Nimi: _____ Päivämäärä: _____ Pisteet: _____

Surfsharkin tietoturva

Surfsharkin tietoturvaominaisuuksien tarkastelu, mukaan lukien CleanWeb-mainosesto, MultiHop-dynaaminen reititys, Nexus SDN -arkkitehtuuri, vain RAM-muistia käyttävä palvelinpark ja Camouflage-tila.

SURFSHARKIN TIETOTURVAN OPPIMISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: Surfsharkin tietoturva-arkkitehtuuri. Tutustut vain RAM-muistissa toimivaan palvelinlaitteistoon, Nexus SDN:n dynaamiseen IP-kierrätykseen, CleanWeb-mainosten estoon ja MultiHop-reititykseen.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse VPN- ja verkkoturvallisuuden määritykset.**
- [ ] **Osat 5–7: Ratkaise ristisanatehtäviä ja sanahakuja.**
- [ ] **Osat 8–9: Ratkaise tapaustutkimuksia ja salakirjoitushaaste.**
- [ ] **Osa 10: Tarkista perus- ja jatkotason UKK-sivut.**
- [ ] **Osa 11: Tutustu 10 mielenkiintoiseen tosielämän faktaan.**
- [ ] **Bonus: Nopeat vastaukset -haaste.**

Avaa VPN.comin parhaiden VPN-palvelujen opas

URL: https://www.vpn.com/fi/vpn/surfshark/tietoturva/

Oppimispolkusi: Surfsharkin tietoturva

- Analysoi Surfsharkin tietoturvan teknistä arkkitehtuuria ja määräyksiä.
- Määritä asiakasasetukset estämään IP-, DNS- ja WebRTC-liikenteen vuodot.
- Vertaile mukautettua hinnoittelua, kokeilua ja suorituskykyominaisuuksia vakiomalleihin.

SURFSHARKIN TIETOTURVAOPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: pelkästään RAM-muistia käyttävä infrastruktuuri, Nexus SDN ja CleanWeb. Lopuksi bonustehtävä Nopeat vastaukset.

PELKKÄÄ RAM-MUISTIA KÄYTTÄVÄ PALVELINKALUSTO, NEXUS SDN JA CLEANWEB-ARKKITEHTUURI (JOHDANTO)

Surfshark suojaa käyttäjien yksityisyyttä vain RAM-muistissa toimivalla palvelinparkilla, Nexus-ohjelmistopohjaisella verkolla ja IP Rotatorilla, CleanWeb-mainosten estolla sekä Dynamic MultiHop -salausreiteillä.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. **1. Mikä on Surfsharkin integroidun mainos- ja haittaohjelmaneston nimi?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Mitä laitearkkitehtuuria Surfshark käyttää kaikilla palvelimillaan?**
   - A) Kiintolevyt
   - B) 100 % pelkkä RAM
   - C) Optinen tallennus
   - D) Magneettinauha

3. **3. Mikä ominaisuus reitittää liikenteen kahden eri VPN-palvelimen kautta?**
   - A) Ohittaja
   - B) MultiHop (Double VPN)
   - C) Nexus-verkko
   - D) Staattinen IP

4. **4. Mikä häivytysominaisuus naamioi VPN-liikenteen tavalliseksi verkkodataksi?**
   - A) Kill Switch
   - B) Camouflage-tila
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. **5. Mikä on Surfshark Bypasser -työkalun tehtävä?**
   - A) Speed Booster
   - B) Split Tunneling
   - C) Salasanojen hallinta
   - D) DNS-selvittäjä

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Pelkkää RAM-muistia käyttävät palvelimet poistavat kaikki toimintatiedot heti palvelimen uudelleenkäynnistyksessä.

○ Tosi ○ Epätosi

7 Kysymys 7

7. Camouflage Mode estää internetpalveluntarjoajia havaitsemasta, että käytät VPN:ää.

○ Tosi ○ Epätosi

8 Kysymys 8

8. CleanWeb 2.0 toimii selainlaajennuksissa ja estää evästesuostumusikkunat.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Surfshark säilyttää tilapäisiä yhteyksien aikaleimoja ja kaistankäyttölokeja.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Nexus-verkko vaihtaa käyttäjien IP-osoitteita säännöllisesti katkaisematta yhteyttä.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

Lue jokainen alla oleva lause ja täytä aukko oikealla termillä sanapankista.

