

Navn: Dato: Point:

VPN til fjernadgang

Sikring af fjernmedarbejderes enheder, flerfaktorgodkendelse og IPsec

OVERBLIK OVER VPN TIL FJERNADGANG

ELEV

ELEVSTATUS

Netværksforsvarer-spor

SIKKER

FORBINDELSSTATUS

Beskytter datapakker

100%

LÆKAGEFORSVAR

DNS- og IPv6-lækagebeskyttelse

Velkommen! Dette opgavehæfte guider dig gennem netværk med VPN til fjernadgang. Du vil udforske klient-til-site-tunneler, flerfaktorlogin, tilstandstjek af enheder, båndbreddegrænser og sikkerhedsrevision via syslog.

OPGAVEARKETS KONTROLPUNKTER

- ☐ Del 1-4: Lær VPN- og netværkssikkerhedskonfigurationer.
- ☐ Del 5-7: Løs kryds og tværs samt ordjagt.
- ☐ Del 8-9: Løs casestudier og chifferudfordring.
- ☐ Del 10: Gennemgå grundlæggende og avanceret FAQ.
- ☐ Del 11: Udforsk 10 interessante fakta fra virkeligheden.

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

URL: <https://www.vpn.com/vpn/best-vpn-for-business-remote-access/>

Din læringsplan for VPN til fjernadgang

- Sikr fjernmedarbejderes enheder, når de tilgår lokale netværksknudepunkter.
- Opsæt politikker for flerfaktorgodkendelse ved fjernlogin.
- Opsæt klient-til-site-konfigurationer med IPsec og OpenVPN.
- Gennemgå logfiler over fjernforbindelser for brud på adgangskontrollen.
- Indfør tilstandstjek af enheder, før der gives adgang til netværket.
- Optimér serverens gennemløb, så fjernarbejde ikke kvæler båndbredden.

VEJLEDNING TIL VPN TIL FJERNADGANG

Besvar multiple choice- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden på tilstandstjek og flerfaktorlogin.

KLIENT-TIL-SITE-TUNNELER OG ENHEDERS TILSTAND (INTRODUKTION)

VPN til fjernadgang opretter sikre klient-til-site-tunneler for medarbejdere uden for kontoret. At sikre disse forbindelser kræver flerfaktorgodkendelse (MFA) ved login, tilstandstjek af enhederne og revision af logfiler via centrale syslog-servere.

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

Kontrolpunkt 1: Multiple choice-udfordring

- 1** 1. Hvilken godkendelsesstandard bør portaler til fjernadgang kræve?

 - ☐ A) Flerfaktor
 - ☐ B) Én faktor
 - ☐ C) Ukrypteret
 - ☐ D) Lokal gæst
- 2** 2. Hvilken protokol er standard til at sikre klient-til-site-forbindelser ved fjernarbejde?

 - ☐ A) OpenVPN
 - ☐ B) SOCKS5
 - ☐ C) PPTP
 - ☐ D) FTP
- 3** 3. Hvilket tjek kontrollerer, om en fjern-pc er ren, før den forbinder?

 - ☐ A) Tilstandstjek
 - ☐ B) Hastighedstest
 - ☐ C) Pingtest
 - ☐ D) Hukommelsestælling
- 4** 4. Hvor gemmes fjernmedarbejdernes forbindelseslogfiler til sikkerhedsrevision?

 - ☐ A) Syslog-server
 - ☐ B) Registreringsnøgle
 - ☐ C) Klientens hukommelse
 - ☐ D) Webbrowseren
- 5** 5. Hvad sker der, når antallet af fjernmedarbejdere overstiger gatewayens båndbredde?

 - ☐ A) Båndbredden kvæles
 - ☐ B) DNS-lækage
 - ☐ C) Handshake godkendes
 - ☐ D) IP-adressen afsløres

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Flerfaktorgodkendelse tilføjer en ekstra kode, der sikrer fjernlogin.

