Nimi: _____ Päivämäärä: _____ Pisteet: _____

Miten valitset VPN:n Tehtävämoniste

VPN-palveluntarjoajien, tietoturvastandardien, tarkastusten ja lokikäytäntöjen arviointi

VPN, OPPIMISEN YLEISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: virtuaalisten yksityisverkkojen (VPN) perusperiaatteet. Tutustut siihen, miten salatut tunnelit suojaavat tietojasi, miten verkkoprotokollat toimivat ja miten tunnistat ja ehkäiset yksityisyysvuotoja.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse VPN-käsitteet ja -protokollat.**
- [ ] **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 VPN-opas

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

Oppimispolkusi: VPN

- Arvioi palveluntarjoajan lainkäyttövaltaa ja lokittomuuskäytäntöjä yksityisyyden kannalta.
- Vertaile tunnelointiprotokollia, kuten WireGuardia ja OpenVPN:ää, nopeuden kannalta.
- Analysoi tietoturvaominaisuuksia, kuten kill switchejä ja vain RAM-muistia käyttäviä palvelinsolmuja.
- Tunnista riippumattomat tietoturva-auditoinnit ja hinnoittelupaketit valintaa tehdessäsi.
- Valitse palvelinsijainnit nopeutesi ja maantieteellisten estojen ohittamisen tarpeiden mukaan.

VALINTATEHTÄVÄMONISTEEN OHJEET

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

VPN:N VALINTA (JOHDANTO)

Oikean VPN:n valinta edellyttää markkinointipuheiden taakse katsomista. Luotettavalla palveluntarjoajalla on oltava todennettu zero-logs-käytäntö, turvalliset salausprotokollat ja avoimen lähdekoodin asiakasohjelmat. Arvioimalla tietoturvaominaisuuksia, lainkäyttöalueita ja nopeutta voit valita VPN:n, joka vastaa digitaalisen suojauksesi tarpeita.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mikä on keskeinen tekijä turvallista VPN-palveluntarjoajaa valittaessa?

- A. Palvelinmaiden määrä
- B. Riippumattomasti auditoitu lokittomuuskäytäntö
- C. Edullisin kuukausihintataso
- D. Näyttävät mainossponsoroinnit

2. Mikä VPN-protokolla tarjoaa parhaan tasapainon nopeuden ja auditoitavuuden välillä?

- A. PPTP (vanha)
- B. L2TP/IPSec
- C. OpenVPN vain TCP:n yli
- D. WireGuard

3. Miksi käyttäjien tulisi välttää ilmaisia VPN:iä arkaluonteisissa toimissa?

- A. Ne on kielletty Yhdysvalloissa
- B. Ne myyvät usein verkkoselaushistoriasi
- C. Ne eivät tue tavallista verkkoselausta
- D. Ne vaativat erikoislaitteiston yhdistämiseen

4. Mitä palveluntarjoajan kotimaan lainkäyttöalue määrää?

- A. Palvelinyhteyden nopeus
- B. Tuettujen laitteiden tyypit
- C. Tietojen säilytystä ja kotietsintälupia koskevat paikalliset lait
- D. Asiakassovelluksen visuaalinen teema

5. Mikä on VPN-asiakasohjelman 'kill switch' -ominaisuuden ensisijainen tarkoitus?

- A. Estää internetyhteyden, jos VPN-yhteys katkeaa
- B. Poistaa kaikki laitteelle asennetut sovellukset
- C. Palvelinyhteyden nopeuden kaksinkertaistaminen
- D. Käyttöjärjestelmän käynnistämiseksi uudelleen joutenoloaikana

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. VPN suojaa laitettasi haittaohjelmalatauksilta ja virustiedostoilta.

○ Tosi ○ Epätosi

7 Kysymys 7

7. Deloitten kaltaisten yritysten riippumattomat auditoinnit vahvistavat nollalokivaatimukset.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Palveluntarjoajan kotimaan lait eivät vaikuta käyttäjätietojen yksityisyyteen.

○ Tosi ○ Epätosi

9 Kysymys 9

9. WireGuardin kompakti koodipohja on helpompi auditoida kuin OpenVPN:n.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Ilmaiset VPN:t myyvät usein mainoksia tai seuraavat käyttäjiä kattaakseen palvelinkustannuksia.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Riippumattomasti todennettu _____ -käytäntö sitouttaa VPN-palveluntarjoajan olemaan tallentamatta verkkohistoriaasi.

