

Navn: _____

Dato: _____

Point: _____

Surfsharks sikkerhed

Gennemgang af Surfsharks sikkerhed, herunder CleanWeb, MultiHop

OVERBLIK OVER SURFSHARKS SIKKERHED

ELEV

ELEVSTATUS

Netværksforsvarer-spor

SIKKER

FORBINDELSSTATUS

Beskytter datapakker

100%

LÆKAGEFORSVAR

DNS- og IPv6-lækagebeskyttelse

Velkommen! Dette opgavehæfte guider dig gennem

Surfsharks sikkerhedsopbygning. Du vil udforske servere med kun RAM, dynamisk IP-rotation i SDN-nettet Nexus, reklameblokering med CleanWeb og routing med MultiHop.

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/surfshark-security/>

Din læringsplan for Surfsharks sikkerhed

- Analysér den tekniske opbygning og reglerne bag Surfsharks sikkerhed.
- Konfigurer klientindstillinger, så IP-, DNS- og WebRTC-trafik ikke lækker.
- Sammenlign skræddersyet prissætning, prøveperiode og ydeevne med standardmodellerne.

VEJLEDNING TIL SURFSHARKS SIKKERHED

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 om servere med kun RAM, SDN-nettet Nexus og CleanWeb.

SERVERE MED KUN RAM, SDN-NETTET NEXUS OG CLEANWEB (INTRODUKTION)

Surfshark beskytter brugerne fuldt ud med servere, der 100 % kører på RAM, det softwaredefinerede net Nexus med IP Rotator, reklameblokering med CleanWeb og krypterede ruter med Dynamic MultiHop.

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

Kontrolpunkt 1: Multiple choice-udfordring

1 1. Hvad hedder Surfsharks indbyggede blokering af reklamer og skadesoftware?

- ☐ A) AdGuard
- ☐ B) CleanWeb
- ☐ C) ThreatShield
- ☐ D) NetBlocker

2 2. Hvilken hardware bruger Surfshark på alle servere?

- ☐ A) Harddiske
- ☐ B) 100 % kun RAM
- ☐ C) Optisk lagring
- ☐ D) Magnetbånd

3 3. Hvilken funktion sender trafikken gennem to forskellige servere?

- ☐ A) Bypasser
- ☐ B) MultiHop (dobbelt VPN)
- ☐ C) Nexus-nettet
- ☐ D) Fast IP

4 4. Hvilken sløring forklæder VPN-trafik som almindelig webtrafik?

- ☐ A) Kill switch
- ☐ B) Camouflage
- ☐ C) CleanWeb 2.0
- ☐ D) Split tunneling

5 5. Hvad gør Surfsharks Bypasser?

- ☐ A) Øger hastigheden
- ☐ B) Split tunneling
- ☐ C) Adgangskodeadministrator
- ☐ D) DNS-server

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Servere med kun RAM sletter alle data øjeblikkeligt ved genstart.

☐

Sandt

☐

Falsk

7 Spørgsmål 7

7. Camouflage forhindrer udbyderen i at se, at du bruger VPN.

☐

Sandt

☐

Falsk

8 Spørgsmål 8

8. CleanWeb 2.0 blokerer cookie-bannere via browserudvidelser.

☐

Sandt

☐

Falsk

9 Spørgsmål 9

9. Surfshark gemmer midlertidigt tidspunkter og båndbreddeforbrug.

☐

Sandt

☐

Falsk

10 Spørgsmål 10

10. Nexus skifter jævnligt brugerens IP uden at afbryde forbindelsen.

☐

Sandt

☐

Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. Irriterende reklamer, springsscripts og phishinglinks blokeres af _____ filtre.
2. Brugernes aktivitet efterlader ingen spor, fordi serverne kører i _____ hukommelse.
3. Data sendes gennem to krypterede servere med _____ tunneler.
4. For at skjule VPN-brug for udbyderen slår man _____ tilstand.
5. At lade netbankprogrammer gå uden om tunnelen styres af _____ indstillinger.
6. Den nye SDN-opbygning, der forbinder alle servere, er _____ systemet.

ORDBANK MED FAGUDTRYK

BYPASSER

CAMOUFLAGE

CLEANWEB
MULTIHOPIPROTATOR
NEXUS

KILLSWITCH

KUNRAM

Skriv dine svar her:

1.

2.

3.

4.

5.

6.

