Nimi: _____ Päivämäärä: _____ Pisteet: _____

Paras VPN yksityisyyteen

Lainkäyttöalueiden, vain RAM-muistia käyttävien palvelimien ja auditoitujen lokittomuuskäytäntöjen analysointi.

PARAS VPN YKSITYISYYTEEN: OPPIMISEN YLEISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: VPN-yksityisyyden ja auditoitujen palvelininfrastruktuurien perusperiaatteet. Tutustut lainkäyttöalueisiin, Five Eyes -liittoumiin, pelkästään RAM-muistia käyttäviin verkkoihin ja kolmansien osapuolten no-logs-todistuksiin.

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/paras-vpn-yksityisyyteen/

Oppimispolkusi: yksityisyyden VPN

- Analysoi oikeudellisten toimivaltojen vaikutusta käyttäjätietojen säilyttämiseen ja suojaukseen.
- Arvioi pelkästään RAM-muistia käyttävien haihtuvien palvelininfrastruktuurien tietoturvaetuja.
- Tarkista palveluntarjoajan vaatimustenmukaisuus riippumattomien kolmannen osapuolen lokittomuusauditointien avulla.
- Arvioi Multi-hop Secure Core -reitityksen tarjoamaa uhkamallinnussuojaa.
- Toteuta anonyymit rekisteröitymiskulut, jotka käyttävät luotuja numeerisia tiliavaimia.
- Määritä hätätilanteiden Kill Switch -käytännöt, jotka pudottavat liikenteen verkkohäiriöiden aikana.

YKSITYISYYS-VPN-OPAS, OHJEET

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

TIETOSUOJA JA AUDITOITU INFRASTRUKTUURI (JOHDANTO)

VPN-palveluntarjoajan yksityisyyden arviointi edellyttää sen lainkäyttövallan, palvelininfrastruktuurin ja kolmannen osapuolen tarkastushistorian analysointia. Vain RAM-muistia käyttävät palvelimet on suunniteltu niin, että muistissa oleva data pyyhitään jokaisen uudelleenkäynnistyksen yhteydessä, mikä auttaa suojaamaan asiakkaan henkilöllisyyttä.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. 1. Mikä on pelkästään RAM-muistia käyttävän palvelininfrastruktuurin tärkein hyöty?
   - A) Tietojen automaattinen pyyhintä uudelleenkäynnistyksissä
   - B) Pysyvä pitkäaikainen tallennus
   - C) Hitaammat yhteysnopeudet
   - D) Korkeat laitteiston ylläpitokustannukset

2. 2. Mikä VPN-lainkäyttöalue toimii Five Eyes -tiedustelu-yhteenliittymän ulkopuolella?
   - A) Panama
   - B) Yhdysvallat
   - C) Yhdistynyt kuningaskunta
   - D) Kanada

3. 3. Mikä auditointiyritys varmisti NordVPN:n tiukan no-logs-käytännön?
   - A) Deloitte
   - B) PwC
   - C) KPMG
   - D) Ernst & Young

4. 4. Mikä on Proton VPN:n kaksoishyppy-yksityisyysreititysominaisuuden nimi?
   - A) Secure Core
   - B) Quick Connect
   - C) Jaettu tunneli
   - D) NetShield

5. 5. Mikä palveluntarjoaja sallii rekisteröitymisen pelkällä luodulla tilinumerolla?
   - A) Mullvad
   - B) NordVPN
   - C) ExpressVPN
   - D) Proton VPN

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Auditoidun lokittomuuskäytännön mukaan VPN-palveluntarjoaja ei tallenna toimintaa eikä yhteyksien aikaleimoja.

○ Tosi ○ Epätosi

7 Kysymys 7

7. Five Eyes -tiedusteluliittouma on kumppanuus, joka ei jaa valvonta- tai verkkotietoja.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Pelkkää RAM-muistia käyttävät palvelimet säilyttävät käyttäjien yhteystiedot rajattomasti vielä järjestelmän virrankatkaisun jälkeenkin.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Proton VPN julkaisee täysin avoimen lähdekoodin kaikissa asiakassovelluksissaan.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Mullvad vaatii käyttäjiä syöttämään rekisteröitymisen yhteydessä vahvistetun sähköpostiosoitteen ja oikean nimen.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. VPN-palveluntarjoajat käyttävät palvelimia, joita kutsutaan nimellä _____ , jotta muistissa oleva data tyhjennetään jokaisessa uudelleenkäynnistyksessä.