1. Ärsyttävät verkkomainokset, seurantakomentosarjat ja tietojenkalasteluun johtavat linkit estävät _____ -suodattimet.

2. Käyttäjän toiminnasta ei jää rikosteknistä jälkeä, koska palvelimet käyttävät muistia, jonka tyyppi on _____ .

3. Datan reititys kahden erillisen salatun palvelinhypyn kautta toteutetaan _____ -tunneleilla.

4. VPN-käytön piilottamiseksi internetoperaattoreilta käyttäjät aktivoivat _____ -tilan.

5. Pankkisovellusten ohjaus VPN-tunnelin ohi hoidetaan _____ -asetuksilla.

6. Palvelinkantaa yhdistävä seuraavan sukupolven SDN-arkkitehtuuri on _____ -järjestelmä.

SANASTON SANAPANKKI

BYPASSER CAMOUFLAGE CLEANWEB KILL SWITCH MULTIHOP NEXUS RAM-ONLY VAIHTUVA IP

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: VPN- ja verkkokäsitteiden yhdistäminen

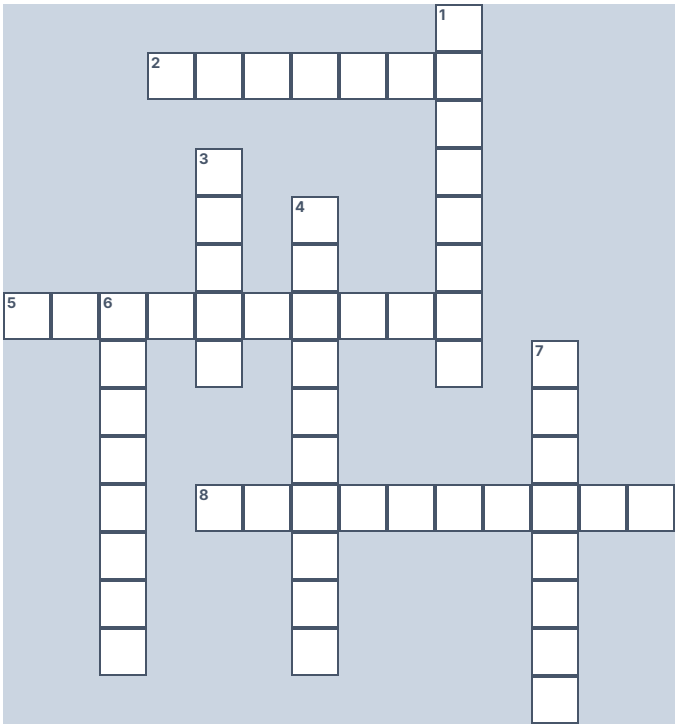
MÄÄRITELMIEN YHDISTÄMINEN

Yhdistä kukin vasemman puolen sanastotermi oikean puolen oikeaan määritelmään kirjoittamalla vastaava kirjain (A–H) täytettävään kenttään.

☐	1. CLEANWEB	A	Automaattinen turvaominaisuus, joka estää verkkoliikenteen VPN:n katketessa.
☐	2. RAM-ONLY	B	Jaetun tunneloinnin toiminto, jonka avulla valitut sovellukset voivat ohittaa VPN:n.
☐	3. MULTIHOP	C	Kehittynyt suodatin, joka estää mainokset, haittaohjelmat ja evästesuostumusbannerit.
☐	4. CAMOUFLAGE	D	Haihtuvaa muistia käyttävät palvelimet, jotka pyyhkivät kaikki tiedot jokaisen virrankatkaisun yhteydessä.
☐	5. OHITTAJA	E	Ominaisuus, joka vaihtaa ulkoisen IP-osoitteesi säännöllisesti katkaisematta tunneleita.
☐	6. KILL SWITCH	F	Hämäysteknologia, joka piilottaa VPN-tunnisteet ja jäljittelee tavallista HTTPS-liikennettä.
☐	7. NEXUS	G	Kaksois-VPN-reititysominaisuus, joka salaa liikenteen kahden eri palvelinsolmun kautta.
☐	8. KIERTÄVÄ	H	Yksityinen ohjelmistopohjainen verkko, joka yhdistää kaikki palvelimet yhtenäiseksi verkoksi.