Kontrolpunkt 4: Match VPN- og netværksbegreber

MATCH DEFINITIONER

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

CLEANWEB

D

Sløring, der skjuler VPN-kendetegn, så trafikken ligner almindelig HTTPS.

RAMONLYX

E

Split tunneling, der lader udvalgte programmer gå uden om VPN'en.

MULTIHOP

A

Et avanceret filter mod reklamer, skadesoftware og cookie-bannere.

CAMOFLGE

H

En funktion, der jævnligt skifter din IP uden at afbryde tunnelen.

BYPASSER

G

Et eget softwaredefineret net, der samler alle servere.

KILLSWCH

C

Dobbelt VPN, der krypterer trafikken gennem to servere.

NEXUSNET

B

Servere med flygtig hukommelse, der sletter alt ved hver genstart.

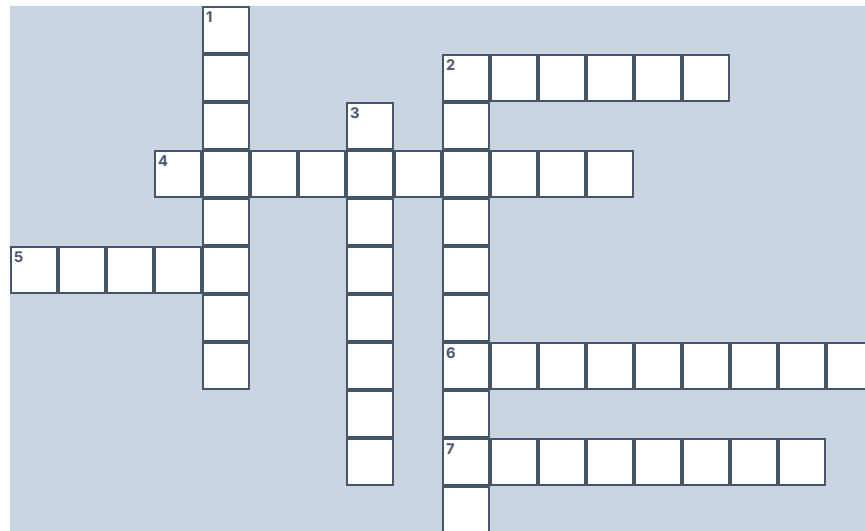
ROTATING

F

En automatisk sikkerhedsfunktion, der blokerer trafikken ved udfald.

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. Servere der sletter alt ved genstart (6)
- 4. Sloering der ligner HTTPS (10)
- 5. Softwaredefineret servernet (5)
- 6. Skifter IP uden at afbryde (9)
- 7. Filter mod reklamer og skadesoftware (8)

LODRETTE NØGLER

- 1. Lader programmer gaa uden om VPN (8)
- 2. Blokerer trafikken ved udfald (10)
- 3. Dobbelt VPN gennem to lande (8)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

2 vandret: Servere der sletter alt ved genstart (6 bogstaver):

4 vandret: Sloering der ligner HTTPS (10 bogstaver):

5 vandret: Softwaredefineret servernet (5 bogstaver):

6 vandret: Skifter IP uden at afbryde (9 bogstaver):

7 vandret: Filter mod reklamer og skadesoftware (8 bogstaver):

LODRETTE NØGLER

1 lodret: Lader programmer gaa uden om VPN (8 bogstaver):

2 lodret: Blokerer trafikken ved udfald (10 bogstaver):

3 lodret: Dobbelt VPN gennem to lande (8 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

CLEANWEB

KUNRAM

MULTIHOP
NEXUSCAMOUFLAGE
IPROTATOR

BYPASSER

KILLSWITCH

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. CLEANWEB
- B. RAMONLYX
- C. MULTIHOP
- D. CAMOFLGE
- E. BYPASSER
- F. KILLSWCH
- G. NEXUSNET
- H. ROTATING

DEFINITIONER OG MATCHFELTER

- ☐ 1. Et avanceret filter mod reklamer, skadesoftware og cookie-bannere.
- ☐ 2. Servere med flygtig hukommelse, der sletter alt ved hver genstart.
- ☐ 3. Dobbelt VPN, der krypterer trafikken gennem to servere.
- ☐ 4. Sløring, der skjuler VPN-kendetegn, så trafikken ligner almindelig HTTPS.
- ☐ 5. Split tunneling, der lader udvalgte programmer gå uden om VPN'en.
- ☐ 6. En automatisk sikkerhedsfunktion, der blokerer trafikken ved udfald.
- ☐ 7. Et eget softwaredefineret net, der samler alle servere.
- ☐ 8. En funktion, der jævnligt skifter din IP uden at afbryde tunnelen.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige begreber om virtuelle private netværk (VPN). Skriv dine svar i indtastningsfelterne.