☐ Sandt ☐ Falsk

7 Spørgsmål 7

7. Tilstandstjek giver enheder med slukket firewall adgang til private servere.

☐ Sandt ☐ Falsk

8 Spørgsmål 8

8. Logfiler fra fjernadgang er afgørende for at spore uautoriseret adgang til firmanetværket.

☐ Sandt ☐ Falsk

9 Spørgsmål 9

9. OpenVPN og IPsec er forældede protokoller, der ikke krypterer klientens data.

☐ Sandt ☐ Falsk

10 Spørgsmål 10

10. Gatewayens båndbredde kvæles, når fjerntrafikken overstiger netkortets kapacitet.

☐ Sandt ☐ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. For at beskytte firmaportaler skal fjernlogin kræve _____ godkendelse. _____ godkendelse.
2. Fjernklienter krypterer data i tunnelen med standardprotokoller som _____. _____ protokoller.
3. Enheder skal bestå et _____ sikkerhedstjek, før de får adgang til netværket. _____ tjek før de får adgang til netværket.
4. Logfiler til revision sendes løbende til en central _____-server. _____ server.
5. Tung trafik i arbejdstiden kan give _____ på gatewayen. _____ overbelastning.
6. Virtuelle adapterdrivere håndterer klient-til-site-_____ på Windows og macOS. _____ på Windows og macOS.

ORDBANK MED FAGUDTRYK

BAANDBREDDE

FIREWALL

FLERFAKTOR
TILSTANDKRYPTERING
TUNNELERING

OPENVPN

SYSLOG

Skriv dine svar her:

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

Kontrolpunkt 4: Match domænebegreber

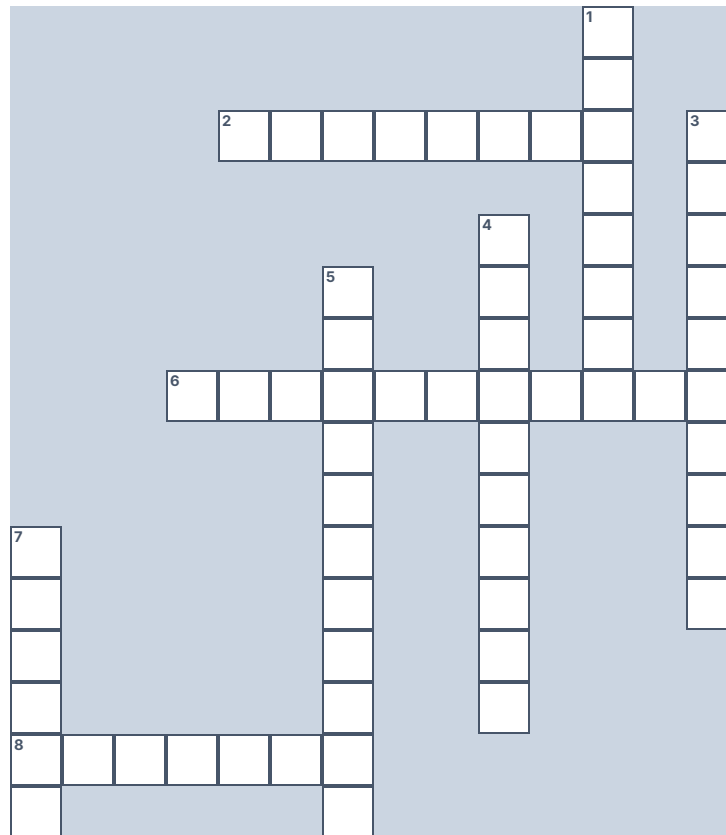
MATCH DEFINITIONER

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

	FLERFAKTOR	H	Systemregler der filtrerer trafik.
	OPENVPN	D	Central opsamler af sikkerhedslogfiler.
	TILSTAND	E	Grænse for netværkets datakapacitet.
	SYSLOG	F	Kryptografisk omformning af pakker.
	BÅNDBREDDE	G	Indpakning af data i en sikker vej.
	KRYPTERING	C	Kontrol af fjernhedens tilstand.
	TUNNELERING	A	Loginsikkerhed der kræver ekstra koder.
	FIREWALL	B	Standardprotokol til klient-til-site.

