Nimi: _____ Päivämäärä: _____ Pisteet: _____

Miten piilotat IP-osoitteesi Tehtävämoniste

IP-osoitteiden piilottaminen, sijainnin peittäminen, välityspalvelin, Tor sekä DNS-/WebRTC-vuotojen estäminen

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

- Selitä, miten IP-osoitteet toimivat ja miten ne vuotavat sijainteja.
- Vertaile välityspalvelimia, Toria ja VPN:iä verkko-osoitteiden peittämisessä.
- Tunnista menetelmät DNS- ja WebRTC-vuotojen havaitsemiseen ja estämiseen.
- Ymmärrä, miten verkkosivustot seuraavat käyttäjiä heidän julkisen IP-osoitteensa avulla.
- Arvioi usean hypyn reititystä ja salattuja tunneleita IP-osoitteen suojaamiseksi.

IP-SUOJAUS: TEHTÄVÄMONISTEEN OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: IP-osoitteesi piilottaminen ja vuotojen estäminen. Lopuksi bonustehtävä Nopeat vastaukset.

IP-OSOITTEEN PIILOTTAMINEN (JOHDANTO)

IP-osoitteesi on digitaalinen postiosoite, joka paljastaa fyysisen sijaintisi ja verkkokäyttäytymisesi. IP-osoitteen piilottaminen on ensimmäinen puolustuslinja verkkoseurantaa, kohdennettua profilointia ja sijaintiin perustuvia estoja vastaan. Kun ymmärrät, miten osoitteesi peitetään turvallisesti, voit suojata yksityisyyttäsi verkossa.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mitä laitteen julkinen IP-osoite paljastaa vierailemillesi verkkosivustoille?

- A. Käyttäjän luottokorttinumeron
- B. Likimääräisen sijaintisi ja internetoperaattorisi nimen
- C. Koko paikallisen tiedostohakemiston
- D. Näppäimistön kieliasetukset

2. Mikä menetelmä piilottaa IP-osoitteesi ja salaa kaiken liikenteen koko järjestelmässä?

- A. Tavallinen verkkovälityspalvelin
- B. Selaimen evästeiden tyhjentäminen
- C. Virtuaalinen erillisverkko (VPN)
- D. Natiivin palomuurin poistaminen käytöstä

3. Mikä on ilmaisen verkkovälityspalvelimen käytön merkittävä yksityisyysrajoite?

- A. Se ei salaa tietoliikennettä julkisissa verkoissa
- B. Se edellyttää ulkoisen käyttöjärjestelmän asentamista
- C. Se on täysin laiton Yhdysvalloissa
- D. Se vaatii oman puhelinlinjayhteyden

4. Miten Tor-verkko tarjoaa käyttäjille korkean anonymiteetin?

- A. Nopeuttamalla yhteysnopeuksia
- B. Reitittämällä liikenteen kolmen vapaaehtoisten ylläpitämän välityssolmun kautta
- C. Rekisteröimällä nimesi maailmanlaajuiseen tietokantaan
- D. Rajoittamalla pääsyn vain valtion virastoille

5. Mikä on DNS-vuoto?

- A. Virhe, jossa sähköposti lähetetään väärään osoitteeseen
- B. Kun DNS-kyselyt ohittavat VPN-tunnelin ja menevät internetyhteyden tarjoajalle
- C. Paikallisen reitittimen virtalähteen laitevika
- D. Päivitys paikallisen verkkosovittimen ajuriin

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Välityspalvelin salaa taustalla olevan käyttöjärjestelmän liikenteen aivan kuten VPN.

○ Tosi ○ Epätosi

7 Kysymys 7

7. Torin reititys on erittäin turvallista, mutta hidastaa verkon selausnopeutta.

○ Tosi ○ Epätosi

8 Kysymys 8

8. WebRTC-vuodot voivat paljastaa oikean IP-osoitteesi aktiivisen VPN-istunnon aikana.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Kun VPN on päällä eikä vuotoja ole, internetoperaattorisi ei voi nähdä, millä verkkosivustoilla vierailet.