1. EANCWLBE

5. RNMKAU

2. TMPUOHIL

6. GUOLACAFEM

3. AYBSSREP

7. ILKIWTCHSL

4. XSUNE

8. RTOIOPATR

Kontrolpunkt 8: VPN- og netværkscasestudier

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

CASESTUDIE 1: OMGÅELSE AF FILTRE PÅ SKOLE OG ARBEJDE



Scenarie: En studerende opdager, at universitetets wi-fi blokerer alle almindelige porte til OpenVPN og WireGuard.

Diskussion: Hvilken funktion i Surfshark lader den studerende forbinde uden at blive opdaget af netværksadministratorerne?

CASESTUDIE 2: RISIKABEL JOURNALISTISK UNDERSØGELSE



Scenarie: En undersøgende journalist har brug for ekstra beskyttelse mod overvågning under research i følsomme virksomhedsdokumenter.

Diskussion: Hvordan giver Dynamic MultiHop bedre beskyttelse end routing gennem én server?

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.

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

3	1	13	15	21	6	12	1	7	5	19	11	10	21	12	5	18	
4	9	14	22	16	14	6	15	18	21	4	2	25	4	5	18	5	14

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 Surfshark CleanWeb?

CleanWeb er en indbygget funktion, der blokerer reklamer, sporing, skadesoftware og phishingsider.

Q2: Hvad er servere med kun RAM?

Servere, der kører i flygtig hukommelse, så alle data slettes øjeblikkeligt ved genstart.

Q3: Hvad er Surfshark MultiHop?

MultiHop (dobbelt VPN) sender og krypterer forbindelsen gennem to forskellige lokationer.

Q4: Hvordan virker Camouflage?

Camouflage slører VPN-trafikken, så udbyderen ikke kan se, at du bruger VPN.

Q5: Hvad er Bypasser?

Bypasser er Surfsharks split tunneling, der lader bestemte programmer eller websteder gå uden om VPN'en.

Kontrolpunkt 10: Grundlæggende VPN-FAQ (del B)

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

Q6: Har Surfshark en kill switch?

Ja, den afbryder internettet, hvis VPN'en pludselig falder ud.

Q7: Hvilken kryptering bruger Surfshark?

Surfshark bruger AES-256-GCM med SHA-512 til godkendelse.

Q8: Er no-logs-politikken revideret?

Ja, Deloitte har uafhængigt revideret og bekræftet den.

Q9: Hvad er Surfshark Nexus?

Nexus er en avanceret SDN-opbygning, der samler alle servere i ét net for jævnere routing.

Q10: Hvad er IP Rotator?

IP Rotator skifter automatisk din IP med få minutters mellemrum uden at afbryde forbindelsen.

Kontrolpunkt 11: Avanceret VPN-FAQ (del A)

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

Q1: Hvordan adskiller Dynamic MultiHop sig fra almindelig dobbelt VPN?

Du kan selv vælge enhver kombination af indgangs- og udgangsserver i hele verden.

Q2: Virker CleanWeb 2.0 i browserudvidelser?

Ja, den blokerer videoreklamer, cookie-bannere og advarselsbannere i Chrome og Firefox.

Q3: Hvad er Alternative ID?

Alternative ID laver unikke aliaser, e-mailadresser og skjulte telefonnumre.

Q4: Hvordan forhindrer Surfshark DNS-lækager?

Alle opslag går gennem private DNS-servere uden viden om brugeren på hver server.

Q5: Understøtter Surfshark ChaCha20 på mobil?

Ja, WireGuard på Android og iOS bruger ChaCha20-Poly1305, der er meget effektiv på mobil.

Kontrolpunkt 11: Avanceret VPN-FAQ (del B)

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

Q6: Hvad er NoBorders?

NoBorders opdager automatisk begrænsede net og tilbyder særlige servere.

Q7: Hvem har revideret browserudvidelserne?

Det uafhængige sikkerhedsfirma Cure53 har revideret både udvidelser og servere.