Tarkistuspiste 5: Ristikko

Ratkaise ristikko kirjoittamalla kirjaimia aktiivisiin valkoisiin ruutuihin. Numerot vastaavat alla olevia vihjeitä.



VAAKASUORAAN

2. Haihtuvaa muistia käyttävä palvelinlaitteisto, joka tyhjentää kaiken datan jokaisen virrankatkaisun yhteydessä (7)

5. Hämäystekniikka, joka piilottaa VPN-tunnisteet ja jäljittelee tavallista HTTPS-liikennettä (10)

8. Ominaisuus, joka vaihtaa ulkoisen IP-osoitteesi säännöllisesti keskeyttämättä tunneleita (10)

PYSTYSUORAAN

1. Jaetun tunneloinnin toiminto, jonka avulla valitut sovellukset ohittavat VPN:n (8)

3. Oma ohjelmistopohjainen verkko, joka yhdistää kaikki palvelimet yhtenäiseksi mesh-verkoksi (5)

4. Automaattinen suojaominaisuus, joka estää verkkoliikenteen VPN-yhteyden pettäessä (10)

6. Kaksois-VPN-reititysominaisuus, joka salaa liikenteen kahden erillisen palvelinsolmun kautta (8)

7. Edistynyt suodatin, joka estää mainokset, haittaohjelmat ja evästeilmoitukset (8)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

Näytönlukijan ja näppäimistön käyttäjät voivat kirjoittaa ristikon vastaukset suoraan alla oleviin tekstikenttiin.

VAAKASUORAAN

2 vaakasuoraan: Haihtuvaa muistia käyttävä palvelinlaitteisto, joka tyhjentää kaiken datan jokaisen virrankatkaisun yhteydessä (7 kirjainta):

5 vaakasuoraan: Hämäystekniikka, joka piilottaa VPN-tunnisteet ja jäljittelee tavallista HTTPS-liikennettä (10 kirjainta):

8 vaakasuoraan: Ominaisuus, joka vaihtaa ulkoisen IP-osoitteesi säännöllisesti keskeyttämättä tunneleita (10 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Jaetun tunneloinnin toiminto, jonka avulla valitut sovellukset ohittavat VPN:n (8 kirjainta):

3 pystysuoraan: Oma ohjelmistopohjainen verkko, joka yhdistää kaikki palvelimet yhtenäiseksi mesh-verkoksi (5 kirjainta):

4 pystysuoraan: Automaattinen suojaominaisuus, joka estää verkkoliikenteen VPN-yhteyden pettäessä (10 kirjainta):

6 pystysuoraan: Kaksois-VPN-reititysominaisuus, joka salaa liikenteen kahden erillisen palvelinsolmun kautta (8 kirjainta):

7 pystysuoraan: Edistynyt suodatin, joka estää mainokset, haittaohjelmat ja evästeilmoitukset (8 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

Etsi ruudukosta 8 piilotettua keskeistä sanastotermiä. Sanat voivat olla vaaka-, pysty- tai vinosuunnassa.

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

SANASTOLISTA

CLEANWEB, RAMONLY, MULTIHOP, NEXUS, CAMOUFLAGE, VAIHTUVAIP, BYPASSER, KILLSWITCH

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

Yhdistä kukin sanahaun 8 sanastotermistä sen oikeaan määritelmään kirjoittamalla kirjain (A–H) tyhjään kohtaan.