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

- 2. Systemregler der filtrerer trafik (8)
- 6. Grænse for netværkets datakapacitet (11)
- 8. Standardprotokol til klient-til-site (7)

LODRETTE NØGLER

- 1. Kontrol af fjernenhedens sikkerhedstilstand (8)
- 3. Kryptografisk omformning af pakker (10)
- 4. Loginsikkerhed der kræver ekstra koder (10)
- 5. Indpakning af data i en sikker vej (11)
- 7. Central opsamler af sikkerhedslogfiler (6)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

2 vandret: Systemregler der filtrerer trafik (8 bogstaver):

6 vandret: Grænse for netværkets datakapacitet (11 bogstaver):

8 vandret: Standardprotokol til klient-til-site (7 bogstaver):

LODRETTE NØGLER

1 lodret: Kontrol af fjernenhedens sikkerhedstilstand (8 bogstaver):

3 lodret: Kryptografisk omformning af pakker (10 bogstaver):

4 lodret: Loginsikkerhed der kræver ekstra koder (10 bogstaver):

5 lodret: Indpakning af data i en sikker vej (11 bogstaver):

7 lodret: Central opsamler af sikkerhedslogfiler (6 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

FLERFAKTOR

OPENVPN

TILSTAND

SYSLOG

BAANDBREDDE

KRYPTERING

TUNNELERING

FIREWALL

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK

- A. FLERFAKTOR
- B. OPENVPN
- C. TILSTAND
- D. SYSLOG
- E. BAANDBREDDE
- F. KRYPTERING
- G. TUNNELERING
- H. FIREWALL

DEFINITIONER OG MATCHFELTER

- 1. Loginsikkerhed der kræver ekstra koder.
- 2. Standardprotokol til klient-til-site.
- 3. Kontrol af fjernenhedens tilstand.
- 4. Central opsamler af sikkerhedslogfiler.
- 5. Grænse for netværkets datakapacitet.
- 6. Kryptografisk omformning af pakker.
- 7. Indpakning af data i en sikker vej.
- 8. Systemregler der filtrerer trafik.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige begreber om domænemægling. Skriv dine svar i indtastningsfelterne.

1. OKAFLETRRE

5. VNNEOPP

2. STDINATL

6. OLSSGY

3. BRBEADED
N

7. RPKREINGTY

4. ENGLNEIRTUN

8. EIWLFLAR

Kontrolpunkt 8: Casestudier om domænemægling

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

CASESTUDIE 1: KRAV OM MFA



Scenarie: En analytiker forsøger at logge ind i firmadatabasen under fjernarbejde. Brugernavn og adgangskode er korrekte, men VPN-portalen blokerer adgangen og kræver en kode fra en fysisk nøgle.

Diskussion: Hvilken sikkerhedspolitik står bag dette ekstra verifikationstrin?

CASESTUDIE 2: KRAV TIL ENHEDENS TILSTAND



Scenarie: En ekstern konsulent forbinder sin private bærbare til firmanetværket. VPN-klienten afbryder straks forbindelsen og oplyser, at antivirusdefinitionerne er forældede.

Diskussion: Hvilket særligt tjek på VPN-gatewayen blokerede dette forsøg?

Sidste udfordring: Afkod chifferet

En netværksingeniør sikrer routingkanaler og klienttunneler. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter. Afkodet cybersikkerhedsbesked:

BOGSTAV-TIL-TAL-KRYPTERINGSNØGLE

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

Afkodet cybersikkerhedsbesked:

19	9	11	11	5	18	6	10	5	18	14	1	4	7	1	14	7
	11	18	1	5	22	5	18	19	20	1	5	18	11	5		
		11	15	14	20	18	15	12	12	5	18					

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z).

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del A)

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

Q1: Hvad er VPN til fjernadgang?

En sikker forbindelsesmetode, der lader medarbejdere uden for kontoret forbinde direkte til firmaets private servere.

Q2: Hvad er forskellen på klient-til-site og site-til-site?

Klient-til-site forbinder enkelte brugerenheder, mens site-til-site forbinder hele fysiske kontorer.

Q3: Hvad er et tilstandstjek af en enhed?

En scanning, der kontrollerer fjernenhedens sikkerhed (antivirus, opdateringsniveau), før der gives adgang.

Q4: Hvorfor bruges OpenVPN til fjernadgang?

På grund af den stærke sikkerhedsprotokol, understøttelsen af flere platforme og evnen til at håndtere enkeltforbindelser.

Q5: Hvordan beskytter MFA fjernadgang?

Den tilføjer en ekstra kode, så adgang blokeres, selv hvis medarbejderens adgangskode er lækket eller stjålet.

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del B)

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

Q6: Hvad er en syslog-server?

Et centralt logarkiv, der gemmer forbindelseshændelser, login og systemadvarsler til brug for revision.

Q7: Hvad kvæler båndbredden?