Q8: Hvordan beskytter Surfshark mod IPv6-lækager?

IPv6 sendes sikkert gennem tunnelen eller blokeres, så intet lækker ukrypteret.

Q9: Hvilket lands lovgivning gælder for Surfshark?

Hollandsk lov, med den strenge europæiske databeskyttelsesforordning (GDPR).

Q10: Understøtter Surfshark sikkerhedsnøgler til tottrinsbekræftelse?

Ja, kontoen kan sikres med FIDO2-nøgler og godkendelsesapps.

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

1. Alle Surfsharks 3.200+ servere kører udelukkende på flygtig RAM uden diske.

2. VPN-INDSIGT

2. Revisionsgiganten Deloitte har bekræftet, at Surfshark overholder sin strenge no-logs-politik.

3. VPN-INDSIGT

3. Nexus samler alle servere verden over i et dynamisk softwaredefineret net.

4. VPN-INDSIGT

4. IP Rotator skifter brugerens IP hvert 5.-10. minut uden at afbryde forbindelsen.

5. VPN-INDSIGT

5. CleanWeb 2.0 blokerer påtrængende cookie-bannere og videoreklamer direkte i browseren.

6. VPN-INDSIGT

6. Dynamic MultiHop lader dig bygge egne ruter gennem to servere i op til 100 lande.

7. VPN-INDSIGT

7. Camouflage fjerner VPN-kendetegn, så trafikken ikke kan skelnes fra almindelig HTTPS.

8. VPN-INDSIGT

8. Alternative ID laver engangsaliasser og skjulte e-mails, der beskytter mod datalæk.

9. VPN-INDSIGT

9. Surfshark bruger AES-256-GCM og ChaCha20 med WireGuard.

10. VPN-INDSIGT

10. NoBorders slås automatisk til på begrænsede net og giver en robust tunnel.

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] Surfshark B.V. (2024). Surfshark VPN: opbygning, MultiHop i Nexus og servere med kun RAM.

<https://surfshark.com/features>

[3] Deloitte. (2023). Uafhængig erklæring: Surfsharks overholdelse af no-logs og serveropsætning. Deloitte Audit.

<https://surfshark.com/blog/no-logs-audit>

[5] Frankel, S., Hoffman, P., Orebaugh, A. og Park, R. (2020). Guide to IPsec VPNs (NIST Special Publication 800-77 Rev. 1). National Institute of Standards and Technology.

<https://doi.org/10.6028/NIST.SP.800-77r1>

[7] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P. og Kivinen, T. (2014). Internet Key Exchange Protocol Version 2 (IKEv2) (RFC 7296). IETF.

<https://datatracker.ietf.org/doc/html/rfc7296>

[2] Surfshark B.V. (2024). Servicevilkår, 30 dages pengene-tilbage-garanti og abonnementer.

<https://surfshark.com/pricing>

[4] Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). Internet Engineering Task Force (IETF).

<https://datatracker.ietf.org/doc/html/rfc8446>

[6] Barker, E. og McKay, K. (2019). Guidelines for the Selection, Configuration, and Use of TLS Implementations (NIST SP 800-52 Rev. 2). NIST.

<https://doi.org/10.6028/NIST.SP.800-52r2>

[8] Electronic Frontier Foundation. (2024). Surveillance Self-Defense: Choosing the VPN That's Right for You. EFF.

<https://ssd.eff.org/module/choosing-vpn-thats-right-you>

Facitliste: Kontrolpunkt 1 – Multiple choice

1

**Indbygget
indholdsblokering**

FORSVAR MOD REKLAMER OG SKADESOFTWARE

Rigtigt svar: B

UNDERVISNINGSNOTE

CleanWeb er Surfsharks indbyggede filter, der på netværksniveau blokerer reklamer, sporingsdomæner, phishingsider og skadelige scripts. Kilde: CleanWebs sikkerhedsspecifikationer [Ref 1].

CleanWeb er Surfsharks indbyggede filter, der blokerer reklamer, sporingsdomæner, phishingsider og skadelige scripts på

2

**100 % servere med
kun RAM**

RAM-OPBYGNING

Rigtigt svar: B

UNDERVISNINGSNOTE

Surfshark kører udelukkende servere uden diske, hvor styresystem og data ligger i flygtig hukommelse og forsvinder helt ved genstart. Kilde: Cure53s revision [Ref 2].