2. Moderni _____ -protokolla tarjoaa suuren nopeuden ja käyttää hyvin pientä koodikantaa.

3. Turvaominaisuus nimeltä _____ pysäyttää kaiken liikenteen, jos VPN-yhteys katkeaa yllättäen.

4. Palveluntarjoajan oikeudellinen _____ ratkaisee, onko se valvontasopimusten alainen.

5. _____ -palvelimet auttavat estämään käyttäjätietojen säilymisen uudelleenkäynnistyksen jälkeen.

6. Nollatietoväitteiden todentamiseksi tarvitaan tunnettujen yritysten tekemä kolmannen osapuolen suorittama tietoturva _____ .

SANASTON SANAPANKKI

ILMAINEN VPN | KILL SWITCH | LAINKÄYTTÖALUE | MULTIHOP | NO-LOGS | RAM-ONLY | TARKASTUS | WIREGUARD

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Verkkokäsitteiden yhdistäminen

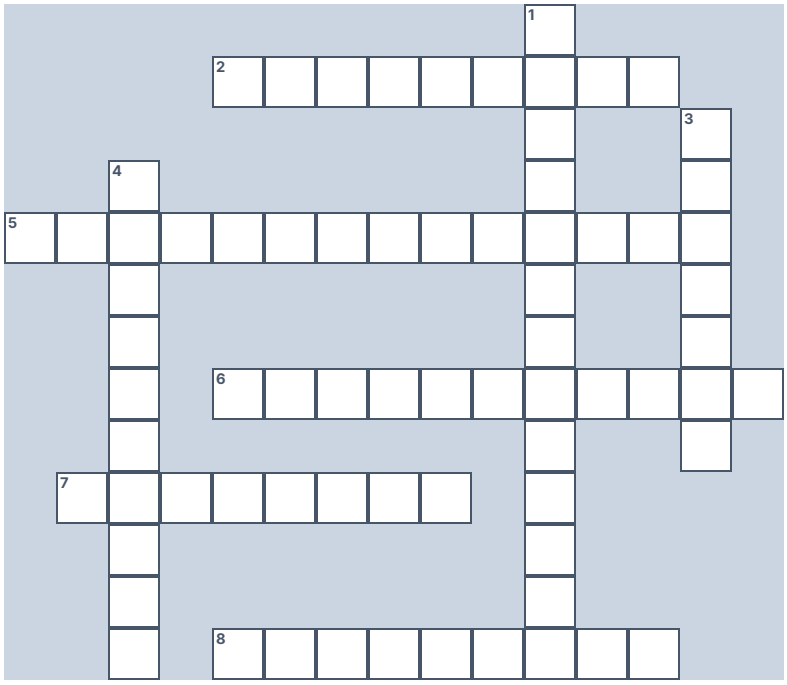
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. WireGuard	A	Riskialtis yhteyspalvelu, joka tuottaa usein tuloa kirjaamalla ja myymällä selaintietoja.
☐	2. Tarkastetut lokit	B	Turvamekanismi, joka estää internetreitityksen, jos suojattu tunneli katkeaa.
☐	3. Oikeudenkäyttöalue	C	Kansainvälinen tiedustelutietojen jakamisliitto, johon kuuluvat Yhdysvallat, Iso-Britannia, Kanada, Australia ja Uusi-Seelanti.
☐	4. Kill switch	D	Laitteistoinfrastruktuuri, joka toimii haihtuvalla muistilla, joten tietoja ei tallenneta levylle.
☐	5. Five Eyes	E	Maantieteellinen alue, joka määrää VPN-palveluntarjoajan oikeudelliset velvoitteet.
☐	6. Ilmainen VPN	F	Moderni nopea protokolla, jossa on noin 4 000 riviä erittäin helposti auditoitavaa koodia.
☐	7. Vain RAM-muistia käyttävät palvelimet	G	Kypsä, laajasti tarkastettu avoimen lähdekoodin protokolla, jonka koodikanta on paljon suurempi kuin WireGuardin.
☐	8. OpenVPN	H	Riippumattomien kolmansien osapuolten kyberturvallisuusyritysten vahvistama yksityisyysväite.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

2. Moderni, nopea protokolla, jonka koodia on noin 4 000 riviä ja joka on erittäin helppo tarkastaa (9)

5. Maantieteellinen alue, joka määrää VPN-palveluntarjoajan oikeudelliset velvoitteet (14)

6. Riskialtis yhteyspalvelu, joka rahoittaa toimintansa usein kirjaamalla ja myymällä selaintietoja (11)

7. Kansainvälinen tiedustelutietojen jakamisen liitto USA:n, Britannian, Kanadan, Australian ja Uuden-Seelannin välillä (8)