2. Korkean riskin ympäristöissä Proton VPN:n _____ ohjaa liikenteen kahden palvelinhypyn kautta.

3. Paikka, jossa palveluntarjoaja on perustettu, on sen oikeudellinen _____ , joka määrää tietolait.

4. _____ on auditoinut NordVPN:n tiukat yksityisyysväitteet useita kertoja vaatimustenmukaisuuden osoittamiseksi.

5. Mullvad vaatii vain satunnaisen tilinumeron; tämä maksimoi sen, mitä kutsutaan nimellä _____ .

6. Jos VPN-tunneli katkeaa yllättäen, sisäänrakennettu _____ estää kaiken internetliikenteen.

SANASTON SANAPANKKI

ANONYMITEETTI | AVOIN KOODI | DELOITTE | KILL SWITCH | LAINKÄYTTÖALUE | SECURE CORE | TUNNELOINTI | VAIN RAM

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Keskeisten käsitteiden yhdistäminen

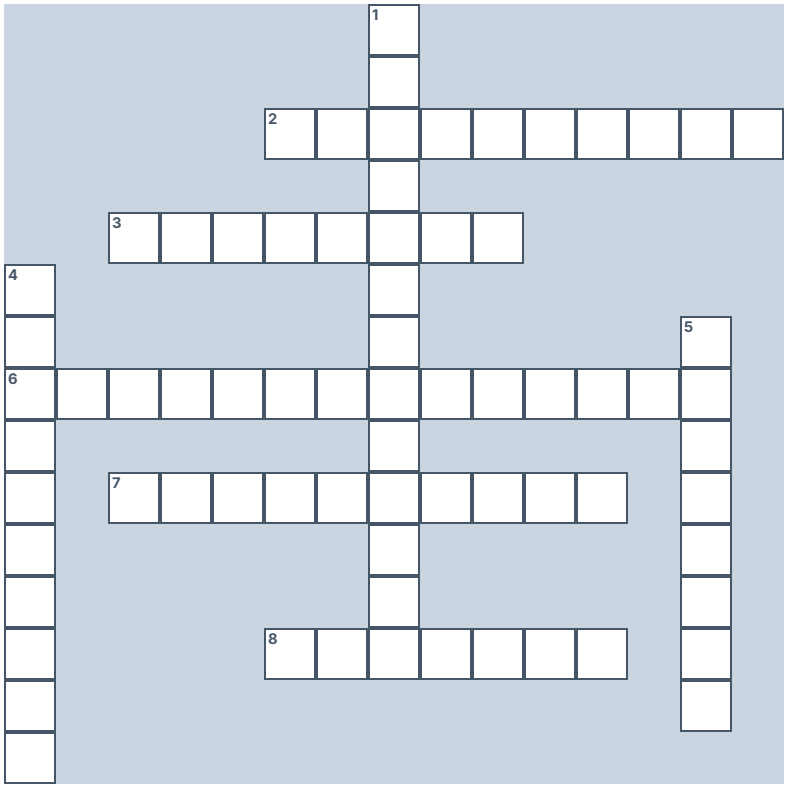
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. VAIN RAM	A	Oikeudellinen alue, jonka lait koskevat VPN-palveluntarjoajan tietoja.
☐	2. SECURE CORE	B	Julkisesti tarkastettavissa oleva ohjelmistoasiakkaan koodi.
☐	3. LAINKÄYTTÖVALTA	C	Rekisteröitymistapa, joka käyttää tilinumeroita sähköpostiosoitteiden sijaan.
☐	4. DELOITTE	D	Maailmanlaajuinen tiedustelutietojen jakamisen liittouma.
☐	5. ANONYMITEETTI	E	Ominaisuus, joka estää liikenteen, jos VPN-tunneli katkeaa.
☐	6. KILL SWITCH	F	Palvelimen haihtuva muisti, joka pyyhitään jokaisessa uudelleenkäynnistyksessä.
☐	7. AVOIN KOODI	G	Multi-hop-reititys yksityisyysystävällisten palvelimien kautta.
☐	8. FIVE EYES	H	Riippumaton auditointiyritys, joka varmentaa lokittomuuskäytännöt.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