Surfshark kører udelukkende servere uden diske, hvor styresystem og data ligger i flygtig hukommelse og forsvinder

3

**Dobbelt tunnel
med MultiHop**

MULTIHOP-VPN

Rigtigt svar: B

UNDERVISNINGSNOTE

MultiHop (dobbelt VPN) krypterer trafikken gennem to servere i hvert sit land og forhindrer korrelationsangreb. Kilde: Surfsharks guide til MultiHop [Ref 3].

MultiHop (dobbelt VPN) krypterer trafikken gennem to servere i hvert sit land og forhindrer korrelationsangreb.

4

**Sløring med
Camouflage**

OBFUSKERING

Rigtigt svar: B

UNDERVISNINGSNOTE

Camouflage ændrer OpenVPN-headerne, så VPN-trafik ligner HTTPS og slipper forbi strenge firewalls. Kilde: Surfsharks hvidbog om sløring [Ref 4].

Camouflage ændrer OpenVPN-headerne, så VPN-trafik ligner HTTPS og slipper forbi strenge

5

**Split tunneling med
Bypasser**

SPLIT TUNNELING

Rigtigt svar: B

UNDERVISNINGSNOTE

Bypasser er Surfsharks split tunneling, hvor valgte programmer eller websteder går direkte via den almindelige forbindelse. Kilde: Surfsharks programfunktioner [Ref 5].

Bypasser er Surfsharks split tunneling, hvor valgte programmer eller websteder går direkte via den almindelige

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 Sletning i flygtig hukommelse SERVERSIKKERHED

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Servere med kun RAM gemmer intet på faste diske; en genstart sletter straks al hukommelse. Kilde: Opbygning af RAM-servere [Ref 6].

Servere med kun RAM gemmer intet på faste diske; en genstart sletter straks al hukommelse.

7 Skjult for udbyderen med Camouflage SKJULT TRAFIK

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Camouflage fjerner OpenVPNs kendetegn, så udbyderen ikke kan se, at brugeren er på VPN. Kilde: Guide til dyb pakkeinspektion [Ref 7].

Camouflage fjerner OpenVPNs kendetegn, så udbyderen ikke kan se, at brugeren er på VPN.

8 CleanWeb 2.0 i browseren BROWSERUDVIDELSE

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

CleanWeb 2.0 blokerer via browserudvidelser cookie-bannere, videoreklamer og skadelige omdirigeringer i real- tid. Kilde: Udgivelsesnoter til CleanWeb 2.0 [Ref 8].

CleanWeb 2.0 blokerer via browserudvidelser cookie-bannere, videoreklamer og skadelige omdirigeringer i real-

9 Ingen logning af forbindelser NO-LOGS-POLITIK

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Surfshark har en streng, uafhængigt revideret no-logs-politik og gemmer hverken IP-adresser, tidspunkter eller forbrug. Kilde: Deloitte's revision [Ref 9].

Surfshark har en streng, uafhængigt revideret no-logs-politik og gemmer hverken IP-adresser, tidspunkter eller

10 Dynamisk IP-rotation i Nexus NEXUS-NETTET

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Det softwaredefinerede net Nexus skifter brugerens IP med få minutters mellemrum uden at afbryde forbindelsen. Kilde: Opbygningen af Nexus [Ref 10].

Det softwaredefinerede net Nexus skifter brugerens IP med få minutters mellemrum uden at afbryde

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 CLEANWEB	B RAMONLYX	C MULTI HOP	D CAMOFLGE
E BYPASSER	F KILLSWCH	G NEXUSNET	H ROTATING

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 CLEANWEB	2 RAMONLYX	3 MULTI HOP	4 CAMOFLGE
5 BYPASSER	6 NEXUSNET		

DISKUSSIONSNOTER TIL UNDERVISERE

Protokollens ydeevne:

Kontrollér, at eleverne forstår, hvordan WireGuard, OpenVPN og proprietære protokoller afvejer kryptografisk belastning mod forsinkelse i gennemløbet.

Privatliv og jurisdiktion:

Understreg betydningen af uafhængige tredjepartsrevisioner af no-logs-politikker (Deloitte, Cure53, SEC Consult) og privatlivsvenlige jurisdiktioner.