SANASTOTERMIT

- **A. CLEANWEB**
- **B. RAMONLY**
- **C. MULTIHOP**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. VAIHTUVAIP**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Hämäystekniikka, joka piilottaa VPN-tunnisteet ja jäljittelee tavallista HTTPS-liikennettä.
2. Automaattinen suojaominaisuus, joka estää verkkoliikenteen VPN-yhteyden pettäessä.
3. Edistynyt suodatin, joka estää mainokset, haittaohjelmat ja evästeilmoitukset.
4. Jaetun tunneloinnin toiminto, jonka avulla valitut sovellukset ohittavat VPN:n.
5. Haihtuvaa muistia käyttävä palvelinlaitteisto, joka tyhjentää kaiken datan jokaisen virrankatkaisun yhteydessä.
6. Ominaisuus, joka vaihtaa ulkoisen IP-osoitteesi säännöllisesti keskeyttämättä tunneleita.
7. Kaksois-VPN-reititysominaisuus, joka salaa liikenteen kahden erillisen palvelinsolmun kautta.
8. Oma ohjelmistopohjainen verkko, joka yhdistää kaikki palvelimet yhtenäiseksi mesh-verkoksi.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä virtuaalisen yksityisverkon (VPN) käsitteitä ja termejä. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. **EANCWLBE**
2. **TMPUOHIL**
3. **AYBSSREP**
4. **XSUNE**
5. **NYOMRLA**
6. **GUOLACAFEM**
7. **ILKIWTCHSL**
8. **IHUPVTAVAI**

Bonustehtävä: Nopeat vastaukset

3 VASTAUSTA JOKAISEEN LUOKKAAN. VOITTAJA ON SE, JOKA TÄYTTÄÄ LISTAN ENSIMMÄISENÄ.

1	Palvelun Surfshark tietoturvaominaisuuksia			
2	Merkkejä siitä, että VPN-yhteytesi on hidas			
3	VPN-protokollia, jotka tunnet			
4	Asioita, joita salaus suojaa			
5	Julkisen Wi-Fin uhkia			
6	Maita, jotka tunnetaan vahvoista tietosuojalaeistaan			
7	Tapoja tehdä vahva salasana			
8	Laitteita, joihin asentaisit palvelun Surfshark			
9	Kysymyksiä palvelun Surfshark asiakastuelle			
10	Asetuksia, jotka otat käyttöön lisäturvaksi			
11	Asioita, jotka Surfshark voi piilottaa verkostasi			
12	VPN-vuotojen tyyppejä			
13	Tietoja, joita VPN:n ei pitäisi koskaan tallentaa			
14	Sanoja, jotka kuvaavat hyvää VPN-sovellusta			
15	Asioita, joita tarkastus voi tutkia			

Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: KAMPUKSEN JA TYÖPAIKAN SUODATTIMIEN OHITTAMINEN

👷

Tilanne: Opiskelija huomaa, että hänen yliopistokampuksensa Wi-Fi estää kaikki tavalliset OpenVPN- ja WireGuard-portit.

Keskustelukysymys: Mikä Surfsharkin ominaisuus antaa opiskelijan yhdistää verkon ylläpitäjien huomaamatta?

TAPAUSTUTKIMUS 2: KORKEAN RISKIN TOIMITTAJAN TUTKINTA

👷

Tilanne: Tutkiva toimittaja tarvitsee lisäsuojaa valvontaa vastaan tutkiessaan arkaluonteisia yritystietueita.

Keskustelukysymys: Miten Dynamic MultiHop tarjoaa paremman yksityisyyden kuin yhden palvelimen reititys?

Tarkistuspiste 9: Salakirjoituksen purkaminen

Verkkoinsinööri suojaa reititysreittejä ja asiakastunneleita. Käytä alla olevaa kirjain–numero-avainta purkaaksesi viestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

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

14	5	24	21	19		10	1		22	1	9	8	20	21	22	1		9	16

19	21	15	10	1	1	22	1	20

25	11	19	9	20	25	9	19	25	25	20	20	28

Purettu viesti:

VIHJE: JOKAINEN NUMERO VASTAA KIRJAIMEN PAIKKAA AAKKOSISSA (ESIM. 1 = A, 2 = B, 29 = Ö).

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, perustaso (Osa A)

Tutustu yleisimpiin kysymyksiin ja vastauksiin virtuaalisista yksityisverkoista (VPN) ja tunneloinnista.

Q1: Mikä on Surfshark CleanWeb?

CleanWeb on integroitu tietoturvaominaisuus, joka estää mainokset, seurantaohjelmat, haittaohjelmat ja tietojenkalastelusivustot.

