Nimi: _____ Päivämäärä: _____ Pisteet: _____

# Mullvadin turvallisuus

Mullvad VPN:n tietoturva-arkkitehtuurin analysointi, mukaan lukien levyttömät vain RAM-muistia käyttävät palvelimet, auditoidut lokittomuuskäytännöt, paikallinen avainten luonti, WireGuard-salaus ja kvanttiturvalliset tunnelimääritykset.

## MULLVADIN TURVALLISUUDEN OPPIMISKATSAUS

**OPPIJA**
**OPISKELIJASTATUS**
Verkon puolustajan polku

**TURVALLINEN**
**YHTEYDEN TILA**
Datapakettien suojaaminen

**AKTIIVINEN**
**VUOTOSUOJA**
DNS- ja IPv6-vuodonesto

**Tervetuloa!** Tämä tehtäväpaketti käsittelee aihetta: Mullvadin tietoturva-arkkitehtuuri. Tutustut levyttömiin vain RAM-muistia käyttäviin palvelimiin, auditoituihin zero-logs-käytäntöihin, paikalliseen avainten luontiin ja kvanttiturvallisiin tunneleihin.

**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/mullvad/tietoturva/

# Oppimispolkusi: Mullvadin tietoturva

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

### MULLVADIN TURVALLISUUSOPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: Mullvadin yksityisyyttä painottavat palvelinhallinnat. Lopuksi bonustehtävä Nopeat vastaukset.

### NIMETTÖMYYTTÄ ENSISIJAISTAVAN INFRASTRUKTUURIN JA RAM-TASOJEN ARVIOINTI (JOHDANTO)

Mullvad ei käytä tavallisia salasanalla suojattuja tilejä vaan satunnaisesti luotuja 16-numeroisia koodeja. Sen infrastruktuuri on rakennettu levyttömistä, pelkkää RAM-muistia käyttävistä solmuista, paikallisesti luoduista WireGuard-avaimista ja auditoiduista tietoja säilyttämättömyyden käytännöistä.

**LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.**

# Tarkistuspiste 1: Monivalintahaaste

1. **1. Mikä tunnelointiprotokolla on oletuksena Mullvadin sovelluksessa?**
   - A) OpenVPN
   - B) WireGuard
   - C) IKEv2
   - D) PPTP

2. **2. Mitä Mullvad vaatii uuden tilin luomiseen?**
   - A) Ei mitään
   - B) Sähköpostiosoite
   - C) Puhelinnumero
   - D) Henkilöllisyysasiakirja

3. **3. Mikä kryptografinen tunneli suojaa kvanttitietokoneilta?**
   - A) AES-256-GCM
   - B) Kvantti-WireGuard
   - C) RSA-4096
   - D) SOCKS5-välityspalvelin

4. **4. Mikä turvamekanismi estää WebRTC-vuotovaarat?**
   - A) Selainlaajennus
   - B) Verkon Kill Switch
   - C) WebRTC:n reitittäminen VPN-liitännän kautta
   - D) Split tunneling

5. **5. Mikä multihop-ominaisuus reitittää liikenteen usean solmun kautta?**
   - A) Kaksois-NAT
   - B) WireGuard Multihop
   - C) Chameleon-protokolla
   - D) Bypasser

## Tarkistuspiste 2: Tosi vai epätosi -haaste

### 6 Kysymys 6

6. Mullvad vaatii sähköpostiosoitteen tilin luonnin yhteydessä.

○ Tosi ○ Epätosi

### 7 Kysymys 7

7. SOCKS5-välityspalvelimia voi määrittää Mullvad-tunneleiden sisälle.

○ Tosi ○ Epätosi

### 8 Kysymys 8

8. Mullvad omistaa ja ylläpitää kaikkea palvelinlaitteistoaan.

○ Tosi ○ Epätosi

### 9 Kysymys 9

9. Network Kill Switch on oletuksena aina käytössä.

○ Tosi ○ Epätosi

### 10 Kysymys 10

10. Postitse lähetetyt käteismaksut eivät ole lainkaan palautettavissa.

○ Tosi ○ Epätosi

# Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Mullvad käyttää ensisijaisena nopeana suojattuna tunnelointiprotokollanaan _____ .