Når fjernmedarbejdernes samlede båndbreddebehov overstiger hastigheden på firmaets gateway.

Q8: Kan jeg forbinde min hjemmecomputer til firmaets VPN?

Kun hvis enheden består firmaets tilstandstjek og er godkendt af IT-administratorerne.

Q9: Hvad er indkapsling i netværket?

Indpakning af datapakker under transport i krypterede protokolhoveder, så overførslen sikres.

Q10: Hvordan optimerer split tunneling fjernadgang?

Den lader medarbejdere bruge deres lokale udbyder til almindelig surfing, mens arbejdsfiler sendes gennem VPN'en.

Kontrolpunkt 11: Avanceret VPN-FAQ (del A)

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

Q1: Hvordan styrker certifikatbaseret godkendelse fjernadgang?

Den binder adgangen til forudinstallerede digitale certifikater og blokerer uadministrerede eller uautoriserede enheder.

Q2: Hvilken sikkerhedsrisiko giver split tunneling ved fjernarbejde?

Den skaber en mulig bro, hvor en kompromitteret lokal enhed kan føre trusler ind i det private netværk.

Q3: Hvordan undersøger tilstandstjek registreringsdatabasen?

VPN-klienten kører lokale scripts, der læser registreringsstier for at se, om firmaets sikkerhedssoftware kører.

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

For at sende logfiler hurtigt med mindst mulig overhead, selvom sikre opsætninger i dag kræver TLS over TCP.

Q5: Hvordan løser virksomheder flaskehalse på gatewayen?

Ved at indføre load balancere og fordele fjerntrafikken på regionale serverknodepunkter.

Kontrolpunkt 11: Avanceret VPN-FAQ (del B)

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

Q6: Hvad bruges virtuelle TAP/TUN-adaptre til på fjernklienter?

De fungerer som virtuelle netkort og sender enhedens TCP/IP-trafik direkte ind i den krypterede tunnel.

Q7: Hvordan understøtter IKEv2 MOBIKE mobilt fjernarbejde?

Den opdaterer løbende bindingen til IP-adressen, så VPN'en holder ved skift mellem Wi-Fi og mobildata.

Q8: Hvad er forskellen på split og fuld tunnelrouting?

Fuld routing sender al enhedens internettrafik gennem VPN'en, mens split routing kun sender trafik til firmaets adresser.

Q9: Hvordan håndterer NAT-enheder VPN-fjernforbindelser?

Ved at knytte lokale portintervaller til offentlige gateway-IP-adresser, så returnerende krypterede pakker finder vej.

Q10: Hvilke standarder kræver revision af fjernadgang?

Standarder som HIPAA, SOC 2 og PCI DSS kræver logning og overvågning af alle fjernforbindelser.

Del 11: 10 VPN-fakta og indsigter fra virkeligheden

Gennemgå virkelige fakta om VPN-krypteringshastigheder, protokolrevisioner, mobil forbindelse og fjernarbejde i virksomheder.

1. VPN-INDSIGT

VPN til fjernadgang opretter sikre klient-til-site-tunneler for medarbejdere uden for kontoret.

2. VPN-INDSIGT

Regelsæt kræver flerfaktorgodkendelse for at beskytte virksomhedens portaler til fjernadgang.

3. VPN-INDSIGT

Tilstandstjek kontrollerer klientens lokale sikkerhedsindstillinger, før der gives adgang til det private netværk.

4. VPN-INDSIGT

Syslog-servere samler forbindelseslogfiler, så uautoriserede adgangsforsøg kan opdages og revideres.

5. VPN-INDSIGT

Gatewayens båndbredde kvæles, når den samlede fjerntrafik overstiger serverens internetgrænse.

6. VPN-INDSIGT

Virtuelle netværksadapters pakker styresystemets netværksforespørgsler ind i sikre protokoller.

7. VPN-INDSIGT

Understøttelse af MOBIKE lader fjernklienter skifte netværk uden at miste VPN-tunnelen.

8. VPN-INDSIGT

Fuld tunnelrouting sikrer al medarbejderens internettrafik, men belaster firmaets gateway mere.

9. VPN-INDSIGT

Certifikatgodkendelse binder adgangen til VPN direkte til firmaets administrerede hardware.

10. VPN-INDSIGT

SOC 2 kræver detaljeret logning og sporing af alle fjernlogin i virksomheden.