○ Tosi ○ Epätosi

10 Kysymys 10

10. IP-osoitteesi piilottaminen estää seurannan selaimen sormenjäljen avulla.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Suojatun tunnelin ohittava ja verkkotunnuskyselysi paljastava tilanne on nimeltään _____ .

2. Selainpohjaiset _____ **-viestintärajapinnat voivat vahingossa paljastaa alkuperäisen IP-osoitteesi.**

3. Selainliikennettä uudelleenohjaava mutta pakettien sisältöä salaamaton palvelu on _____ .

4. Monikerroksinen salaus tarjoaa korkean anonymiteetin tason verkossa, jonka nimi on _____ .

5. Operaattorisi antama ja alueesi paljastava julkinen tunnisteesi on _____ .

6. Alueellisten mediaesteiden ohittaminen onnistuu menetelmällä nimeltä _____ .

SANASTON SANAPANKKI

DNS-VUOTO HAITTAOHJELMA IP-OSOITE PROKSIPALVELIN SEURANTA SIJAINTIPEITTO TOR WEBRTC

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Verkkokäsitteiden yhdistäminen

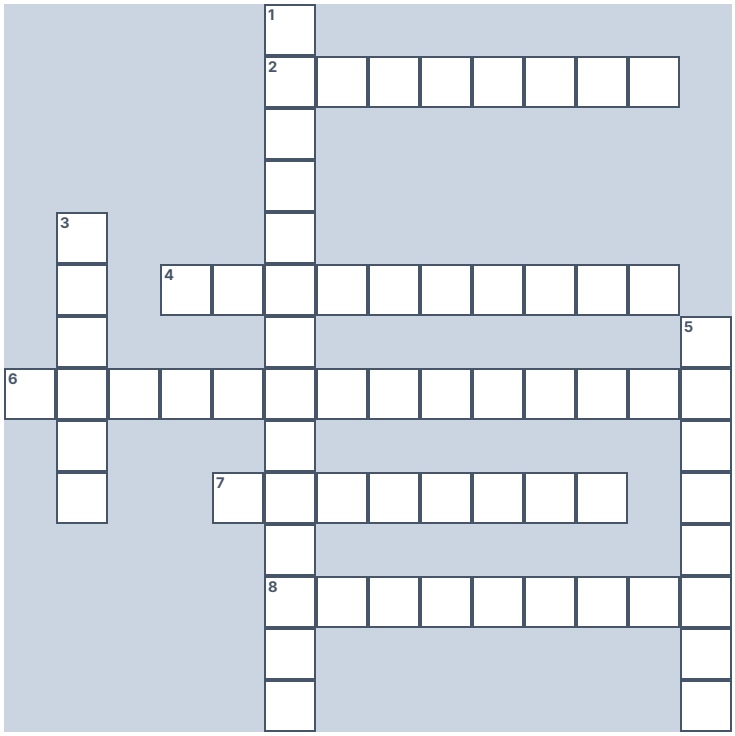
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. IP-osoite	A	Salaa laitteen kaiken liikenteen ja reitittää sen VPN-palvelimen kautta.
☐	2. VPN-tunneli	B	Reitittää datan kolmen vapaaehtoisen palvelimen kautta ja salaa kerrokset jokaisessa vaiheessa.
☐	3. Tor-verkko	C	Yhteyden reititys toisen maan palvelimen kautta maantieteellisten estojen ohittamiseksi.
☐	4. Verkkovälityspalvelin	D	Yksilöllinen numeerinen tunniste, joka yksilöi laiteliitännän internetissä.
☐	5. DNS-vuoto	E	Ohjaa selainliikennettä sovellustasolla ilman järjestelmän salausta.
☐	6. WebRTC-rajapinta	F	Teleyrityksesi tekemä salaamattoman internetliikenteen kohteiden lokitus.
☐	7. Sijainnin peittäminen	G	Kyselyt, jotka ratkeavat VPN-tunnelin ulkopuolella ja paljastavat vierailtujen verkkotunnusten nimet palveluntarjoajalle.
☐	8. Operaattorin suorittama seuranta	H	Selaimen ääni- ja videotoiminto, joka voi ohittaa tunnelit ja paljastaa todelliset IP-osoitteet.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