2. Tietojen reititystä kahden palvelinsijainnin kautta kutsutaan nimellä _____ .

3. Levylle tallentuvien lokien estämiseksi Mullvad käyttää erillisiä _____ -solmuja.

4. Järjestelmän liikenne estetään tunnelin pettäessä sisäänrakennetulla _____ -varamekanismilla.

5. Tarkastuslausunnot vahvistavat, että Mullvadin käyttämä todennettu ja tiukka periaate on _____ .

6. Sovellusten sisäinen reititys voidaan eristää mukautetulla _____ -määrityksellä.

7. Post-kvanttisalausalgoritmit suojaavat tietoja tunnelissa, joka on _____ .

8. Yksityisiä nimipalvelimia otetaan käyttöön maailmanlaajuisesti vaarallisten uhkien estämiseksi, joita ovat esimerkiksi _____ .

**SANASTON SANAPANKKI**

DNS-VUODOT KILL SWITCH KVANTTIKESTÄVÄ LOKITTOMUUS MULTIHOP RAM-ONLY SOCKS5 WIREGUARD

**Kirjoita vastauksesi tähän:**

1. 2.

3. 4.

5. 6.

7. 8.

# Tarkistuspiste 4: VPN- ja verkkokäsitteiden yhdistäminen

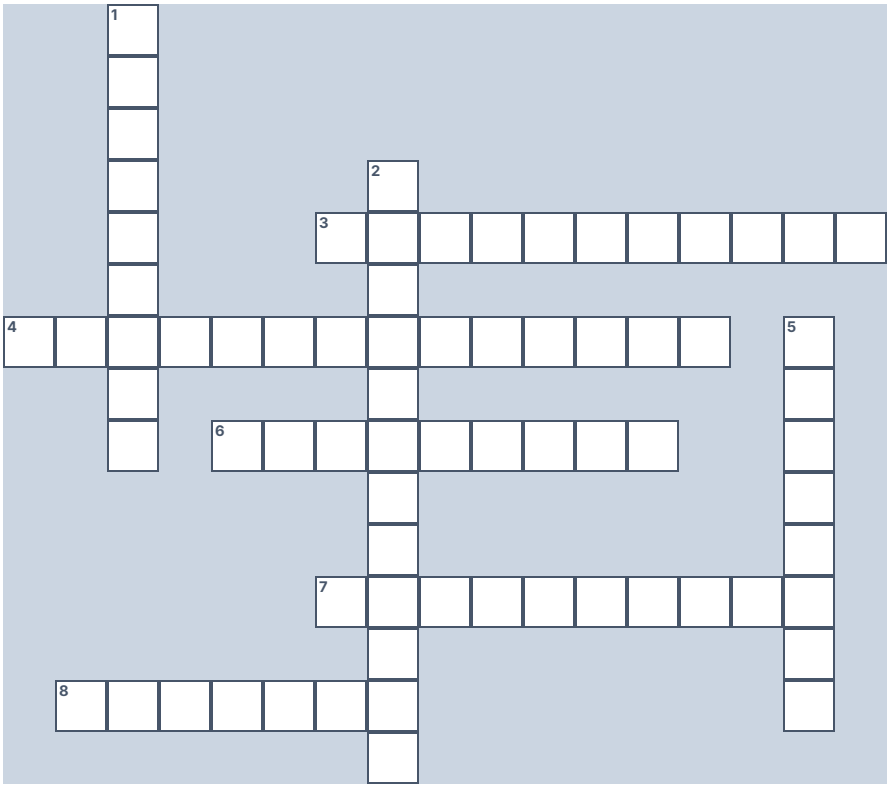
## MÄÄRITELMIEN YHDISTÄMINEN

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

| | | | |
|---|---|---|---|
| ☐ | 1. WIREGUARD | A | Turvaominaisuus, joka katkaisee liikenteen, kun VPN katkeaa. |
| ☐ | 2. MULTIHOP | B | Kevyt ja tehokas suojattu tunnelointiprotokolla. |
| ☐ | 3. VAIN RAM | C | Sisäinen välityspalvelinprotokolla, jota käytetään asiakassovellusten eristämiseen. |
| ☐ | 4. KILL SWITCH | D | Liikenteen reititys sisääntulo- ja ulostulopalvelinsolmun kautta. |
| ☐ | 5. LOKITTOMUUS | E | Salausmekanismit, jotka on suunniteltu kestämään kvanttihyökkäyksiä. |
| ☐ | 6. SOCKS-VÄLITYS | F | DNS-kyselyjen kohteiden paljastuminen VPN-tunnelin ulkopuolella. |
| ☐ | 7. KVANTTIKESTÄVÄ | G | Haihtuvaa muistia käyttävät palvelimet, jotka eivät säilytä tietoja uudelleenkäynnistyksen jälkeen. |
| ☐ | 8. DNS-VUODOT | H | Nollasäilytyksen tietostandardi, jonka riippumattomat auditoinnit ovat varmentaneet. |

# Tarkistuspiste 5: Ristikko

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