8. Yksityisyysväite, jonka riippumattomat kolmannen osapuolen tietoturvayritykset ovat todentaneet (9)

PYSTYSUORAAN

1. Laitteistoinfrastruktuuri, joka toimii kokonaan haihtuvalla muistilla ja estää tietojen tallentamisen (13)

3. Kypsä, laajasti tarkastettu avoimen lähdekoodin protokolla, jonka koodikanta on paljon WireGuardia suurempi (7)

4. Suojamekanismi, joka estää internetliikenteen reitityksen, jos suojattu tunneli katkeaa (10)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

2 vaakasuoraan: Moderni, nopea protokolla, jonka koodia on noin 4 000 riviä ja joka on erittäin helppo tarkastaa (9 kirjainta):

5 vaakasuoraan: Maantieteellinen alue, joka määrää VPN-palveluntarjoajan oikeudelliset velvoitteet (14 kirjainta):

6 vaakasuoraan: Riskialtis yhteyspalvelu, joka rahoittaa toimintansa usein kirjaamalla ja myymällä selaintietoja (11 kirjainta):

7 vaakasuoraan: Kansainvälinen tiedustelutietojen jakamisen liitto USA:n, Britannian, Kanadan, Australian ja Uuden-Seelannin välillä (8 kirjainta):

8 vaakasuoraan: Yksityisyysväite, jonka riippumattomat kolmannen osapuolen tietoturvayritykset ovat todentaneet (9 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Laitteistoinfrastruktuuri, joka toimii kokonaan haihtuvalla muistilla ja estää tietojen tallentamisen (13 kirjainta):

3 pystysuoraan: Kypsä, laajasti tarkastettu avoimen lähdekoodin protokolla, jonka koodikanta on paljon WireGuardia suurempi (7 kirjainta):

4 pystysuoraan: Suojamekanismi, joka estää internetliikenteen reitityksen, jos suojattu tunneli katkeaa (10 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

WIREGUARD, TARKASTUS, LAINKÄYTTÖALUE, KILLSWITCH, FIVEEYES, ILMAINENVPN, RAMPALVELIMET, OPENVPN

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. WIREGUARD**
- **B. TARKASTUS**
- **C. LAINKÄYTTÖALUE**
- **D. KILLSWITCH**
- **E. FIVEEYES**
- **F. ILMAINENVPN**
- **G. RAMPALVELIMET**
- **H. OPENVPN**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Kansainvälinen tiedustelutietojen jakamisen liitto USA:n, Britannian, Kanadan, Australian ja Uuden-Seelannin välillä.
2. Moderni, nopea protokolla, jonka koodia on noin 4 000 riviä ja joka on erittäin helppo tarkastaa.
3. Kypsä, laajasti tarkastettu avoimen lähdekoodin protokolla, jonka koodikanta on paljon WireGuardia suurempi.
4. Riskialtis yhteyspalvelu, joka rahoittaa toimintansa usein kirjaamalla ja myymällä selaintietoja.
5. Suojamekanismi, joka estää internetliikenteen reitityksen, jos suojattu tunneli katkeaa.
6. Laitteistoinfrastruktuuri, joka toimii kokonaan haihtuvalla muistilla ja estää tietojen tallentamisen.
7. Maantieteellinen alue, joka määrää VPN-palveluntarjoajan oikeudelliset velvoitteet.
8. Yksityisyysväite, jonka riippumattomat kolmannen osapuolen tietoturvayritykset ovat todentaneet.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä VPN-käsitteitä ja -termejä. Kirjoita vastauksesi täytettäviin syöttökenttiin.

1. **UGEIWARDR**

2. **KAÄIYULLTEÖ ATN**

3. **EIFEYSEV**

4. **LELMEATVMI RAP**

5. **TAASSKTUR**

6. **CSLITKIWHL**

7. **NIILENVPMNA**

8. **PNNOPVE**

Bonustehtävä: Nopeat vastaukset

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

1	Asioita, jotka VPN voi piilottaa			
2	Asioita, jotka ovat hintaa tärkeämpiä			
3	Paikkoja, joista voit lukea VPN-arvosteluja			
4	Asioita, joilta VPN ei voi suojata sinua			
5	Kysymyksiä VPN-yrityksen myyntitiimille			
6	Asioita, jotka internetoperaattorisi näkee			
7	Kohteita tarkistuslistallasi VPN:ää valitessasi			
8	Paikkoja, joissa käyttäisit VPN:ää			
9	Varoitusmerkkejä VPN-palveluntarjoajassa			
10	Yksityisyyteen liittyviä sanoja			
11	Asioita, jotka testaisit ensin			
12	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
13	Syitä käyttää VPN:ää matkustaessa			
14	Laitteita, jotka voivat käyttää VPN:ää			
15	Myyttejä VPN:istä			