Q2: Mitä ovat pelkkää RAM-muistia käyttävät palvelimet?

Pelkkää RAM-muistia käyttävät palvelimet toimivat haihtuvalla muistilla, eli muistissa olevat tiedot tyhjenevät aina, kun palvelimet käynnistyvät uudelleen.

Q3: Mikä on Surfshark MultiHop?

MultiHop (Double VPN) reitittää ja salaa internet-yhteytesi kahden eri palvelinsijainnin kautta.

Q4: Miten Camouflage Mode toimii?

Camouflage Mode hämää VPN-liikenteen, jotta internetpalveluntarjoajasi ei näe, että käytät VPN:ää.

Q5: Mikä on Bypasser-ominaisuus?

Bypasser on Surfsharkin split tunneling -työkalu, jonka avulla tietyt sovellukset tai verkkosivustot voivat ohittaa VPN:n.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, perustaso (Osa B)

Tutustu yleisimpiin kysymyksiin ja vastauksiin virtuaalisista yksityisverkoista (VPN) ja tunneloinnista.

Q6: Onko Surfsharkissa Kill Switch?

Kyllä, Kill Switch katkaisee internetyhteytesi, jos VPN katkeaa odottamatta.

Q7: Mitä salausstandardia Surfshark käyttää?

Surfshark käyttää AES-256-GCM:ää ja ChaCha20:tä sekä AEGIS-256X2:ta uudessa Dausos-protokollassaan.

Q8: Onko Surfsharkin lokittomuuskäytäntö tarkastettu?

Kyllä, Deloitte varmensi Surfsharkin no-logs-käytännön vuonna 2023 ja uudelleen vuonna 2025.

Q9: Mikä on Surfshark Nexus?

Nexus on kehittynyt SDN-arkkitehtuuri, joka yhdistää kaikki palvelimet yhtenäiseksi verkoksi sujuvampaa reititystä varten.

Q10: Mikä on IP Rotator -ominaisuus?

IP-kierrättäjä vaihtaa IP-osoitteesi automaattisesti muutaman minuutin välein katkaisematta VPN-istuntoasi.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, jatkotaso (Osa C)

Tutustu VPN-tunnelointiprotokollien, mobiiliasiakasohjelmien integraatioiden ja yrityskäyttöönoton edistyneisiin teknisiin puoliin.

Q1: Miten Dynamic MultiHop eroaa perinteisestä kaksois-VPN:stä?

Dynamic MultiHop antaa sinun mukauttaa mitä tahansa sisääntulo- ja ulostulopalvelinten yhdistelmää maailmanlaajuisesti.

Q2: Toimiiko CleanWeb 2.0 selainlaajennuksissa?

Kyllä, CleanWeb 2.0 estää videomainokset, evästesuostumusikkunat ja ilmoitusbannerit Chromessa ja Firefoxissa.

Q3: Mitä Alternative ID tietoturvapaketissa on?

Alternative ID luo yksilöllisiä henkilökohtaisia nimimerkkejä, sähköpostiosoitteita ja puhelinnumeropeitteitä.

Q4: Miten Surfshark estää DNS-vuodot?

Surfshark reitittää kaikki verkkotunnuspyynnöt omien yksityisten DNS-palvelimiensa kautta jokaisessa solmussa.

Q5: Tukeeko Surfshark ChaCha20-salausta mobiilissa?

Kyllä, WireGuard käyttää Androidilla ja iOS:llä ChaCha20-Poly1305:tä erinomaisen mobiilitehokkuuden saavuttamiseksi.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, jatkotaso (Osa D)

Tutustu VPN-tunnelointiprotokollien, mobiiliasiakasohjelmien integraatioiden ja yrityskäyttöönoton edistyneisiin teknisiin puoliin.

Q6: Mikä on NoBorders-tila Surfsharkissa?

NoBorders tunnistaa automaattisesti rajoittavat verkkoympäristöt ja tarjoaa erikoistuneita palvelimia.

Q7: Kuka suoritti Surfsharkin selainlaajennusten tietoturvatarkastukset?

