas.

4. VPN-INSIKT

Syslog-servrar samlar loggar över anslutningar för att granska och upptäcka obehöriga åtkomstförsök.

5. VPN-INSIKT

Flaskhalsar i gatewayens bandbredd uppstår när den samlade fjärrtrafiken överstiger serverns internetgränser.

6. VPN-INSIKT

Virtuella nätverksadaptrar kapslar in operativsystemets nätverksfrågor i säkra protokoll.

7. VPN-INSIKT

Stöd för MOBIKE gör att fjärrklienter kan byta nätverk utan att VPN-tunneln bryts.

8. VPN-INSIKT

Routning av hela tunneln skyddar all internettrafik från medarbetarna men ökar belastningen på företagets gateway.

9. VPN-INSIKT

Certifikatautentisering knyter behörighet för VPN-anslutning direkt till företagshanterad hårdvara.

10. VPN-INSIKT

Ramverk som SOC 2 och PCI DSS förväntar sig loggning och övervakning av fjärråtkomstsessioner.

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/

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

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

Facit: Kontrollpunkt 1 – Flerval

1 **Inloggningstoken** MFA-SÄKERHET **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Multifaktorautentisering kräver en andra verifiering vid inloggning. Källa: MFA Implementation.

2 **OpenVPN-tunnel** KLIENT-TILL-PLATS **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

OpenVPN är ett standardprotokoll för att säkra tunnlar mellan klient och plats. Källa: OpenVPN Client.

3 **Granskningar av säkerhetsstatus** ENHETSKONTROLL **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Kontroller av säkerhetsstatus skannar slutpunkter efter aktiva brandväggar och antivirusverktyg. Källa: Posture Compliance.

4 **Logginsamlare** SYSLOG-SERVER **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Syslog-servrar samlar in loggar över säkerhetshändelser för att övervaka åtkomstöverträdelser. Källa: Syslog Standard.

5 **Kortöverskridning** GATEWAYFLASKHALS **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Flaskhals i gatewayens bandbredd uppstår när användartrafiken överstiger servergränserna. Källa: Capacity Planning.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Inloggningstoken** MFA-KONTROLLER **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Multifaktorautentisering kräver en andra verifiering vid inloggning. Källa: MFA Implementation.

7 **Fråga 7** **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Hållningskontroller blockerar enheter vars brandvägg eller antivirus är avstängt, så sådana enheter nekas.

8 **Logginsamlare** SYSLOG-SERVER **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Syslog-servrar samlar in loggar över säkerhetshändelser för att övervaka åtkomstöverträdelser. Källa: Syslog Standard.

9 **Fråga 9** **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

OpenVPN och IPsec är aktuella protokoll som krypterar trafiken från fjärrklienter.

10 **Kortöverskridning** GATEWAYFLASKHALS **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Flaskhals i gatewayens bandbredd uppstår när användartrafiken överstiger servergränserna. Källa: Capacity Planning.

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. MULTIFAKTOR	D 2. OPENVPN	E 3. SÄKERHETSLÄGE	B 4. SYSLOG
C 5. BANDBREDD	G 6. KRYPTERING	A 7. TUNNLING	F 8. BRANDVÄGG

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 FLERFAKTOR	2 OPENVPN	3 HÄLSOKONTROLL	4 SYSLOG
5 BANDBREDD	6 TUNNLING		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 D – SYSLOG	2 H – BRANDVÄGG	3 G – TUNNLING	4 F – KRYPTERING
5 B – OPENVPN	6 E – BANDBREDD	7 C – HÄLSOKONTROLL	8 A – FLERFAKTOR

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara MULTIFAKTOR, OPENVPN och SÄKERHETSLÄGE med egna ord och ge ett exempel på varje.

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

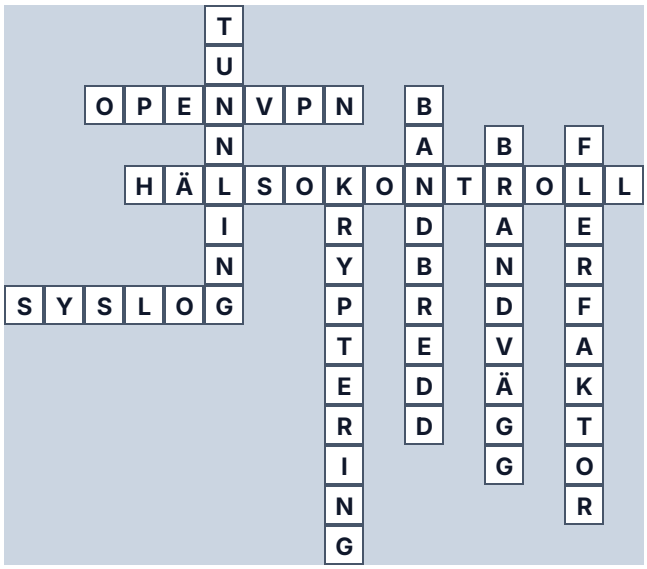
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

2 vågrätt: OPENVPN Standardprotokoll mellan klient och plats (7 bokstäver)

6 vågrätt: HÄLSOKONTROLL Validering av fjärrenhetens skick (13 bokstäver)

8 vågrätt: SYSLOG Central insamlare av säkerhetsloggar (6 bokstäver)

LODRÄTT

1 lodrätt: TUNNLING Inkapsling av data i en säker väg (8 bokstäver)

3 lodrätt: BANDBREDD Gräns för nätverkets datakapacitet (9 bokstäver)

4 lodrätt: BRANDVÄGG Regler för system som filtrerar trafik (9 bokstäver)

5 lodrätt: FLERFAKTOR Inloggningsskydd som kräver extra tokens (10 bokstäver)

7 lodrätt: KRYPTERING Kryptografisk förvrängning av paket (10 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. OKAFLFTRRE — **FLERFAKTOR**
2. LOÄKLHOOLTRNS — **HÄLSOKONTROLL**
3. BRBAEDDDN — **BANDBREDD**
4. NNGILTUN — **TUNNLING**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. RPKREINGTY — **KRYPTERING**
8. GDGBNRVÄA — **BRANDVÄGG**

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"FJÄRRÅTKOMST VIA VPN SKYDDAR SLUTENHETER"

Facit till fallstudierna

A Fallstudie 1: Tillämpa MFA

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En företagsanalytiker försöker logga in i företagets databas under distansarbete. Hen anger rätt användarnamn och lösenord, men VPN-portalen blockerar åtkomsten och kräver en kod från en fysisk token.
- Rekommenderad strategi och lösning: Företagets VPN-portal tillämpar en strikt policy för multifaktorautentisering (MFA) för att säkra fjärrinloggningar.

B Fallstudie 2: Efterlevnad av Posture

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En konsult ansluter sin privata bärbara dator till företagets fjärrnätverk. VPN-klienten kopplar omedelbart från anslutningen och meddelar användaren att antivirusdefinitionerna är föråldrade.
- Rekommenderad strategi och lösning: Gatewayen för fjärråtkomst utförde en kontroll av slutpunktens säkerhetsstatus och blockerade enheten på grund av föråldrade säkerhetskonfigurationer.