2. Yksilöllinen numerotunniste, joka tunnistaa laitteen verkkoliitännän internetissä (8)

4. Salaa laitteen kaiken liikenteen ja reitittää sen VPN-palvelimen kautta (10)

6. Ohjaa selainliikenteen sovellustasolla ilman järjestelmätason salausta (14)

7. Internetoperaattorisi suorittama salaamattoman verkkoliikenteen kohteiden kirjaaminen (8)

8. Reitittää tiedot kolmen vapaaehtoisen palvelimen kautta ja salaa kerrokset jokaisessa vaiheessa (9)

PYSTYSUORAAN

1. Yhteyden reitittäminen toisen maan palvelimen kautta maantieteellisten estojen ohittamiseksi (14)

3. Selaimen ääni- ja videoominaisuus, joka voi ohittaa tunnelit ja paljastaa todelliset IP-osoitteet (6)

5. Kyselyt, jotka selvitetään VPN-tunnelin ulkopuolella ja paljastavat vierailtujen verkkotunnusten nimet internetoperaattorille (8)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

2 vaakasuoraan: Yksilöllinen numerotunniste, joka tunnistaa laitteen verkkoliitännän internetissä (8 kirjainta):

4 vaakasuoraan: Salaa laitteen kaiken liikenteen ja reitittää sen VPN-palvelimen kautta (10 kirjainta):

6 vaakasuoraan: Ohjaa selainliikenteen sovellustasolla ilman järjestelmätason salausta (14 kirjainta):

7 vaakasuoraan: Internetoperaattorisi suorittama salaamattoman verkkoliikenteen kohteiden kirjaaminen (8 kirjainta):

8 vaakasuoraan: Reitittää tiedot kolmen vapaaehtoisen palvelimen kautta ja salaa kerrokset jokaisessa vaiheessa (9 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Yhteyden reitittäminen toisen maan palvelimen kautta maantieteellisten estojen ohittamiseksi (14 kirjainta):

3 pystysuoraan: Selaimen ääni- ja videoominaisuus, joka voi ohittaa tunnelit ja paljastaa todelliset IP-osoitteet (6 kirjainta):

5 pystysuoraan: Kyselyt, jotka selvitetään VPN-tunnelin ulkopuolella ja paljastavat vierailtujen verkkotunnusten nimet internetoperaattorille (8 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

IPOSOITE, VPNTUNNELI, TORVERKKO, PROKSIPALVELIN, DNSVUOTO, WEBRTC, SIJAINTIPEITTO, SEURANTA

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. IPOSOITE**
- **B. VPNTUNNELI**
- **C. TORVERKKO**
- **D. PROKSIPALVELIN**
- **E. DNSVUOTO**
- **F. WEBRTC**
- **G. SIJAINTIPEITTO**
- **H. SEURANTA**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Ohjaa selainliikenteen sovellustasolla ilman järjestelmätason salausta.
2. Yhteyden reitittäminen toisen maan palvelimen kautta maantieteellisten estojen ohittamiseksi.
3. Selaimen ääni- ja videoominaisuus, joka voi ohittaa tunnelit ja paljastaa todelliset IP-osoitteet.
4. Yksilöllinen numerotunniste, joka tunnistaa laitteen verkkoliitännän internetissä.
5. Reitittää tiedot kolmen vapaaehtoisen palvelimen kautta ja salaa kerrokset jokaisessa vaiheessa.
6. Internetoperaattorisi suorittama salaamattoman verkkoliikenteen kohteiden kirjaaminen.
7. Kyselyt, jotka selvitetään VPN-tunnelin ulkopuolella ja paljastavat vierailtujen verkkotunnusten nimet internetoperaattorille.
8. Salaa laitteen kaiken liikenteen ja reitittää sen VPN-palvelimen kautta.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. TSOIIPEO
2. OTKVORKER
3. VNDUOOTS
4. ITTEAPNOITI SJI
5. ENIPTNUVLN
6. IPESOLAIVPR LNK
7. TWRCBE
8. REAASTNU