2. Julkisesti tarkastettavissa oleva ohjelmistoasiakkaan koodi (10)

3. Maailmanlaajuinen tiedustelutiedon jakamisen liittouma (8)

6. Oikeudellinen alue, joka säätelee VPN-palveluntarjoajan dataa (14)

7. Monihyppyinen reititys yksityisyyttä suojaavien palvelimien kautta (10)

8. Haihtuva palvelimen muisti, joka tyhjennetään jokaisessa uudelleenkäynnistyksessä (7)

PYSTYSUORAAN

1. Rekisteröitymistapa, jossa sähköpostin sijaan käytetään tilinumeroita (13)

4. Ominaisuus, joka estää liikenteen, jos VPN-tunneli katkeaa (10)

5. Riippumaton tilintarkastusyritys, joka varmentaa no-logs-käytännöt (8)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

2 vaakasuoraan: Julkisesti tarkastettavissa oleva ohjelmistoasiakkaan koodi (10 kirjainta):

3 vaakasuoraan: Maailmanlaajuinen tiedustelutiedon jakamisen liittouma (8 kirjainta):

6 vaakasuoraan: Oikeudellinen alue, joka säätelee VPN-palveluntarjoajan dataa (14 kirjainta):

7 vaakasuoraan: Monihyppyinen reititys yksityisyyttä suojaavien palvelimien kautta (10 kirjainta):

8 vaakasuoraan: Haihtuva palvelimen muisti, joka tyhjennetään jokaisessa uudelleenkäynnistyksessä (7 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Rekisteröitymistapa, jossa sähköpostin sijaan käytetään tilinumeroita (13 kirjainta):

4 pystysuoraan: Ominaisuus, joka estää liikenteen, jos VPN-tunneli katkeaa (10 kirjainta):

5 pystysuoraan: Riippumaton tilintarkastusyritys, joka varmentaa no-logs-käytännöt (8 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

VAINRAM SECURECORE LAINKÄYTTÖALUE DELOITTE ANONYMITEETTI
KILLSWITCH AVOINKOODI FIVEEYES

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. VAINRAM**
- **B. SECURECORE**
- **C. LAINKÄYTTÖALUE**
- **D. DELOITTE**
- **E. ANONYMITEETTI**
- **F. KILLSWITCH**
- **G. AVOINKOODI**
- **H. FIVEEYES**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Monihyppyinen reititys yksityisyyttä suojaavien palvelimien kautta.
2. Haihtuva palvelimen muisti, joka tyhjennetään jokaisessa uudelleenkäynnistyksessä.
3. Riippumaton tilintarkastusyritys, joka varmentaa no-logs-käytännöt.
4. Oikeudellinen alue, joka säätelee VPN-palveluntarjoajan dataa.
5. Ominaisuus, joka estää liikenteen, jos VPN-tunneli katkeaa.
6. Maailmanlaajuinen tiedustelutiedon jakamisen liittouma.
7. Rekisteröitymistapa, jossa sähköpostin sijaan käytetään tilinumeroita.
8. Julkisesti tarkastettavissa oleva ohjelmistoasiakkaan koodi.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi tämän monisteen keskeiset käsitteet. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. **NAVRMIA**
2. **KAÄIYULLTEÖ ATN**
3. **NATEETIOIYM TN**
4. **KDNIIOOAVO**
5. **OEEEUCRSRC**
6. **TEOTDIEL**
7. **ILKIWTCHSL**
8. **EIESFEYV**

Bonustehtävä: Nopeat vastaukset

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

1	VPN-palveluja, jotka tunnet			
2	Tapoja tulla seuratuksi vähemmän			
3	Puhelimesi yksityisyysasetuksia			
4	Laitteita, jotka voivat käyttää VPN:ää			
5	Yksityisyyteen liittyviä sanoja			
6	Asioita, jotka VPN voi piilottaa			
7	Myyttejä VPN:istä			
8	Sanoja, jotka tarkoittavat "salainen"			
9	Paikkoja, joissa käyttäisit VPN:ää			
10	Asioita, jotka haluat pitää yksityisinä verkossa			
11	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
12	Yrityksiä, jotka keräävät tietoja sinusta			
13	Asioita, joilta VPN ei voi suojata sinua			
14	Lokittomuuskäytännön lupauksia			
15	Syitä käyttää VPN:ää matkustaessa			

Tarkistuspiste 8: VPN:n yksityisyyden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: AUDITOITU VARMENNUS

👷

Tilanne: Rahoitusalan yritys haluaa varmistaa, ettei sen VPN-palveluntarjoaja säilytä yhteyksien aikaleimoja, IP-lokeja tai dataan liittyviä toimintatietueita, ja vaatii virallisia kolmannen osapuolen vahvistusraportteja.