Tekniske referencer og kilder

Studieguiden og de interaktive opgaver er sammensat ud fra globale tekniske standarder, specifikationer og lovgivningsmæssige rammer.

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[1] NIST Special Publication 800-46: Sikring af systemer til fjernadgang.

<https://csrc.nist.gov/>

[3] OpenVPN: konfiguration og specifikationer for klient-til-site.

<https://openvpn.net/>

[5] Implementeringsguide til flerfaktorgodkendelse (MFA).

<https://owasp.org/>

[7] IETF RFC 5246: Transport Layer Security-protokollen (TLS).

<https://datatracker.ietf.org/doc/rfc5246/>

[9] Sikkerhedstjekliste og god praksis for fjernarbejde.

<https://www.cisa.gov/>

[2] CISA's retningslinjer for sikkerhed ved hjemmearbejde og fjernadgang.

<https://www.cisa.gov/>

[4] Syslog-protokollen og standarder for sikkerhedslogfiler.

<https://datatracker.ietf.org/>

[6] Tilstandstjek af enheder og regler for overholdelse.

<https://www.vpn.com/posture/>

[8] Planlægning af båndbredde og justering af netværkskapacitet.

<https://www.cloudflare.com/>

[10] NIST's retningslinjer for sikring af mobile arbejdsstationer.

<https://csrc.nist.gov/>

Facitliste: Kontrolpunkt 1 – Multiple choice

1 Loginkoder

MFA-SIKKERHED

Rigtigt svar: A

UNDERVISNINGSNOTE

Flerfaktorgodkendelse kræver ekstra verifikation ved login. Kilde: MFA Implementation [Ref 5].

Flerfaktorgodkendelse kræver ekstra verifikation ved login.

2 OpenVPN-tunnel

KLIENT-TIL-SITE

Rigtigt svar: A

UNDERVISNINGSNOTE

OpenVPN er en standardprotokol til sikring af klient-til-site-tunneler. Kilde: OpenVPN Client [Ref 3].

OpenVPN er en standardprotokol til sikring af klient-til-site-tunneler.

3 Tilstandsrevision

ENHEDSTJEK

Rigtigt svar: A

UNDERVISNINGSNOTE

Tilstandstjek scanner enheder for aktiv firewall og antivirus. Kilde: Posture Compliance [Ref 6].

Tilstandstjek scanner enheder for aktiv firewall og antivirus.

4 Logopsamler

SYSLOG-SERVER

Rigtigt svar: A

UNDERVISNINGSNOTE

Syslog-servere samler sikkerhedslogfiler og overvåger brud på adgangskontrollen. Kilde: Syslog Standard [Ref 4].

Syslog-servere samler sikkerhedslogfiler og overvåger brud på adgangskontrollen.

5 Netkort
overbelastet

GATEWAY KVÆLES

Rigtigt svar: A

UNDERVISNINGSNOTE

Gatewayens båndbredde kvæles, når brugertrafikken overstiger serverens grænser. Kilde: Capacity Planning [Ref 8].

Gatewayens båndbredde kvæles, når brugertrafikken overstiger serverens grænser.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6

Loginkoder

MFA-KONTROL

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Flerfaktorgodkendelse kræver ekstra verifikation ved login. Kilde: MFA Implementation [Ref 5].

Flerfaktorgodkendelse kræver ekstra verifikation ved login.

7

OpenVPN-tunnel

OPENVPN-KLIENT

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

OpenVPN er en standardprotokol til sikring af klient-til-site-tunneler. Kilde: OpenVPN Client [Ref 3].

OpenVPN er en standardprotokol til sikring af klient-til-site-tunneler.

8

Tilstandsrevision

COMPLIANCE-TJEK

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Tilstandstjek scanner enheder for aktiv firewall og antivirus. Kilde: Posture Compliance [Ref 6].

Tilstandstjek scanner enheder for aktiv firewall og antivirus.

9

Logopsamler

SYSLOG-SERVER

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Syslog-servere samler sikkerhedslogfiler og overvåger brud på adgangskontrollen. Kilde: Syslog Standard [Ref 4].

Syslog-servere samler sikkerhedslogfiler og overvåger brud på adgangskontrollen.

10

Netkort
overbelastet

GATEWAY KVÆLES

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Gatewayens båndbredde kvæles, når brugertrafikken overstiger serverens grænser. Kilde: Capacity Planning [Ref 8].