Bonustehtävä: Nopeat vastaukset

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

1	Syitä käyttää VPN:ää matkustaessa			
2	Selaimia, jotka tunnet			
3	Asioita, jotka VPN voi piilottaa			
4	Yksityisyyteen liittyviä sanoja			
5	Sanoja tästä tehtävämonisteesta, jotka haluat muistaa			
6	Asioita, jotka verkkosivusto voi arvata IP-osoitteestasi			
7	Numeroita tai merkkejä IP-osoitteessa			
8	Myyttejä VPN:istä			
9	VPN-palveluja, jotka tunnet			
10	Asioita, jotka internetoperaattorisi näkee			
11	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
12	Asioita, jotka voivat vuotaa todellisen IP-osoitteesi			
13	Syitä piilottaa sijaintisi			
14	Tapoja piilottaa IP-osoitteesi			
15	Laitteita, jotka voivat käyttää VPN:ää			

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 IP-peittämiskoulutuksesi loppuun purkamalla tämä salainen viesti digitaalisten jälkien piilottamisesta.

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

16 9 9 12 15 20 1 15 19 15 9 20 20 5 5 19 9

19 1 12 1 20 21 12 12 1

10 28 18 10 5 19 20 5 12 13 28 12 12 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: Piilottaako verkkovälityspalvelin IP-osoitteeni?

Kyllä, mutta vain sen kautta lähetetylle liikenteelle, yleensä selaimellesi. Useimmat verkkovälityspalvelimet eivät salaa tietojasi, joten internetyhteyden tarjoajasi tai verkon ylläpitäjä voi silti nähdä, mitä lähetät ja vastaanotat.

Q5: Onko IP-osoitteen piilottaminen laillista?

Monissa maissa kyllä, mutta jotkin maat rajoittavat tai kieltävät VPN:t ja muut IP-osoitteen piilottamiseen käytettävät työkalut. IP-osoitteesi piilottaminen ei koskaan tee laittomasta teosta laillista, joten tarkista paikalliset lait ennen käyttöä.

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

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

Q6: Piilottaako Tor IP-osoitteeni?

Kyllä. Tor lähettää liikenteesi kolmen vapaaehtoisen välityssolmun (sisääntulo-, väli- ja ulostulosolmu) kautta, joten verkkosivustot näkevät ulostulosolmun osoitteen, eikä yksikään solmu tiedä sekä sitä, kuka olet, että sitä, minne olet menossa. [1]

Q7: Mitä IP-osoitteeni paljastaa?

Julkinen IP-osoitteesi paljastaa yleensä internetpalveluntarjoajasi ja likimääräisen sijaintisi, kuten maasi tai kaupunkisi. Sivustot voivat myös käyttää sitä yhdistääkseen vierailusi toisiinsa ja soveltaakseen maantieteellisiä estoja.

Q8: Miten tarkistan, että se on piilotettu?

Yhdistä VPN:ääsi, avaa sitten IP-osoitteen tarkistussivusto ja suorita DNS- ja WebRTC-vuototestit. Näytettävien IP-osoitteen ja DNS-palvelinten pitäisi kuulua VPN:lle, ei internetpalveluntarjoajallesi. Jos todellinen IP-osoitteesi näkyy, ota vuotosuojaus käyttöön.