Keskustelukysymys: Mitä tiettyä sertifiointia yrityksen tulisi etsiä näiden väitteiden todentamiseksi?

TAPAUSTUTKIMUS 2: VALVONTASUOJA

👷

Tilanne: Korkean riskin lainkäyttöalueella toimiva toimittaja tarvitsee luottamuksellisten materiaalien reitittämistä toimittajalleen samalla kun hän suojaa yhteytensä kansalliselta päätepisteiden valvonnalta.

Keskustelukysymys: Minkä tietyn VPN-määritysominaisuuden toimittajan tulisi ottaa käyttöön päätepisteiden seurannan estämiseksi?

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

1	21	4	9	20	15	9	4	21	20		18	1	13

16	1	12	22	5	12	9	13	5	20		20	1	11	1	1	22	1	20

25	11	19	9	20	25	9	19	25	25	4	5	14

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 tarkastettu no-logs-käytäntö?

Se on käytäntö, jonka riippumattomat kolmannen osapuolen auditoinnit ovat varmentaneet ja joka vahvistaa, ettei VPN kirjaa IP-osoitteita, yhteyslokeja tai selaushistoriaa.

Q2: Miksi palvelimen sijainnin lainkäyttöalue on tärkeä?

Lainkäyttövalta määrää, mitä tietosuojalakeja sovelletaan ja voivatko viranomaiset laillisesti velvoittaa palveluntarjoajan kirjaamaan käyttäjätietoja.

Q3: Mitä pelkkää RAM-muistia käyttävät VPN-palvelimet ovat?

Ne ovat levyttömiä palvelimia, jotka toimivat kokonaan haihtuvassa muistissa, joten muistissa oleva data pyyhkiytyy virtakatkoksessa tai uudelleenkäynnistyksessä.

Q4: Mikä on VPN Kill Switch?

Suojausominaisuus, joka estää internetyhteyden, jos VPN-yhteys katkeaa, ja ehkäisee raakadatan vuotamisen internetoperaattorillesi.

Q5: Miten multi-hop-reititys toimii?

Se reitittää liikenteesi kahden tai useamman eri maissa sijaitsevan palvelimen kautta, mikä estää ketään jäljittämästä yhteyttäsi poistumissolmuun.

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

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

Q6: Voiko VPN taata täydellisen anonymiteetin?

Ei. Anonyymi rekisteröityminen, käteis- tai kryptovaluuttamaksu ja Tor VPN:n päällä vähentävät sitä, mikä voidaan yhdistää sinuun.

Q7: Mikä on DNS-vuoto?

Altistuminen, jossa selain lähettää verkkotunnuskyselyt paikallisen internetoperaattorin DNS-palvelimille salatun VPN-tunnelin sijaan.

Q8: Miksi avoin lähdekoodi on parempi yksityisyyden kannalta?

Se mahdollistaa asiakassovellusten julkisen tarkastuksen ja varmistaa, ettei niissä ole takaovia tai seurantamoduuleja.

Q9: Miten WebRTC-vuotosuojaus toimii?

Se estää selaimia paljastamasta todellisia paikallisia ja julkisia IP-osoitteitasi tiedonsiirtoprotokollien kautta.

Q10: Mitä ovat Five Eyes -valvontaliittoumat?

Yhdysvaltojen, Ison-Britannian, Kanadan, Australian ja Uuden-Seelannin väliset tiedustelutietojen jakamisjärjestelyt, joissa jaetaan sieppattua dataa.

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

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

Q1: Miten pelkkään RAM-muistiin perustuva arkkitehtuuri estää tietojen palauttamisen?

Koska fyysisiä kiintolevyjä ei ole, palvelimen fyysinen takavarikointi ei tuota luettavaa dataa, kun virta on katkaistu.