## VAAKASUORAAN

**3. Riippumattomien tarkastusten todentama nollasäilytysstandardi (11)**

**4. Salausmekanismit, jotka on suunniteltu kestämään kvanttihyökkäyksiä (14)**

**6. DNS-kyselyjen kohteiden paljastuminen VPN-tunnelin ulkopuolella (9)**

**7. Suojaominaisuus, joka katkaisee liikenteen VPN-yhteyden pettäessä (10)**

**8. Haihtuvaa muistia käyttävä palvelinlaitteisto, joka ei säilytä dataa uudelleenkäynnistyksen jälkeen (7)**

## PYSTYSUORAAN

**1. Kevyt ja tehokas suojattu tunnelointiprotokolla (9)**

**2. Sisäinen välityspalvelinprotokolla, jota käytetään asiakassovellusten eristämiseen (12)**

**5. Liikenteen reititys sisääntulo- ja poistumispalvelinsolmun kautta (8)**

# Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

## VAAKASUORAAN

**3 vaakasuoraan: Riippumattomien tarkastusten todentama nollasäilytysstandardi (11 kirjainta):**

**4 vaakasuoraan: Salausmekanismit, jotka on suunniteltu kestämään kvanttihyökkäyksiä (14 kirjainta):**

**6 vaakasuoraan: DNS-kyselyjen kohteiden paljastuminen VPN-tunnelin ulkopuolella (9 kirjainta):**

**7 vaakasuoraan: Suojaominaisuus, joka katkaisee liikenteen VPN-yhteyden pettäessä (10 kirjainta):**

**8 vaakasuoraan: Haihtuvaa muistia käyttävä palvelinlaitteisto, joka ei säilytä dataa uudelleenkäynnistyksen jälkeen (7 kirjainta):**

## PYSTYSUORAAN

**1 pystysuoraan: Kevyt ja tehokas suojattu tunnelointiprotokolla (9 kirjainta):**

**2 pystysuoraan: Sisäinen välityspalvelinprotokolla, jota käytetään asiakassovellusten eristämiseen (12 kirjainta):**

**5 pystysuoraan: Liikenteen reititys sisääntulo- ja poistumispalvelinsolmun kautta (8 kirjainta):**

## Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

**SANASTOLISTA**

WIREGUARD MULTIHOP RAMONLY KILLSWITCH LOKITTOMUUS
SOCKSVÄLITYS KVANTTIKESTÄVÄ DNSVUODOT

# Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

**SANASTOTERMIT**

- **A. WIREGUARD**
- **B. MULTIHOP**
- **C. RAMONLY**
- **D. KILLSWITCH**
- **E. LOKITTOMUUS**
- **F. SOCKSVÄLITYS**
- **G. KVANTTIKESTÄVÄ**
- **H. DNSVUODOT**

**MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT**

1. Sisäinen välityspalvelinprotokolla, jota käytetään asiakassovellusten eristämiseen.
2. Salausmekanismit, jotka on suunniteltu kestämään kvanttihyökkäyksiä.
3. Kevyt ja tehokas suojattu tunnelointiprotokolla.
4. Haihtuvaa muistia käyttävä palvelinlaitteisto, joka ei säilytä dataa uudelleenkäynnistyksen jälkeen.
5. Suojaominaisuus, joka katkaisee liikenteen VPN-yhteyden pettäessä.
6. Liikenteen reititys sisääntulo- ja poistumispalvelinsolmun kautta.
7. DNS-kyselyjen kohteiden paljastuminen VPN-tunnelin ulkopuolella.
8. Riippumattomien tarkastusten todentama nollasäilytysstandardi.

## Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. UGEIWARDR
2. RMYLNOA
3. LOTMKOUSTUI
4. VIVSNETÄKÄTKAT
5. IHUPTMOL
6. CSLITKIWHL
7. LISSOÄSTYCVK
8. TUODVNODS

# Bonustehtävä: Nopeat vastaukset

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

| | | | | |
|---|---|---|---|---|
| 1 | Palvelun Mullvad tietoturvaominaisuuksia | | | |
| 2 | Kysymyksiä palvelun Mullvad asiakastuelle | | | |
| 3 | Tapoja tehdä vahva salasana | | | |
| 4 | Ihmisiä, joille suosittelisit palvelua Mullvad | | | |
| 5 | Asioita, joita tarkastus voi tutkia | | | |
| 6 | Maita, jotka tunnetaan vahvoista tietosuojalaeistaan | | | |
| 7 | Asioita, joita teet verkossa joka päivä | | | |
| 8 | Maita, joissa haluaisit palvelun Mullvad palvelimia | | | |
| 9 | Asetuksia, jotka otat käyttöön lisäturvaksi | | | |
| 10 | Asioita, joita salaus suojaa | | | |
| 11 | VPN-vuotojen tyyppejä | | | |
| 12 | Tietoturvasanoja, jotka opit tässä tehtävämonisteessa | | | |
| 13 | Julkisen Wi-Fin uhkia | | | |
| 14 | Sovelluksia, joita käyttäisit yhdessä palvelun Mullvad kanssa | | | |
| 15 | Laitteita, joihin asentaisit palvelun Mullvad | | | |

# Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

### TAPAUSTUTKIMUS 1: KVANTTIKESTÄVYYDEN INTEGROINTI

👷

**Tilanne:** Rahoitusyhtiön on suojattava tiedostonsiirrot tulevaa kvanttipurkua vastaan.

**Keskustelukysymys:** Mitä tunnelimääritystä heidän tulisi käyttää Mullvadin sovelluksessa?

### TAPAUSTUTKIMUS 2: SALAINEN TUTKIVA REITITYS

👷

**Tilanne:** Tutkija haluaa kaksoisreitittää verkkonsa peittääkseen sisääntulopisteensä.

**Keskustelukysymys:** Mikä Mullvadin ominaisuus tulisi ottaa käyttöön usean palvelimen kautta tapahtuvan reitityksen saavuttamiseksi?

# 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**

| 13 | 21 | 12 | 12 | 22 | 1 | 4 | | 20 | 9 | 12 | 9 | | 5 | 9 | | 22 | 1 | 1 | 4 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | |

| 19 | 1 | 12 | 1 | 19 | 1 | 14 | 1 | 1 | | 20 | 1 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | |

| 19 | 28 | 8 | 11 | 29 | 16 | 15 | 19 | 20 | 9 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

**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: Miten Mullvad suojaa tilit?

Mullvad käyttää luotua 16-numeroista tilinumeroa, eikä salasanaa tai sähköpostia tarvita. [1]

### Q2: Mitä protokollaa Mullvad priorisoi?

Mullvad asettaa WireGuardin etusijalle sen nopeuden, yksinkertaisuuden ja modernin salaustekniikan vuoksi. [9]

### Q3: Tarkastetaanko Mullvadin palvelimet?

Kyllä, kolmannen osapuolen tietoturvayritykset tekevät säännöllisiä infrastruktuuri- ja koodiauditointeja.