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: Miksi verkkosivustot voivat edelleen seurata minua, kun piilotan IP-osoitteeni?

IP-osoitteesi piilottaminen ei estä selaimen sormenjälkiseurantaa. Seurantapalvelut voivat yhdistää esimerkiksi näytön resoluution, asennetut fontit ja selaimen asetukset tunnisteeksi, ja myös evästeet tai sisäänkirjautuneet tilit voivat tunnistaa sinut, joten käytä myös yksityisyyttä korostavaa selainta. [3]

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: Voiko IPv6-liikenne vuotaa todellisen IP-osoitteeni?

Kyllä, jos VPN tunneloi vain IPv4:n. Laitteesi voi silloin lähettää IPv6-liikennettä tunnelin ulkopuolella ja paljastaa internetpalveluntarjoajan antaman osoitteen. Käytä VPN:ää, joka tunneloi tai estää IPv6:n, ja varmista asia IPv6-vuototestillä.

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: Paljastaako jaettu tunnelointi todellisen IP-osoitteeni?

Kyllä, niiden sovellusten osalta, jotka suljet pois. Tunnelin ulkopuolelle lähetetty liikenne käyttää todellista IP-osoitettasi, ja RFC 8828:n mukaan WebRTC voi paljastaa internetpalveluntarjoajan osoitteen jaetun tunneloinnin VPN:n takana, ellei selain rajoita sitä. [2]

Q7: Mikä on jaettu IP-osoite ja miten se auttaa yksityisyydessä?

Jaetulla IP-osoitteella monet VPN-käyttäjät näkyvät verkossa samalla osoitteella samanaikaisesti. Siksi verkkosivuston on paljon vaikeampi yhdistää yksittäinen vierailu sinuun kuin pelkästään sinun käyttämällä erillisellä IP-osoitteella.

Q8: Näkeekö palveluntarjoajani, että käytän VPN:ää IP-osoitteeni piilottamiseen?

Yleensä kyllä. Palveluntarjoajasi näkee, että yhdistät VPN-palvelimen IP-osoitteeseen, milloin yhdistät ja kuinka paljon dataa lähetät, mutta ei käyttämiäsi verkkosivustoja eikä salatun tunnelin sisältöä.

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: Kumpi on parempi IP-osoitteen piilottamiseen, välityspalvelin vai VPN?

VPN on yleensä parempi. Se piilottaa IP-osoitteesi kaikilta laitteen sovelluksilta ja salaa liikenteen, kun taas verkkovälityspalvelin kattaa tyypillisesti vain selaimen eikä usein lisää salausta.

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.

2. SORMENJÄLKIEN KERÄÄMINEN

IP-osoitteesi piilottaminen ei estä selaimen sormenjälkiseurantaa, joka voi tunnistaa sinut esimerkiksi näytön resoluution ja asennettujen fonttien perusteella. [3]

3. WIREGUARD-VALLANKUMOUS

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

4. WEBRTC-OSOITTEEN PALJASTUMINEN

RFC 8828 varoittaa, että WebRTC voi paljastaa sekä VPN:n julkisen osoitteen että sen palveluntarjoajan osoitteen, jonka kautta VPN toimii, ellei selain rajoita sitä. [2]

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. TOR-PIIRIN UUDELLEENKÄYTTÖ

Tor käyttää samaa piiriä noin kymmenen minuuttia ja rakentaa sitten uuden, mikä tekee selaustoimintasi yhdistämisestä vaikeampaa. [1]

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. [1]

10. VÄLITYSPALVELIMET VS. VPN-TUNNELIT

Verkkovälityspalvelin muuttaa IP-osoitetta, jonka sivusto näkee selainliikenteestäsi, mutta toisin kuin VPN, se ei yleensä salaa liikennettä eikä kata muita laitteesi sovelluksia. [5]

Tekniset viitteet ja lähteet

Tässä tehtävämonisteessa käytetyt lainatut julkaisut, salausmääritykset ja viralliset asiakirjastandardit.