Infrastruktursikkerhed:

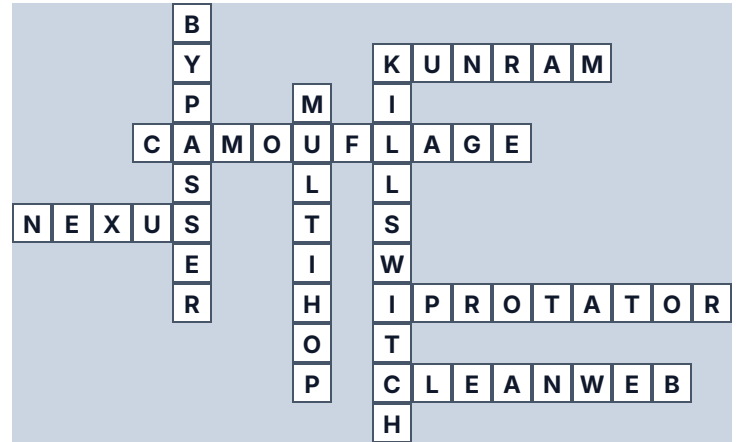
Fremhæv kill switch-beskyttelse, diskløse RAM-only-serverparker, forebyggelse af DNS-lækager og multi-hop-routing.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: KUNRAM Servere der sletter alt ved genstart (7,10)

4 vandret: CAMOUFLAGE Sloering der ligner HTTPS (9,4)

5 vandret: NEXUS Softwaredefineret servernet (11,1)

6 vandret: IPROTATOR Skifter IP uden at afbryde (13,10)

7 vandret: CLEANWEB Filter mod reklamer og skadesoftware (15,10)

LODRETTE NØGLER

1 lodret: BYPASSER Lader programmer gaa uden om VPN (6,5)

2 lodret: KILLSWITCH Blokerer trafikken ved udfald (7,10)

3 lodret: MULTI HOP Dobbelt VPN gennem to lande (8,8)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. EANCWLBE	CLEANWEB	5. RNMKAU	KUNRAM
2. TMPUOHIL	MULTIHOP	6. GUOLACAFEM	CAMOUFLAGE
3. AYBSSREP	BYPASSER	7. ILKIWTCHSL	KILLSWITCH
4. XSUNE	NEXUS	8. RTOIOPATR	IROTATOR

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"CAMOUFLAGE SKJULER DIN VPN FOR UDBYDEREN"

Facit til VPN- og netværkscasestudier

A CASESTUDIE 1: OMGÅELSE AF FILTRE PÅ SKOLE OG ARBEJDE

[Underviserens løsning](#)

BEDØMMELSESKRITERIER OG LØSNINGSVEJLEDNING

- Analyse af scenariet: En studerende opdager, at universitetets wi-fi blokerer alle almindelige porte til OpenVPN og WireGuard.
- Fokusspørgsmål: Hvilken funktion i Surfshark lader den studerende forbinde uden at blive opdaget af administratorerne?
- Anbefalet strategi og løsning: Den studerende bør slå Camouflage til (med OpenVPN), der fjerner VPN-kendetegn, så firewallen kun ser almindelig HTTPS-surfing.

B CASESTUDIE 2: RISIKABEL JOURNALISTISK UNDERSØGELSE

[Underviserens løsning](#)

BEDØMMELSESKRITERIER OG LØSNINGSVEJLEDNING

- Analyse af scenariet: En undersøgende journalist har brug for ekstra beskyttelse mod overvågning under research i følsomme virksomhedsdokumenter.
- Fokusspørgsmål: Hvordan giver Dynamic MultiHop bedre beskyttelse end routing gennem én server?
- Anbefalet strategi og løsning: Dynamic MultiHop krypterer data to gange via en indgangsserver i ét land og en udgangsserver i et andet, så intet enkelt punkt kan kompromittere forbindelsen.

C CASESTUDIE 3: NETBANK UDEN OM VPN

[Underviserens løsning](#)

BEDØMMELSESKRITERIER OG LØSNINGSVEJLEDNING

- Analyse af scenariet: En bruger vil have VPN-beskyttelse hele tiden, men bankens app blokerer udenlandske VPN-adresser.
- Fokusspørgsmål: Hvordan kan brugeren opsætte Bypasser for at løse konflikten?
- Anbefalet strategi og løsning: Brugeren kan undtage bankens app i Bypasser (split tunneling), så den går direkte via udbyderen, mens alle andre programmer forbliver krypterede.