Riippumaton kyberturvallisuusyritys Cure53 suoritti auditoinnit selainlaajennuksille ja palvelinjärjestelmille.

Q8: Miten Surfshark suojaa IPv6-vuodoilta?

Surfshark reitittää IPv6-liikenteen turvallisesti tai rajoittaa sen turvallisesti salaamattoman vuodon estämiseksi.

Q9: Missä Surfsharkin oikeudellinen lainkäyttöalue sijaitsee?

Surfshark toimii Alankomaiden lain alaisuudessa ja noudattaa tiukkoja eurooppalaisia GDPR-tietosuojastandardeja.

Q10: Tukeeko Surfshark kaksivaiheista tunnistautumista (2FA)?

Kyllä, ja Surfshark One lisää 2FA-lukituksen, jotta vain sinä voit muuttaa ominaisuusasetuksia.

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

Tutustu todellisiin tosiasioihin VPN-salauksen nopeuksista, protokollien auditoinneista, mobiiliyhteyksistä ja yritysten etätyöstä.

1. VPN-OIVALLUS

1. Surfshark kertoo, että sen koko yli 4 500 palvelimen verkko toimii levyttömällä, haihtuvalla RAM-laitteistolla.

2. VPN-OIVALLUS

2. Neljän suuren tilintarkastusyhtiö Deloitte varmensi Surfsharkin lokittomuuskäytännön vuonna 2023 ja uudelleen marraskuussa 2025.

3. VPN-OIVALLUS

3. Oma Nexus-arkkitehtuuri yhdistää kaikki maailmanlaajuiset palvelimet dynaamiseksi ohjelmistopohjaiseksi verkoksi.

4. VPN-OIVALLUS

4. Rotating IP vaihtaa IP-osoitteesi noin viiden minuutin välein katkaisematta VPN-yhteyttä.

5. VPN-OIVALLUS

5. CleanWeb 2.0 estää tungettelevat evästeilmoitukset ja videomainokset suoraan selaimissa.

6. VPN-OIVALLUS

6. Dynamic MultiHop sallii käyttäjien luoda mukautettuja kahden palvelimen salausreittejä 100 maan kesken.

7. VPN-TIETOA

7. Naamiointitila poistaa VPN-otsikkotunnisteet, jolloin liikennettä ei voi erottaa tavallisesta HTTPS-liikenteestä.

8. VPN-TIETOA

8. Alternative ID luo kertakäyttöisiä nimimerkkejä ja sähköpostinaamioita, jotka suojaavat käyttäjiä tietovuodoilta.

9. VPN-TIETOA

9. Surfshark käyttää AES-256-GCM-symmetristä salausta ChaCha20:n rinnalla WireGuard-protokollissa.

10. VPN-OIVALLUS

10. NoBorders-tila aktivoituu automaattisesti rajoitetuissa verkoissa ja tarjoaa joustavan tunnelointiyhteyden.

Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista teknisistä standardeista, määrittelyistä ja sääntelykehyksistä.

TIETEELLISET JA ALAN VIITTEET

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Integroitu sisällönesto** MAINOSTEN JA HAITTAOHJELMIEN TORJUNTA — Oikea vastaus: B

OPETTAJALLE

CleanWeb on Surfsharkin integroitu tietoturvasuodatin, joka estää mainokset, seurantaverkkotunnukset, tietojenkalasteluverkkosivustot ja haitalliset URL-komentosarjat verkkotasolla. Lähde: CleanWeb Security Specs.

2 **100 % RAM-pohjainen infrastruktuuri** RAM-ARKKITEHTUURI — Oikea vastaus: B

OPETTAJALLE

Surfshark käyttää vain RAM-muistissa toimivia palvelimia, joten palvelimen muistissa oleva data tyhjenee, kun palvelin sammutetaan tai käynnistetään uudelleen. Lähde: Cure53 Infrastructure Audit.

3 **MultiHop-kaksoistunnelointi** MULTIHOP-VPN — Oikea vastaus: B

OPETTAJALLE

MultiHop (Double VPN) salaa liikenteen kahden eri maassa sijaitsevan palvelinsolmun kautta liikenteen korrelaatiohyökkäysten estämiseksi. Lähde: Surfshark MultiHop Guide.