TIETEELLISET JA ALAN VIITTEET

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

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

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

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

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

[5] 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

Vastausavain: IP-osoitteiden piilottaminen, sijainnin peittäminen, välityspalvelin, Tor sekä DNS/WebRTC-vuotojen estäminen

1 Kysymys 1

Oikea vastaus: B

OPETTAJALLE

Mitä laitteen julkinen IP-osoite paljastaa vierailemillesi verkkosivustoille? → Likimääräisen sijaintisi ja internetoperaattorisi nimen

2 VPN-järjestelmäsalaus VIIVE

Oikea vastaus: C

OPETTAJALLE

Toisin kuin välityspalvelimet, jotka ohjaavat vain selaimen liikennettä, VPN luo koko järjestelmän kattavan salatun tunnelin, joka suojaa taustasovelluksia, pelejä ja käyttöjärjestelmän kyselyjä. Lähde: Tor Project Relays, W3C WebRTC API.

3 Välityspalvelimen salauksen puute WI-FI-TURVALLISUUS

Oikea vastaus: A

OPETTAJALLE

Verkkovälityspalvelimet vain välittävät selaimen liikennettä salaamatta pakettien sisältöä, joten verkon ylläpitäjä tai internetyhteyden tarjoaja voi silti jäljittää sisältöliikennettäsi. Lähde: IETF Proxy Vulnerabilities.

4 Kysymys 4

Oikea vastaus: B

OPETTAJALLE

Miten Tor-verkko tarjoaa käyttäjille korkean anonymiteetin? → Reitittämällä liikenteen kolmen vapaaehtoisten ylläpitämän välityssolmun kautta

5 DNS-tunnelin vuodot YKSITYISYYS

Oikea vastaus: B

OPETTAJALLE

DNS-vuoto syntyy, kun verkkotunnusten selvityspyynnöt ohittavat VPN-tunnelin ja menevät suoraan internetoperaattorisi selvittimille, jolloin vierailtujen verkkotunnusten tiedot paljastuvat. Lähde: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Välityspalvelimen rajoitusten yksityiskohdat** IP-PEITTO

Oikea vastaus: Epätosi

OPETTAJALLE

Välityspalvelimet toimivat sovellustasolla, eikä niillä ole VPN-tunnelin järjestelmänlaajuista verkkoajuri-integraatiota. Lähde: IETF Proxy Vulnerabilities.

7 **Kysymys 7**

Oikea vastaus: Tosi

OPETTAJALLE

Liikenteen välittäminen kolmen vapaaehtoisen välityssolmun kautta kerroksittaisella salauksella lisää viivettä, joten Tor on yleensä hitaampi kuin suora yhteys.

8 **Kysymys 8**

Oikea vastaus: Tosi

OPETTAJALLE

WebRTC voi paljastaa paikallisia osoitteita ja joissakin VPN-asetuksissa tunnelin alla olevan internetoperaattorin antaman julkisen IP-osoitteen (RFC 8828).

9 **Kysymys 9**

Oikea vastaus: Tosi

OPETTAJALLE

Ilman DNS- tai WebRTC-vuotoja internetoperaattori näkee vain salatun liikenteen VPN-palvelimelle, ei vierailemiasi sivustoja.