Q2: Mikä oli ExpressVPN:n turkkilaisen palvelimen takavarikon oikeudellinen merkitys?

Turkkilaiset tutkijat takavarikoivat ExpressVPN-palvelimen vuonna 2017, mutta eivät löytäneet lokeja, jotka olisivat tunnistaneet käyttäjän, mikä tukee sen lokittomuusväitettä. [4]

Q3: Miten Panama ja Brittiläiset Neitsytsaaret hyödyttävät VPN-yksityisyyttä?

Molemmat sijaitsevat Five Eyes -liiton ulkopuolella; NordVPN on Panamassa ja ExpressVPN Brittiläisillä Neitsytsaarilla. [2]

Q4: Mikä on kryptografinen ero Multi-hopin poistumissolmun analyysissä?

Poistumissolmun tarkkailija näkee VPN:stä poistuvan liikenteen, mutta ei voi jäljittää sitä takaisin sisääntulosolmuun, koska ne ovat erillisiä hyppyjä.

Q5: Miten Mullvadin tilijärjestelmä poistaa henkilötiedot?

Mullvad luo rekisteröitymistä varten yksilöllisen 16-numeroisen tilinumeron kysymättä sähköpostiosoitetta, nimeä tai salasanaa. [5]

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

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

Q6: Mikä rooli porttien ohjauksella on yksityisyysmäärityksissä?

Vaikka porttiohjaus on hyödyllinen torrenttien jakamiseen, se voi altistaa aktiiviset paikalliset palvelut, jos palomuuria ei ole sidottu turvallisesti VPN:ään.

Q7: Miten järjestelmätason Kill Switch eroaa sovellustason Kill Switchistä?

Järjestelmätason Kill Switch poistaa koko verkkoliittymän käytöstä, kun taas sovellustason Kill Switch sulkee vain ennalta valitut sovellukset.

Q8: Miksi Proton VPN julkaisee asiakassovellustensa tarkastusraportit?

Tarkastuslöydösten julkaiseminen antaa kenen tahansa tarkistaa, mitä riippumattomat asiantuntijat, kuten SEC Consult, löysivät sen sovelluksista.

Q9: Miten Tor over VPN voi auttaa suojaamaan metatietoja?

Se salaa liikenteen ennen kuin se siirtyy Tor-verkkoon, jolloin palveluntarjoaja ei tiedä sinun käyttävän Toria.

Q10: Miten Fourteen Eyes -liittouma vaikuttaa VPN-palveluihin?

Fourteen Eyes laajentaa valvontayhteistyötä, mikä tarkoittaa, että jäsenvaltioissa toimivat palveluntarjoajat voidaan velvoittaa jakamaan metatietoja.

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

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

1. VPN-OIVALLUS

Pelkkää RAM-muistia käyttävät palvelimet tallentavat käyttöjärjestelmät ja sovellukset pelkästään haihtuvaan muistiin, joten uudelleenkäynnistyksen jälkeen ei jää jälkiä.

2. VPN-OIVALLUS

NordVPN toimii Panamasta ja ExpressVPN Brittiläisiltä Neitsytsaarilta, jotka molemmat ovat Five Eyes -liittouman ulkopuolella. [2]

3. VPN-OIVALLUS

Deloitten riippumattomat auditoinnit ovat toistuvasti vahvistaneet, että NordVPN noudattaa tiukasti lokittomuuskäytäntöään. [1]

4. VPN-OIVALLUS

VPN:n Kill Switch toimii paikallisena palomuurisääntönä, joka estää suojatun yhdyskäytävätunnelin ulkopuolisen liikenteen.

5. VPN-OIVALLUS

Multi-hop-reititys suojaa käyttäjän henkilöllisyyttä erottamalla sisääntulon IP-osoitteen kohteen poistumissolmusta.

6. VPN-OIVALLUS

Mullvad sallii käyttäjien maksaa postitse lähetetyllä käteisellä paremman taloudellisen anonyymiyden vuoksi.

7. VPN-TIETOA

Avoimen lähdekoodin VPN-asiakasohjelmat ovat ratkaisevia sen osoittamiseksi, ettei ohjelmistossa ole piilotettua telemetriaseurantaa.

8. VPN-TIETOA

DNS-vuotoja syntyy, kun käyttöjärjestelmän tavalliset kyselyt ohittavat määritetyt virtuaaliset verkkosovittimet.