Tarkistuspiste 8: VPN:n tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

SARAH (KAHVILAN OPISKELIJA)

👷 "Hei! Istun Coffee & Bytesissa. Täällä on suojaamaton julkinen verkko nimeltä 'Free_Wi-Fi_No_Password'. Haluan kirjautua koulun sähköpostiin ja lähettää tehtäväni, mutta pelkään hakkereita. Mitä riskejä tämän verkon käyttöön liittyy ilman VPN:ää, ja miten VPN suojaa tietoni?"

ALEX (MATKAILIJAOPISKELIJA)

👷 "Voi ei! Matkustan ulkomailla projektin vuoksi ja yritän katsoa biologiadokumenttia, joka on isännöity kotimaassani olevalla palvelimella. Sivusto kuitenkin sanoo 'Tämä video ei ole saatavilla nykyisessä sijainnissasi.' Miksi minut on estetty, ja miten VPN voi auttaa katsomaan sen?"

Tarkistuspiste 9: Salakirjoituksen purkaminen

Suorita valintaoppaan koulutuksesi loppuun purkamalla tämä piilotettu viesti turvallisen infrastruktuurin valinnasta.

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

22	1	12	9	20	19	5		20	21	18	22	1	12	12	9	14	5	14

10	28	18	10	5	19	20	5	12	13	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, joita mahdolliset asiakkaat esittävät virtuaalisten yksityisverkkojen käytöstä.

Q1: Mikä on VPN ja miten se toimii?

Virtuaalinen yksityisverkko (VPN) salaa internetyhteytesi ja reitittää liikenteesi suojatun etäpalvelimen kautta. Tämä peittää julkisen IP-osoitteesi ja rajoittaa sitä, mitä paikallisverkon tarkkailijat ja internetoperaattorisi näkevät VPN-tunnelin kautta kulkevasta liikenteestä.

Q2: Miksi minun pitäisi käyttää VPN:ää?

VPN suojaa digitaalista yksityisyyttäsi, turvaa yhteytesi julkisissa Wi-Fi-verkoissa (kuten kahviloissa tai lentokentillä), voi vähentää toimintaan perustuvaa kuristusta, kun operaattori ei pysty tunnistamaan salatun liikenteen tyyppiä, ohittaa maantieteelliset rajoitukset globaalin sisällön käyttämiseksi ja auttaa suojaamaan etätyön resursseja.

Q3: Tekeekö VPN minusta täysin nimettömän verkossa?

Ei. Vaikka VPN piilottaa IP-osoitteesi ja salaa liikenteen, sinua voidaan silti seurata selainevästeillä, aktiivisilla tileillä (kuten Google tai Facebook), selaimen sormenjäljillä tai jos VPN-palveluntarjoajasi kirjaa tietosi.

Q4: Hidastaako VPN internet-yhteyteni nopeutta?

Kyllä, hieman. Salausprosessi ja fyysinen etäisyys VPN-palvelimeen lisäävät viivettä ja kuormaa. Vaikutus vaihtelee palveluntarjoajan, protokollan, palvelimen etäisyyden, laitteen ja verkko-olosuhteiden mukaan.

Q5: Miten se ansaitsee rahaa?

Tarkista liiketoimintamalli. Tilaukset, freemium-tasot ja datan myynti vaikuttavat kaikki siihen, kuinka paljon voit luottaa VPN:ään, eikä palvelu, joka ei koskaan kerää tietojasi, voi myydä niitä. Lue ensin tietosuojakäytäntö. [1]

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

Tutustu yleisimpiin kysymyksiin ja vastauksiin, joita mahdolliset asiakkaat esittävät virtuaalisten yksityisverkkojen käytöstä.

Q6: Voinko käyttää ilmaista VPN:ää?

Ilmaiset VPN:t voivat perustua mainontaan, rajoitettuihin ominaisuuksiin, käyttöanalytiikkaan, datakattoihin tai muihin tulonhankintamalleihin. Käyttäjien tulisi tarkistaa palveluntarjoajan tietosuojakäytäntö, omistus, auditoinnit ja liiketoimintamalli ennen käyttöä.