Gatewayens båndbredde kvæles, når brugertrafikken overstiger serverens grænser.

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

A FLERFAKTOR	B OPENVPN	C TILSTAND	D SYSLOG
E BÅNDBREDDE	F KRYPTERING	G TUNNELERING	H FIREWALL

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

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

DISKUSSIONSNOTER TIL UNDERVISERE

Vurderingsnøjagtighed:

Kontrollér, at eleverne forstår, hvordan domænelængde, endelse (.com, .ai) og kommerciel søgevolumen påvirker vurderingsprisen.

Deponeringssikkerhed:

Understreg, at midlerne opbevares på licenserede tredjepartskonti, indtil overdragelsen af domænets WHOIS er verificeret.

Anonym repræsentation:

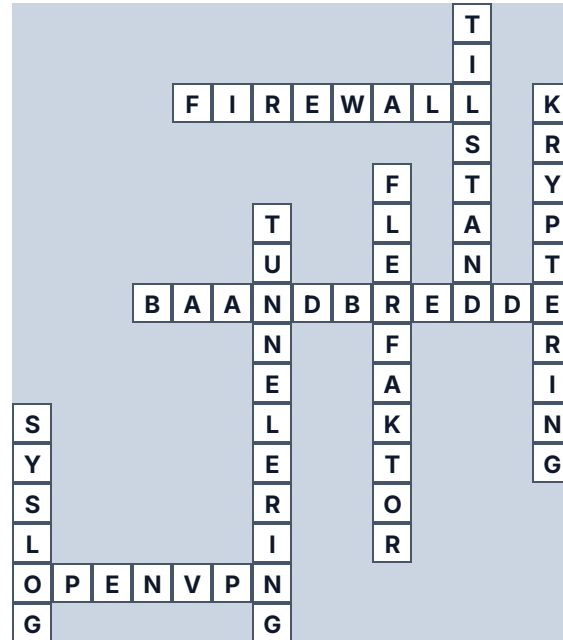
Fremhæv, hvordan fortrolighedsaftaler og tredjepartsrepræsentation forhindrer spekulative prisstigninger under virksomhedsindkøb.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: FIREWALL Systemregler der filtrerer trafik (3,4)

6 vandret: BAANDBREDDE Grænse for netværkets datakapacitet (8,3)

8 vandret: OPENVPN Standardprotokol til klient-til-site (15,0)

LODRETTE NØGLER

1 lodret: TILSTAND Kontrol af fjernhedens sikkerhedstilstand (1,11)

3 lodret: KRYPTERING Kryptografisk omformning af pakker (3,13)

4 lodret: FLERFAKTOR Loginsikkerhed der kræver ekstra koder (5,9)

5 lodret: TUNNELERING Indpakning af data i en sikker vej (6,6)

7 lodret: SYSLOG Central opsamler af sikkerhedslogfiler (11,0)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. OKAFLFTRRE	FLERFAKTOR	5. VNNEOPP	OPENVPN
2. STDINATL	TILSTAND	6. OLSSGY	SYSLOG
7. BRBEAADEDDN	BAANDBREDDE	3. RPKREINGTY	KRYPTERING
4. ENGLNEIRTUN	TUNNELERING	8. EIWLFLAR	FIREWALL

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"SIKKER FJERNADGANG KRAEVER STAERKE KONTROLLER"

Facit til VPN- og netværkscasestudier

A Casestudie 1: Krav om MFA

[Underviserens løsning](#)

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En analytiker forsøger at logge ind i firmadatabasen under fjernarbejde. Brugernavn og adgangskode er korrekte, men VPN-portalen blokerer adgangen og kræver en kode fra en fysisk nøgle.
- Anbefalet strategi og løsning: Virksomhedens VPN-portal håndhæver en streng politik om flerfaktorgodkendelse (MFA), der sikrer fjernlogin.

B Casestudie 2: Krav til enhedens tilstand

[Underviserens løsning](#)

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En ekstern konsulent forbinder sin private bærbare til firmanetværket. VPN-klienten afbryder straks forbindelsen og oplyser, at antivirusdefinitionerne er forældede.
- Anbefalet strategi og løsning: Gatewayen til fjernadgang udførte et tilstandstjek af enheden og blokerede den på grund af forældede sikkerhedsindstillinger.