9. VPN-TIETOA

Jaetut IP-osoitejoukot sekoittavat tuhansia käyttäjiä yhteen, mikä estää ulkopuolisia tarkkailijoita seuraamasta yksittäisten käyttäjien toimintaa.

10. VPN-OIVALLUS

Five Eyes -liittoumaan kuuluvat Yhdysvallat, Britannia, Kanada, Australia ja Uusi-Seelanti.

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[2] NordVPN. (n.d.). Privacy Policy - Nord Account.
https://nordvpn.com/privacy-policy/

[3] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[4] TorrentFreak. (2017). VPN Server Seized to Investigate Russian Ambassador's Assassination.
https://torrentfreak.com/vpn-server-seized-to-investigate-russian-ambassadors-assassination-1171219/

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

[6] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[7] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Vain RAM -muisti** HAIHTUVA RAM — **Oikea vastaus: A**

OPETTAJALLE

Pelkkää RAM-muistia käyttävät palvelimet tallentavat tietoja tilapäisesti haihtuvaan muistiin ja tyhjentävät kaiken uudelleenkäynnistyksessä. Lähde: CISA Telework.

2 **Lainkäyttövalta** LAINMUKAINEN — **Oikea vastaus: A**

OPETTAJALLE

Lainkäyttöalue ratkaisee, voiko valtio pakottaa palveluntarjoajan luovuttamaan lokit. Lähde: Switzerland Jurisdiction.

3 **Kysymys 3** — **Oikea vastaus: A**

OPETTAJALLE

Deloitte on arvioinut NordVPN:n lokittomuuskäytäntöä toistuvasti, viimeksi vuonna 2026 ilmoitetussa kuudennessa arvioinnissa.

4 **Secure Core** MULTI-HOP-HYPYT — **Oikea vastaus: A**

OPETTAJALLE

Secure Core reitittää liikenteen tietosuojamyönteisten hyppyjen kautta ennen poistumista, jotta poistumispisteen vaarantuminen estetään. Lähde: Proton VPN Swiss.

5 **Nimettömyys** NUMEERINEN — **Oikea vastaus: A**

OPETTAJALLE

Mullvad ei vaadi henkilötietoja vaan rekisteröi tilit yksinkertaisilla numerotunnuksilla. Lähde: Mullvad Account.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** — **Oikea vastaus: Tosi**

OPETTAJALLE

Auditoidun lokittomuuskäytännön mukaan VPN-palveluntarjoaja ei tallenna toimintaa eikä yhteyksien aikaleimoja.

7 **Five Eyes** TIEDONJAKOLIITOT — **Oikea vastaus: Epätosi**

OPETTAJALLE

Five Eyes -tiedustelutietojen jakamissopimukset sallivat valtioiden välisen valvontatietojen jakamisen. Lähde: Surveillance Alliances.

8 **Vain RAM -muisti** HAIHTUVA RAM — **Oikea vastaus: Epätosi**

OPETTAJALLE

Pelkkää RAM-muistia käyttävät palvelimet tallentavat tietoja tilapäisesti haihtuvaan muistiin ja tyhjentävät kaiken uudelleenkäynnistyksessä. Lähde: RAM-only Architecture.

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

OPETTAJALLE

Proton VPN julkaisee täysin avoimen lähdekoodin kaikissa asiakassovelluksissaan.

10 **Kysymys 10** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Mullvad ei pyydä sähköpostiosoitetta eikä nimeä; saat sen sijaan satunnaisesti luodun tilinumeron.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

F 1. VAIN RAM	G 2. SECURE CORE	A 3. LAINKÄYTTÖVALTA	H 4. DELOITTE
C 5. ANONYMITEETTI	E 6. KILL SWITCH	B 7. AVOIN KOODI	D 8. FIVE EYES

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 VAIN RAM	2 SECURE CORE	3 LAINKÄYTTÖALUE	4 DELOITTE
5 ANONYMITEETTI	6 KILL SWITCH		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 B – SECURECORE	2 A – VAINRAM	3 D – DELOITTE	4 C – LAINKÄYTTÖALUE
5 F – KILLSWITCH	6 H – FIVEEYES	7 E – ANONYMITEETTI	8 G – AVOINKOODI