Q7: Mikä on "ei lokeja" -käytäntö?

Lokittomuuskäytäntö kuvaa, mitä toiminta- ja yhteystietoja palveluntarjoaja ilmoittaa olevansa säilyttämättä. Tarkka laajuus vaihtelee, joten lukijoiden tulisi tarkistaa käytäntö ja riippumattomien auditointien havainnot.

Q8: Miten valitsen parhaan VPN:n?

Etsi auditoituja lokittomuuskäytäntöjä, vahvoja protokollia (WireGuard, OpenVPN), turvallisia palvelinsijainteja, nopeita yhteyksiä, vain RAM-muistia käyttäviä palvelimia, kill switch -toiminto ja lainkäyttöalue tiedusteluyhteistyöliittoumien (kuten 5/9/14 Eyes) ulkopuolella.

Q9: Voinko käyttää VPN:ää puhelimessani ja älytelevisiossani?

Kyllä. Nykyaikaiset VPN-palveluntarjoajat tarjoavat omat sovellukset iOS:lle, Androidille, macOS:lle, Windowsille, Linuxille ja älytelevisioille sekä reititinasennuksia, jotka suojaavat kaikkia kotiverkkosi laitteita.

Q10: Mikä on kill switch?

Kill Switch on tietoturvaominaisuus, joka katkaisee laitteesi internetyhteyden automaattisesti, jos VPN-yhteys katkeaa. Tämä estää salaamattomien tietojesi tai todellisen IP-osoitteesi vuotamisen.

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

Tutustu virtuaalisten yksityisverkkojen ja suojattujen tunnelointiprotokollien teknisiin ja rakenteellisiin puoliin.

Q1: Mikä ero on WireGuardilla, OpenVPN:llä ja IKEv2:lla?

WireGuard on nykyaikainen, kevyt protokolla (vain noin 4 000 koodiriviä), joka tarjoaa nopeat nopeudet ja lyhyet yhteysajat. OpenVPN on erittäin turvallinen, käytännössä koeteltu avoimen lähdekoodin protokolla. IKEv2 sopii erinomaisesti mobiililaitteille, koska se osaa yhdistää nopeasti uudelleen verkkoa vaihdettaessa.

Q2: Mitä on kaksois-VPN tai Multi-Hop-reititys?

Multi-Hop reitittää liikenteesi kahden tai useamman VPN-palvelimen kautta peräkkäin. Tämä lisää toisen salauskerroksen ja auttaa pitämään todellisen IP-osoitteesi piilossa toiselta hypyltä, jos yksi palvelin vaarantuu.

Q3: Mitä WebRTC-vuoto on ja miten VPN estää sen?

WebRTC on selainprotokolla, joka voi paljastaa oikeat paikalliset ja julkiset IP-osoitteesi, vaikka VPN olisi käytössä. Premium-VPN:t estävät tai väärentävät WebRTC-pyyntöjä pöytäkone- ja mobiilisovelluksissaan sekä selainlaajennuksissaan.

Q4: Mitä pelkkää RAM-muistia käyttävät palvelimet ovat ja miksi niillä on merkitystä?

Perinteiset palvelimet kirjoittavat dataa kiintolevyille, jotka voidaan takavarikoida tai vaarantaa. Pelkkää RAM-muistia käyttävät (levyttömät) palvelimet toimivat kokonaan haihtuvassa muistissa (RAM). Kun palvelin käynnistetään uudelleen tai sammutetaan, muistissa oleva data pyyhkiytyy.

Q5: Miten obfuskointi ohittaa VPN-estot?

Hämäys (eli "Stealth VPN") naamioi VPN-liikenteen paketit tavalliseksi HTTPS-verkkoliikenteeksi (portti 443). Tämä auttaa pääsemään ohi syväpakettitarkastuksen (DPI), jota hallitukset tai koulu- ja toimistoverkot käyttävät VPN-yhteyksien estämiseen.

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

Tutustu virtuaalisten yksityisverkkojen ja suojattujen tunnelointiprotokollien teknisiin ja rakenteellisiin puoliin.

Q6: Mitä jaettu tunnelointi on ja milloin sitä kannattaa käyttää?

Jaetun tunneloinnin avulla voit valita, mitkä sovellukset reitittyvät salatun VPN-tunnelin kautta ja mitkä yhdistävät suoraan internetiin. Käytä sitä reitittääksesi arkaluonteiset pankkisovellukset VPN:n kautta, kun paikalliset pelit yhdistävät suoraan, jolloin vältät VPN:n aiheuttaman viiveen.