### Q4: Tukeeko Mullvad OpenVPN:ää?

Ei, Mullvad poisti OpenVPN:n 15. tammikuuta 2026; se on vain WireGuard. [7]

### Q5: Mikä on Mullvadin kill switch?

Se on integroitu palomuurisääntö, joka estää internetliikenteen, jos VPN epäonnistuu.

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

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

### Q6: Tukeeko Mullvad IPv6:ta?

Kyllä, Mullvad tukee natiivia IPv6-reititystä ja vuotosuojausta.

### Q7: Tarjoaako Mullvad multihopin?

Kyllä, WireGuard multihop mahdollistaa useiden palvelinsijaintien ketjuttamisen.

### Q8: Voinko käyttää mukautettuja DNS-resolvereita?

Kyllä, mukautetut DNS-osoitteet voi määrittää Mullvad-sovelluksen asetuksissa.

### Q9: Miten lokien tallentaminen estetään?

Järjestelmäasetukset poistavat lokituksen käytöstä ja tyhjentävät välimuistit kaikista palvelimen taustaprosesseista.

### Q10: Missä Mullvad on yhtiöitetty?

Mullvad on rekisteröity Göteborgissa Ruotsissa Ruotsin lainkäyttöalueelle.

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

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

### Q1: Miten avainten kierrätys toimii?

Sovellus vaihtaa WireGuard-avaimet automaattisesti; komentorivin oletusväli on 30 päivää. [3]

### Q2: Mitä ovat kvanttiturvalliset tunnelit?

Ne lisäävät WireGuardiin ML-KEM- ja Classic McEliece -avaimenvaihdon tulevien kvanttihyökkäysten torjumiseksi. [2]

### Q3: Miten pelkkää RAM-muistia käyttävät solmut ovat turvallisia?

Nämä solmut eivät kirjoita dataa kiintolevyille, joten fyysisten palvelinten varastaminen on hyödytöntä.

### Q4: Mikä on SOCKS5-välityspalvelimen tehtävä?

Se auttaa reitittämään tiettyjen sovellusten liikennettä tunnelin sisällä ja estää vuodot ulkoisiin verkkoihin.

### Q5: Suojaako Mullvad WebRTC-vuodoilta?

Kyllä, sovellus pakottaa WebRTC-kyselyt kulkemaan VPN-liitännän kautta paikallisten IP-osoitteiden suojaamiseksi.

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

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

### Q6: Miten Mullvad toimii poliisin ratsioissa?

Mullvad ei pidä käyttäjätietokannan lokeja, joten käyttäjätietoja ei voi poimia.

### Q7: Mikä on Ruotsin lainkäyttöalueen riski?

Ruotsi on 14 Eyes -jäsen, mutta Mullvadin lokiton arkkitehtuuri poistaa tietoriskin.

### Q8: Onko asiakassovellusten tarkastukset avointa lähdekoodia?

Kyllä, sovellukset ovat avoimen lähdekoodin (GPL-3) ja yritykset, kuten X41 D-Sec, ovat auditoineet ne. [6]

### Q9: Miten jaettu tunnelointi toimii?

Se käyttää käyttöjärjestelmän reititystaulukoita tiettyjen sovellusten sulkemiseksi pois VPN:n lisäkuormasta.

### Q10: Miten Mullvad käsittelee käteismaksut?

Käteinen lähetetään postitse tunnuskoodin kanssa, hyvitetään käsin ja kuoret silputaan.

## Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

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

**1. VPN-OIVALLUS**

Amagicom AB perusti Mullvadin vuonna 2009 Göteborgissa Ruotsissa.

**2. VPN-OIVALLUS**

Tilinumerot ovat ainoa tunniste, jolla tilejä hyvitetään ja käytetään.

**3. VPN-OIVALLUS**

Käyttäjätietokantaan ei tallenneta nimiä, sähköpostiosoitteita, salasanoja tai puhelinnumeroita.

**4. VPN-OIVALLUS**

WireGuard-avaimet luodaan paikallisesti asiakaslaitteilla palvelinpuolen vaarantumisen estämiseksi.

**5. VPN-OIVALLUS**

Cure53:n vuoden 2024 infrastruktuuriauditoinnissa ei löytynyt VPN-liikenteen anonyymiyden rikkovaa virhettä. [5]

**6. VPN-OIVALLUS**

Jokaisella Mullvadin WireGuard-palvelimella toimii SOCKS5-välityspalvelin, joka on tavoitettavissa vain tunnelissa. [8]

**7. VPN-TIETOA**

WireGuard-liikenne voidaan häivyttää Shadowsocksilla, QUICilla tai LWO:lla palomuurien ohittamiseksi. [10]

**8. VPN-TIETOA**

Mullvad viimeisteli siirtymisen pelkkää RAM-muistia käyttäviin VPN-palvelimiin syyskuussa 2023. [4]

**9. VPN-TIETOA**

ML-KEM ja Classic McEliece neuvottelevat WireGuardille kvanttiturvallisen esijaetun avaimen. [2]

**10. VPN-OIVALLUS**

Käteiskuoret ja niiden muut kuin rahasisällöt silputaan, kun aika on hyvitetty tilille.

# Tekniset viitteet ja lähteet

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

## TIETEELLISET JA ALAN VIITTEET


[1] Mullvad VPN. (n.d.). Why Mullvad VPN?
https://mullvad.net/en/why-mullvad-vpn

[2] Mullvad VPN. (n.d.). Quantum-resistant tunnels with WireGuard.
https://mullvad.net/en/help/quantum-resistant-tunnels-with-wireguard

[3] Mullvad VPN. (n.d.). CLI commands for using WireGuard.
https://mullvad.net/en/help/cli-command-wg

[4] Mullvad VPN. (2023). We have successfully completed our migration to RAM-only VPN infrastructure.
https://mullvad.net/en/blog/we-have-successfully-completed-our-migration-to-ram-only-vpn-infrastructure

[5] Mullvad VPN. (2024). Fourth Infrastructure audit completed by Cure53.
https://mullvad.net/en/blog/fourth-infrastructure-audit-completed-by-cure53

[6] Mullvad VPN. (2024). The report for the 2024 security audit of the app is now available.
https://mullvad.net/en/blog/the-report-for-the-2024-security-audit-of-the-app-is-now-available

[7] Mullvad VPN. (2024). Removing OpenVPN 15th January 2026.
https://mullvad.net/en/blog/removing-openvpn-15th-january-2026

[8] Mullvad VPN. (n.d.). SOCKS5 proxy.
https://mullvad.net/en/help/socks5-proxy

[9] Mullvad VPN. (n.d.). Why WireGuard?
https://mullvad.net/en/help/why-wireguard

[10] Mullvad VPN. (n.d.). Using Mullvad VPN in restrictive locations.
https://mullvad.net/en/help/connecting-to-mullvad-vpn-from-restrictive-locations

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

[12] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

## Vastausavain: Tarkistuspiste 1 – Monivalinta

**1 Kysymys 1** — **Oikea vastaus: B**

**OPETTAJALLE**

Mikä tunnelointiprotokolla on oletuksena Mullvadin sovelluksessa? → WireGuard

**2 Kysymys 2** — **Oikea vastaus: A**

**OPETTAJALLE**

Kun napsautat "generate account", saat tilinumeron; sähköpostiosoitetta tai muita henkilötietoja ei pyydetä.