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit VAIN RAM, SECURE CORE ja LAINKÄYTTÖVALTA omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

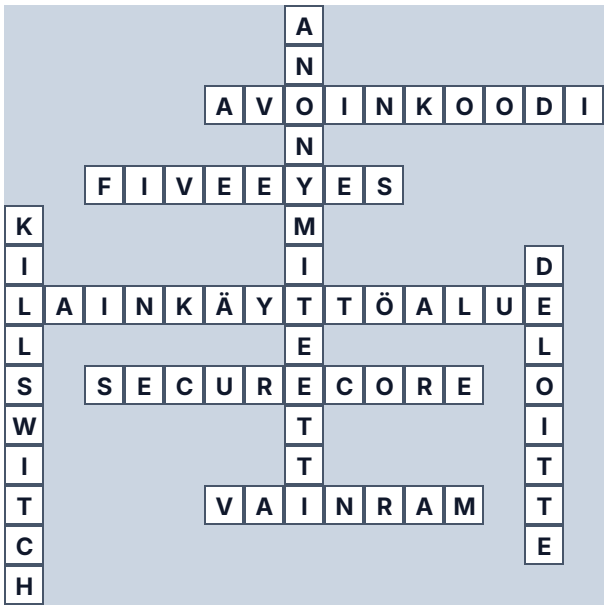
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: AVOINKOODI Julkisesti tarkastettavissa oleva ohjelmistoasiakkaan koodi (10 kirjainta)

3 vaakasuoraan: FIVEEYES Maailmanlaajuinen tiedustelutiedon jakamisen liittouma (8 kirjainta)

6 vaakasuoraan: LAINKÄYTTÖALUE Oikeudellinen alue, joka säätelee VPN-palveluntarjoajan dataa (14 kirjainta)

7 vaakasuoraan: SECURECORE Monihyppyinen reititys yksityisyyttä suojaavien palvelimien kautta (10 kirjainta)

8 vaakasuoraan: VAINRAM Haihtuva palvelimen muisti, joka tyhjennetään jokaisessa uudelleenkäynnistyksessä (7 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: ANONYMITEETTI Rekisteröitymistapa, jossa sähköpostin sijaan käytetään tilinumeroita (13 kirjainta)

4 pystysuoraan: KILLSWITCH Ominaisuus, joka estää liikenteen, jos VPN-tunneli katkeaa (10 kirjainta)

5 pystysuoraan: DELOITTE Riippumaton tilintarkastusyritys, joka varmentaa no-logs-käytännöt (8 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. N A V R M I A — **VAINRAM**
2. K A Ä I Y U L L T E Ö A T N — **LAINKÄYTTÖALUE**
3. N A T E E T I O I Y M T N — **ANONYMITEETTI**
4. K D N I I O O A V O — **AVOINKOODI**
5. O E E E U C R S R C — **SECURECORE**
6. T E O T D I E L — **DELOITTE**
7. I L K I W T C H S L — **KILLSWITCH**
8. E I E S F E Y V — **FIVEEYES**

SALAKIRJOITUSHAASTEEN AVAIN

"AUDITOIDUT RAM PALVELIMET TAKAAVAT YKSITYISYYDEN"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Auditoitu varmennus

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Rahoitusyritys haluaa varmistaa, ettei sen VPN-palveluntarjoaja säilytä yhteysaikaleimoja, IP-lokeja tai tietoaktiviteettitietueita, ja vaatii virallisia kolmannen osapuolen validointiraportteja.
- Suositeltu strategia ja ratkaisu: Yrityksen tulisi pyytää riippumattomia auditointiraportteja suurilta toimijoilta, kuten Deloitte, PwC tai KPMG, jotka nimenomaisesti varmentavat no-logs-käytännön ja infrastruktuurin.

B Tapaustutkimus 2: Valvontasuoja

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Korkean riskin lainkäyttöalueella toimiva toimittaja tarvitsee luottamuksellisen aineiston reitittämistä toimittajalleen samalla kun hän suojaa yhteytensä kansalliselta päätepistevalvonnalta.
- Suositeltu strategia ja ratkaisu: Toimittajan tulisi ottaa käyttöön Proton VPN:n Secure Core -monihyppyreititys, joka ohjaa liikenteen kahden palvelinhypyn kautta yksityisyyttä painottavissa maissa.