4 **Camouflage Mode -tilan hämäys** PEITTELY — Oikea vastaus: B

OPETTAJALLE

Camouflage Mode muokkaa OpenVPN-pakettien otsikoita niin, että VPN-liikenne näyttää tavalliselta HTTPS-liikenteeltä ja ohittaa rajoittavat palomuuriestot. Lähde: Surfshark Stealth Whitepaper.

5 **Split Tunneling Bypasser** JAETTU TUNNELOINTI — Oikea vastaus: B

OPETTAJALLE

Bypasser on Surfsharkin split tunneling -työkalu, jonka avulla käyttäjät voivat valita tietyt sovellukset tai verkkosivustot, jotka reititetään suoraan tavallisen internetyhteyden tarjoajan yhteyden kautta. Lähde: Surfshark Client Features.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Katoavan muistin tietojen pyyhintä** — PALVELINTURVA — Oikea vastaus: Tosi

OPETTAJALLE

Pelkkää RAM-muistia käyttävät palvelimet eivät tallenna dataa pysyville kiintolevyille; laitteiston uudelleenkäynnistys tyhjentää heti koko toimintamuistin. Lähde: RAM Server Architecture.

7 **Camouflage Mode -tilan palveluntarjoajan peittäminen** — LIIKENTEEN PIILOTTAMINEN — Oikea vastaus: Tosi

OPETTAJALLE

Camouflage Mode poistaa OpenVPN-protokollan tunnisteet, jolloin internetpalveluntarjoajat eivät voi havaita, että käyttäjä on yhteydessä VPN-tunneliin. Lähde: Deep Packet Inspection Guide.

8 **CleanWeb 2.0 -selainlaajennukset** — SELAINLAAJENNUS — Oikea vastaus: Tosi

OPETTAJALLE

CleanWeb 2.0 toimii selainlaajennuksissa ja estää evästesuostumusikkunat, videomainokset ja haitalliset uudelleenohjauskomentosarjat reaaliajassa. Lähde: CleanWeb 2.0 Release Notes.

9 **YHTEYSLOKIEN NOLLASÄILYTYS** — LOKITON KÄYTÄNTÖ — Oikea vastaus: Epätosi

OPETTAJALLE

Surfshark noudattaa tiukkaa, itsenäisesti tarkastettua lokittomuuskäytäntöä, eikä tallenna IP-osoitteita, yhteyksien aikaleimoja tai kaistankäyttölokeja. Lähde: Deloitte No-Logs Audit.

10 **Nexus-IP:n dynaaminen kierrätys** — NEXUS-VERKKO — Oikea vastaus: Tosi

OPETTAJALLE

Surfsharkin Nexus-ohjelmistopohjainen verkko vaihtaa käyttäjien IP-osoitteita dynaamisesti muutaman minuutin välein katkaisematta aktiivista VPN-yhteyttä. Lähde: Surfshark Nexus Architecture.

Sanastoavaimet ja arviointikriteerit

Opettajan arviointikriteeri: Anna 1 piste jokaisesta oikeasta yhdistämisestä (yhteensä 8 pistettä) ja asiayhteystermistä (yhteensä 6 pistettä).

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

C 1. CLEANWEB	D 2. RAM-ONLY	G 3. MULTIHOP	F 4. CAMOUFLAGE
B 5. OHITTAJA	A 6. KILL SWITCH	H 7. NEXUS	E 8. KIERTÄVÄ

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 CLEANWEB	2 RAM-ONLY	3 MULTIHOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – RAMONLY	6 H – VAIHTUVAIP	7 C – MULTIHOP	8 G – NEXUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit CLEANWEB, RAM-ONLY ja MULTIHOP omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