Q7: Miten eteenpäin salassapito (Perfect Forward Secrecy) toimii?

PFS varmistaa, että jokaiselle istunnolle luodaan yksilöllinen, väliaikainen salausavain. Vaikka yksityinen avain vaarantuisi tulevaisuudessa, sitä ei voi käyttää menneiden tai tulevien istuntojen purkamiseen, koska ne käyttivät toisistaan riippumattomia avaimia.

Q8: Mitä 5/9/14 Eyes -liittoumat ovat ja miksi minun pitäisi välittää niistä?

Lainkäyttövalta voi vaikuttaa oikeudelliseen menettelyyn, jonka palveluntarjoaja voi kohdata, mutta käytännön yksityisyysriski riippuu myös siitä, mitä tietoja palveluntarjoaja säilyttää, sen teknisestä arkkitehtuurista, omistuksesta, läpinäkyvyysraportoinnista ja auditointihistoriasta.

Q9: Mitä DNS-vuotosuoja on?

DNS-vuodonesto pakottaa laitteesi lähettämään verkkosivujen hakukyselyt (DNS-kyselyt) VPN:n yksityisten, salattujen DNS-palvelimien kautta internetpalveluntarjoajasi palvelimien sijaan. Tämä estää internetpalveluntarjoajaasi seuraamasta, mitä sivustoja vierailet.

Q10: Miksi kannattaa tarkistaa, kuka VPN:ää pyörittää ja tukee?

Maine on tärkeä. Selvitä yrityksen omistajat ja johtajat, etsi julkisia kolmannen osapuolen auditointeja ja tarkista, mitä riippumattomat tietoturva-asiantuntijat ja lehdistö sanovat, ennen kuin luotat siihen. [1]

Osa 11: 10 mielenkiintoista VPN-faktaa ja tosielämän havaintoa

Tutustu näihin erittäin hyödyllisiin, todellisiin tosiasioihin ja oivalluksiin VPN:ien historiasta, markkinoista ja teknologiasta.

1. ENSIMMÄINEN VPN-PROTOKOLLA

PPTP (Point-to-Point Tunneling Protocol), Microsoftin johtaman ryhmän 1990-luvulla kehittämä varhainen VPN-protokolla, katsotaan nykyään turvattomaksi, joten nykyaikaiset VPN:t käyttävät WireGuardia tai OpenVPN:ää. [1]

2. MARKKINA-ARVO

Maailmanlaajuiset VPN-markkinat ovat kasvaneet nopeasti etätyövaatimusten ja yritysten tietoturvatarpeiden lisääntymisen ansiosta.

3. WIREGUARD-VALLANKUMOUS

WireGuardin koodipohja on erittäin virtaviivainen ja suunniteltu tehokkuutta silmällä pitäen, minkä vuoksi sen tietoturvahaavoittuvuudet on helpompi auditoida kuin perinteisten protokollien. [3]

4. TIUKAT TARKASTUSSTANDARDIT

Johtavat VPN-palveluntarjoajat palkkaavat yrityksiä, kuten Deloitten, KPMG:n tai PwC:n, tarkistamaan lokittomuusväitteet, sekä tietoturvayrityksiä, kuten Cure53:n, testaamaan sovelluksensa ja palvelimensa. [4]

5. 5-EYES-LIITTOUMAN ALKUPERÄ

Five Eyes -tiedusteluyhteistyö, johon kuuluvat Yhdysvallat, Britannia, Kanada, Australia ja Uusi-Seelanti, kehittyi liittoutuneiden toisen maailmansodan aikaisesta signaalitiedusteluyhteistyöstä.

6. SYVÄ PAKETTITARKASTUS

Kehittyneet palomuurit käyttävät syväpakettitarkastusta (DPI) verkkopakettien metatietojen analysointiin ja tavallisten VPN-yhteyksien tunnusmerkkien estämiseen.

7. YRITYSKÄYTTÖ

Monet organisaatiot antavat etätyöntekijöilleen VPN:n sisäisten järjestelmien, kuten tietokantojen, käyttöön, minkä vuoksi VPN:t ovat yleinen työpaikan tietoturvatyökalu.

8. HAJAUTETUT VPN:T

Hajautetut VPN:t (dVPN) jakavat liikenteen vertaisten ylläpitämien solmujen verkkoon, mikä vähentää riippuvuutta yhdestä keskitetystä palveluntarjoajasta.