**3 Kysymys 3** — **Oikea vastaus: B**

**OPETTAJALLE**

Mullvadin kvanttiturvalliset WireGuard-tunnelit käyttävät ML-KEM:ia ja Classic McEliecea esijaetun avaimen sopimiseen.

**4 Kysymys 4** — **Oikea vastaus: C**

**OPETTAJALLE**

Mikä turvamekanismi estää WebRTC-vuotovaarat? → WebRTC:n reitittäminen VPN-liitännän kautta

**5 Kysymys 5** — **Oikea vastaus: B**

**OPETTAJALLE**

Mikä multihop-ominaisuus reitittää liikenteen usean solmun kautta? → WireGuard Multihop

## Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

**6** **Kysymys 6** — **Oikea vastaus: Epätosi**

**OPETTAJALLE**

Epätosi: Mullvad ei koskaan pyydä sähköpostiosoitetta; tilit tunnistetaan vain luodun numeron perusteella.

**7** **Kysymys 7** — **Oikea vastaus: Tosi**

**OPETTAJALLE**

SOCKS5-välityspalvelimia voi määrittää Mullvad-tunneleiden sisälle.

**8** **Kysymys 8** — **Oikea vastaus: Epätosi**

**OPETTAJALLE**

Epätosi: Mullvad omistaa joitakin palvelimia, mutta vuokraa myös omistettuja palvelimia palveluntarjoajilta.

**9** **Kysymys 9** — **Oikea vastaus: Tosi**

**OPETTAJALLE**

Network Kill Switch on oletuksena aina käytössä.

**10** **Kysymys 10** — **Oikea vastaus: Tosi**

**OPETTAJALLE**

Postitse lähetetyt käteismaksut eivät ole lainkaan palautettavissa.

# Sanastoavaimet ja arviointikriteerit

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

## TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

| | | | |
|---|---|---|---|
| B 1. WIREGUARD | D 2. MULTIHOP | G 3. VAIN RAM | A 4. KILL SWITCH |
| H 5. LOKITTOMUUS | C 6. SOCKS-VÄLITYS | E 7. KVANTTIKESTÄVÄ | F 8. DNS-VUODOT |

## TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

| | | | |
|---|---|---|---|
| 1 WIREGUARD | 2 MULTIHOP | 3 RAM-ONLY | 4 KILL SWITCH |
| 5 LOKITTOMUUS | 6 SOCKS5 | 7 KVANTTIKESTÄVÄ | 8 DNS-VUODOT |

## TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

| | | | |
|---|---|---|---|
| 1 F – SOCKSVÄLITYS | 2 G – KVANTTIKESTÄVÄ | 3 A – WIREGUARD | 4 C – RAMONLY |
| 5 D – KILLSWITCH | 6 B – MULTIHOP | 7 H – DNSVUODOT | 8 E – LOKITTOMUUS |

### KESKUSTELUMUISTIINPANOT OPETTAJILLE

**Avaintermit:**
Tarkista, osaavatko oppilaat selittää termit WIREGUARD, MULTIHOP ja VAIN RAM omin sanoin ja antaa jokaisesta esimerkin.

**Tapaustutkimukset:**
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

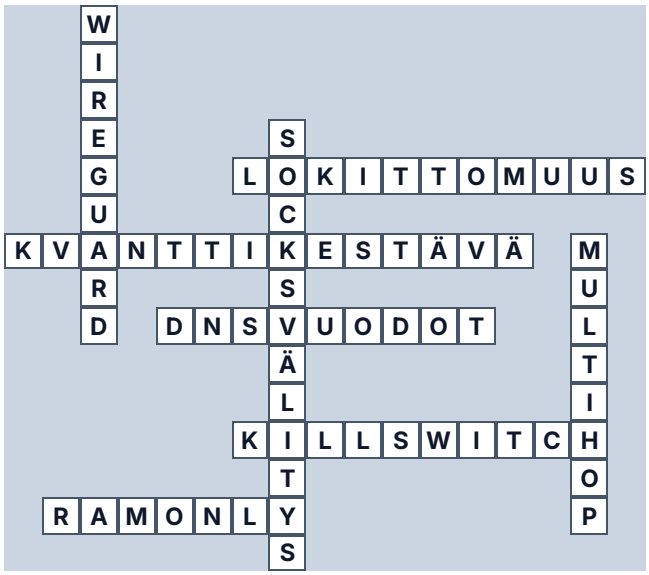
**Lähteiden arviointi:**
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