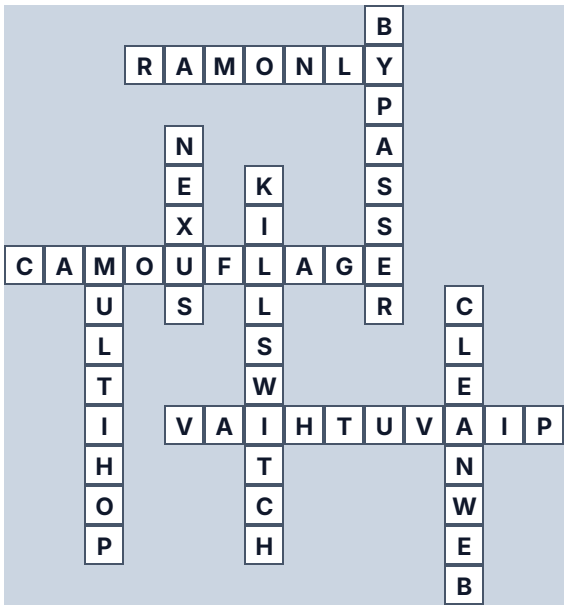
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: RAMONLY Haihtuvaa muistia käyttävä palvelinlaitteisto, joka tyhjentää kaiken datan jokaisen virrankatkaisun yhteydessä (7 kirjainta)

5 vaakasuoraan: CAMOUFLAGE Hämäystekniikka, joka piilottaa VPN-tunnisteet ja jäljittelee tavallista HTTPS-liikennettä (10 kirjainta)

8 vaakasuoraan: VAIHTUVAIP Ominaisuus, joka vaihtaa ulkoisen IP-osoitteesi säännöllisesti keskeyttämättä tunneleita (10 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: BYPASSER Jaetun tunneloinnin toiminto, jonka avulla valitut sovellukset ohittavat VPN:n (8 kirjainta)

3 pystysuoraan: NEXUS Oma ohjelmistopohjainen verkko, joka yhdistää kaikki palvelimet yhtenäiseksi mesh-verkoksi (5 kirjainta)

4 pystysuoraan: KILLSWITCH Automaattinen suojaominaisuus, joka estää verkkoliikenteen VPN-yhteyden pettäessä (10 kirjainta)

6 pystysuoraan: MULTIHOP Kaksois-VPN-reititysominaisuus, joka salaa liikenteen kahden erillisen palvelinsolmun kautta (8 kirjainta)

7 pystysuoraan: CLEANWEB Edistynyt suodatin, joka estää mainokset, haittaohjelmat ja evästeilmoitukset (8 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. N Y O M R L A — **RAMONLY**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. I H U P V T A V A I — **VAIHTUVAIP**

SALAKIRJOITUSHAASTEEN AVAIN

"NEXUS JA VAIHTUVA IP SUOJAAVAT YKSITYISYYTTÄ"

Tapaustutkimusten vastausavain

A TAPAUSTUTKIMUS 1: KAMPUKSEN JA TYÖPAIKAN SUODATTIMIEN OHITTAMINEN

Opettajan ratkaisu

ARVIOINTIKRITEERIT JA RATKAISUOHJEET

- Tilanneanalyysi: Opiskelija huomaa, että hänen yliopistokampuksensa Wi-Fi estää kaikki tavalliset OpenVPN- ja WireGuard-portit.
- Pohdintakysymys: Mikä Surfshark-ominaisuus antaa opiskelijan yhdistää niin, etteivät verkonvalvojat havaitse sitä?
- Suositeltu strategia ja ratkaisu: Ota käyttöön Camouflage Mode (OpenVPN), joka piilottaa VPN:n metatiedot, jotta palomuurit näkevät tavallista HTTPS-selailua.

B TAPAUSTUTKIMUS 2: KORKEAN RISKIN TOIMITTAJAN TUTKINTA

Opettajan ratkaisu

ARVIOINTIKRITEERIT JA RATKAISUOHJEET

- Tilanneanalyysi: Tutkiva toimittaja tarvitsee lisäsuojaa valvontaa vastaan tutkiessaan arkaluonteisia yritysasiakirjoja.
- Pohdintakysymys: Miten Dynamic MultiHop tarjoaa paremman yksityisyyden kuin yhden palvelimen kautta reititys?
- Suositeltu strategia ja ratkaisu: Dynaaminen MultiHop reitittää liikenteen kahdessa maassa sijaitsevien sisääntulo- ja poistumispalvelimien kautta, joten mikään yksittäinen palvelin ei voi paljastaa käyttäjää.