9. TOR VS. VPN-ANONYMITEETTI

VPN tunneloi liikenteen yhden palveluntarjoajan kautta, kun taas Tor (The Onion Router) lähettää liikenteen kolmen vapaaehtoisen välityssolmun (sisääntulo, keski, poistuminen) kautta yksityisyyden maksimoimiseksi. [5]

10. TIETOVUOTOJEN KUSTANNUKSET

VPN:n yhdistäminen zero trust -pääsymalliin, joka tarkistaa jokaisen käyttäjän ja laitteen, auttaa organisaatioita suojaamaan tietoja ja rajoittamaan tietomurtojen vahinkoja.

Tekniset viitteet ja lähteet

Tässä tehtävämonisteessa käytetyt lainatut julkaisut, salausmääritykset ja viralliset asiakirjastandardit.

TIETEELLISET JA ALAN VIITTEET

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

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

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[4] 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

[5] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

Vastausavain: VPN-palveluntarjoajien, tietoturvastandardien, auditointien ja lokikäytäntöjen arviointi

1 **Auditoitu lokikäytäntö** PROTOKOLLAT — **Oikea vastaus: B**

OPETTAJALLE

Riippumattomasti auditoitu lokittomuuskäytäntö on käytännöllisin tapa tarkistaa palveluntarjoajan nollatietoisen yksityisyyden väitteet. Näyttävä markkinointi tai omat väitteet eivät riitä. Lähde: Deloitte Advisory, Cure53 Audit.

2 **WireGuardin ylivoima** VIIVE — **Oikea vastaus: D**

OPETTAJALLE

WireGuard tarjoaa nykyaikaisen, nopean yhteysreitityksen ytimen tilassa ja kompaktin koodipohjan (~4 000 riviä), mikä tekee auditoinneista erittäin tehokkaita. Lähde: IETF Protocol RFC, WireGuard Project.

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

OPETTAJALLE

Ilmaiset VPN:t maksavat silti palvelimista, ja FTC varoittaa, että jotkin VPN-sovellukset jakavat käyttäjätietoja kolmansille osapuolille, esimerkiksi mainosten näyttämiseksi.

4 **Oikeudelliset lainkäyttöalueet** REITITYKSEN HALLINTA — **Oikea vastaus: C**

OPETTAJALLE

Lainkäyttövalta määrää, koskevatko VPN:ää valvontalait, paikalliset tietojen säilytysvelvoitteet ja salaiset viranomaisten haasteet. Lähde: Privacy Rights Clearinghouse.

5 **Kill Switch -suojaus** YKSITYISYYS — **Oikea vastaus: A**

OPETTAJALLE

Kill switch katkaisee heti järjestelmän verkkosovittimen reitityksen, jos tunneli katkeaa, mikä estää oikean IP-osoitteen ja DNS-tietojen paljastumisen. Lähde: IETF Tunnel RFC.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Haittaohjelmien rajoitukset** IP-PEITTO — **Oikea vastaus: Epätosi**

OPETTAJALLE

VPN tarjoaa suojatun salatun yhteyden, mutta se ei skannaa hyötykuormia tai tiedostoja. Haittaohjelmien estämiseen tarvitaan virustorjuntaohjelmisto. Lähde: Deloitte Advisory.

7 **Riippumaton auditointi** NOPEUDET — **Oikea vastaus: Tosi**

OPETTAJALLE

Auditointiraportit varmentavat palvelinohjelmiston määritykset, pelkästään RAM-muistia käyttävän toteutuksen vaatimustenmukaisuuden ja lokitietokantojen puuttumisen. Lähde: Deloitte Advisory, Cure53 Audit.

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

OPETTAJALLE

Palveluntarjoajien on noudatettava kotimaansa lakeja, joihin voi kuulua tietojen säilyttämissääntöjä ja määräyksiä luovuttaa hallussaan olevia tietoja.

9 **Protokollan koodikannan koko** PALOMUURIT — **Oikea vastaus: Tosi**

OPETTAJALLE

Pienempi koodikanta pienentää mahdollista hyökkäyspinta-alaa ja helpottaa tietoturvatiimien työtä protokollan eheyden varmentamisessa. Lähde: WireGuard Project.

10 **Mainosten rahallistaminen** LOKITON — **Oikea vastaus: Tosi**

OPETTAJALLE

Ilman tilausmaksuja ilmaiset VPN:t tukeutuvat tiedonlouhintaan, liikenneprofilointiin ja selaimen mainosinjektioihin tulojen tuottamiseksi. Lähde: EDRi Retention Guidelines.