# Tehtäväavaimet ja opettajan muistiinpanot

## SANAHAUN RATKAISU

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

## RISTIKON RATKAISU




## OPETTAJAN OPAS RISTIKON RATKAISUIHIN

### VAAKASUORAAN

**3 vaakasuoraan: LOKITTOMUUS** Riippumattomien tarkastusten todentama nollasäilytysstandardi (11 kirjainta)

**4 vaakasuoraan: KVANTTIKESTÄVÄ** Salausmekanismit, jotka on suunniteltu kestämään kvanttihyökkäyksiä (14 kirjainta)

**6 vaakasuoraan: DNSVUODOT** DNS-kyselyjen kohteiden paljastuminen VPN-tunnelin ulkopuolella (9 kirjainta)

**7 vaakasuoraan: KILLSWITCH** Suojaominaisuus, joka katkaisee liikenteen VPN-yhteyden pettäessä (10 kirjainta)

**8 vaakasuoraan: RAMONLY** Haihtuvaa muistia käyttävä palvelinlaitteisto, joka ei säilytä dataa uudelleenkäynnistyksen jälkeen (7 kirjainta)

### PYSTYSUORAAN

**1 pystysuoraan: WIREGUARD** Kevyt ja tehokas suojattu tunnelointiprotokolla (9 kirjainta)

**2 pystysuoraan: SOCKSVÄLITYS** Sisäinen välityspalvelinprotokolla, jota käytetään asiakassovellusten eristämiseen (12 kirjainta)

**5 pystysuoraan: MULTIHOP** Liikenteen reititys sisääntulo- ja poistumispalvelinsolmun kautta (8 kirjainta)

# Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

## SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. UGEIWARDR — **WIREGUARD**
2. RMYLNOA — **RAMONLY**
3. LOTMKOUSTUI — **LOKITTOMUUS**
4. VIVSNETÄKÄTKAT — **KVANTTIKESTÄVÄ**
5. IHUPTMOL — **MULTIHOP**
6. CSLITKIWHL — **KILLSWITCH**
7. LISSOÄSTYCVK — **SOCKSVÄLITYS**
8. TUODVNODS — **DNSVUODOT**

### SALAKIRJOITUSHAASTEEN AVAIN

**"MULLVAD TILI EI VAADI SALASANAA TAI SÄHKÖPOSTIA"**

# Tapaustutkimusten vastausavain

## A TAPAUSTUTKIMUS 1: KVANTTIKESTÄVYYDEN INTEGROINTI

Opettajan ratkaisu

### ARVIOINTIOHJE

**Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:**

- Tilanneanalyysi: Rahoitusyhtiön täytyy suojata tiedostosiirrot tulevaa kvanttisalauksen purkua vastaan.
- Suositeltu strategia ja ratkaisu: Ota käyttöön kvanttikestävät WireGuard-tunnelit käyttäen kvanttiturvallisia esijaettuja avaimia.

## B TAPAUSTUTKIMUS 2: SALAINEN TUTKIVA REITITYS

Opettajan ratkaisu

### ARVIOINTIOHJE

**Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:**

- Tilanneanalyysi: Tutkija haluaa reitittää verkkonsa kahden palvelimen kautta piilottaakseen sisääntulopisteensä.
- Suositeltu strategia ja ratkaisu: Ota käyttöön Mullvadin WireGuard Multihop -ominaisuus sisääntulo- ja poistumissolmujen ketjuttamiseksi.