10 **Sormenjälkien keräämisen rajat** LOKITON

Oikea vastaus: Epätosi

OPETTAJALLE

Sormenjälkien keruu kohdistuu laitteen määritysmittareihin (näytön tarkkuus, fontit, laajennukset), jotka pysyvät näkyvissä, vaikka IP-osoite piilotetaan. Lähde: EFF Tracking Evasion.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

D 1. IP-osoite	A 2. VPN-tunneli	B 3. Tor-verkko	E 4. Verkkovälityspalvelin
G 5. DNS-vuoto	H 6. WebRTC-rajapinta	C 7. Sijainnin peittäminen	F 8. Operaattorin suorittama seuranta

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 DNS-VUOTO	2 WEBRTC	3 PROKSIPALVELIN	4 TOR
5 IP-OSOITE	6 SIJAINTIPEITTO		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 D – PROKSIPALVELIN	2 G – SIJAINTIPEITTO	3 F – WEBRTC	4 A – IPOSOITE
5 C – TORVERKKO	6 H – SEURANTA	7 E – DNSVUOTO	8 B – VPNTUNNELI

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit IP-osoite, VPN-tunneli ja Tor-verkko omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

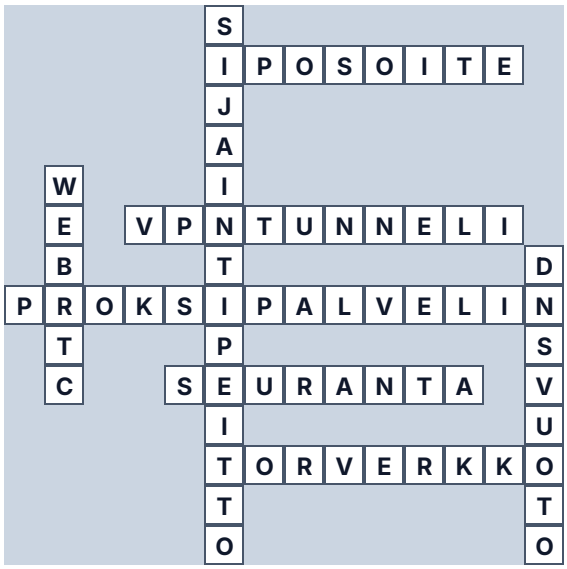
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: IPOSOITE Yksilöllinen numerotunniste, joka tunnistaa laitteen verkkoliitännän internetissä (8 kirjainta)

4 vaakasuoraan: VPNTUNNELI Salaa laitteen kaiken liikenteen ja reitittää sen VPN-palvelimen kautta (10 kirjainta)

6 vaakasuoraan: PROKSIPALVELIN Ohjaa selainliikenteen sovellustasolla ilman järjestelmätason salausta (14 kirjainta)

7 vaakasuoraan: SEURANTA Internetoperaattorisi suorittama salaamattoman verkkoliikenteen kohteiden kirjaaminen (8 kirjainta)

8 vaakasuoraan: TORVERKKO Reitittää tiedot kolmen vapaaehtoisen palvelimen kautta ja salaa kerrokset jokaisessa vaiheessa (9 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: SIJAINTIPEITTO Yhteyden reitittäminen toisen maan palvelimen kautta maantieteellisten estojen ohittamiseksi (14 kirjainta)

3 pystysuoraan: WEBRTC Selaimen ääni- ja videoominaisuus, joka voi ohittaa tunnelit ja paljastaa todelliset IP-osoitteet (6 kirjainta)

5 pystysuoraan: DNSVUOTO Kyselyt, jotka selvitetään VPN-tunnelin ulkopuolella ja paljastavat vierailtujen verkkotunnusten nimet internetoperaattorille (8 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. TSOIIPEO — **IPOSOITE**
2. OTKVORKER — **TORVERKKO**
3. VNDUOOTS — **DNSVUOTO**
4. ITTEAPNOITISJI — **SIJAINTIPEITTO**
5. ENIPTNUVLN — **VPNTUNNELI**
6. IPESOLAIVPRLNK — **PROKSIPALVELIN**
7. TWRCBE — **WEBRTC**
8. REAASTNU — **SEURANTA**

SALAKIRJOITUSHAASTEEN AVAIN

"PIILOTA OSOITTEESI SALATULLA JÄRJESTELMÄLLÄ"

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.