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. WireGuard	H 2. Tarkastetut lokit	E 3. Oikeudenkäyttöalue	B 4. Kill switch
C 5. Five Eyes	A 6. Ilmainen VPN	D 7. Vain RAM-muistia käyttävät palvelimet	G 8. OpenVPN

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 NO-LOGS	2 WIREGUARD	3 KILL SWITCH	4 LAINKÄYTTÖALUE
5 RAM-ONLY	6 TARKASTUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – ILMAINENVPN
5 D – KILLSWITCH	6 G – RAMPALVELIMET	7 C – LAINKÄYTTÖALUE	8 B – TARKASTUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit WireGuard, Tarkastetut lokit ja Oikeudenkäyttöalue 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

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

RISTIKON RATKAISU

							R						
		W	I	R	E	G	U	A	R	D			
							M			O			
	K						P			P			
L	A	I	N	K	Ä	Y	T	T	Ö	A	L	U	E
	L						L			N			
	L						V			V			
	S		I	L	M	A	I	N	E	N	V	P	N
	W						L			N			
F	I	V	E	E	Y	E	S		I				
	T						M						
	C						E						
	H		T	A	R	K	A	S	T	U	S		

OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: WIREGUARD Moderni, nopea protokolla, jonka koodia on noin 4 000 riviä ja joka on erittäin helppo tarkastaa (9 kirjainta)

5 vaakasuoraan: LAINKÄYTTÖALUE Maantieteellinen alue, joka määrää VPN-palveluntarjoajan oikeudelliset velvoitteet (14 kirjainta)

6 vaakasuoraan: ILMAINENVPN Riskialtis yhteyspalvelu, joka rahoittaa toimintansa usein kirjaamalla ja myymällä selaintietoja (11 kirjainta)

7 vaakasuoraan: FIVEEYES Kansainvälinen tiedustelutietojen jakamisen liitto USA:n, Britannian, Kanadan, Australian ja Uuden-Seelannin välillä (8 kirjainta)

8 vaakasuoraan: TARKASTUS Yksityisyysväite, jonka riippumattomat kolmannen osapuolen tietoturvayritykset ovat todentaneet (9 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: RAMPALVELIMET Laitteistoinfrastruktuuri, joka toimii kokonaan haihtuvalla muistilla ja estää tietojen tallentamisen (13 kirjainta)

3 pystysuoraan: OPENVPN Kypsä, laajasti tarkastettu avoimen lähdekoodin protokolla, jonka koodikanta on paljon WireGuardia suurempi (7 kirjainta)

4 pystysuoraan: KILLSWITCH Suojamekanismi, joka estää internetliikenteen reitityksen, jos suojattu tunneli katkeaa (10 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. U G E I W A R D R — **WIREGUARD**
2. K A Ä I Y U L L T E Ö A T N — **LAINKÄYTTÖALUE**
3. E I F E Y S E V — **FIVEEYES**
4. L E L M E A T V M I R A P — **RAMPALVELIMET**
5. T A A S S K T U R — **TARKASTUS**
6. C S L I T K I W H L — **KILLSWITCH**
7. N I I L E N V P M N A — **ILMAINENVPN**
8. P N N O P V E — **OPENVPN**

SALAKIRJOITUSHAASTEEN AVAIN

"VALITSE TURVALLINEN JÄRJESTELMÄ"

Tapaustutkimusten vastausavain

A Tilanne A: Julkisen verkon turvallisuus

NUUSKINTA JA SALAUS | Sarahin dilemma

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Riskit: Pakettien nuuskinta, tietojen sieppaus ja man-in-the-middle-hyökkäykset. Joku samassa kahvilaverkossa voisi kaapata hänen kirjautumistietonsa tai kotitehtävätiedostonsa.
- VPN-suojaus: Salaa verkkopakettien hyötykuormat, jolloin siepattu tunneliliikenne on lukukelvotonta passiivisille paikallisverkon urkkijoille, kun VPN on määritetty oikein.

B Tilanne B: Estettyjen resurssien käyttäminen

MAANTIETEELLISET ESTOT JA IP-OSOITTEET | Alexin dilemma

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Miksi estetty: Suoratoistopalvelu käyttää maantieteellistä estoa, joka yhdistää matkustajan paikallisen IP-osoitteen hänen fyysiseen maahansa ja estää sen aluekohtaisten lisenssien perusteella.
- Miten VPN auttaa: Hän peittää todellisen sijaintinsa reitittämällä liikenteen kotimaansa palvelimen kautta. Sivusto näkee kotimaan IP-osoitteen, mikä sallii pääsyn.