Nimi: _____ Päivämäärä: _____ Pisteet: _____

Miten otat VPN:n käyttöön Tehtävämoniste

VPN:ien määrittäminen Windowsissa, macOS:ssä, Androidissa, iOS:ssä, Linuxissa ja reitittimissä

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

- Vertaile kaupallisia VPN-sovelluksia natiivien asiakkaiden määrittämiseen.
- Määritä VPN-yhteydet reitittimillä koko talon suojaamiseksi.
- Määritä ja hallitse asetustiedostoja, kuten OVPN-tiedostoja tai WireGuard-avaimia.
- Avaa ja suojaa reitittimen tietyt portit tunneliliikennettä varten.
- Tarkista asiakasasennukset DNS-vuototesteillä ja yhteystesteillä.

MÄÄRITYSTEHTÄVÄMONISTEEN OHJEET

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

VPN-MÄÄRITYS (JOHDANTO)

VPN:n määrittäminen manuaalisesti antaa sinulle täyden hallinnan salausavaimiisi ja verkon reititykseen. Määritätpä sitten mobiililaitteesi natiivin asiakasohjelman tai asennat VPN-tunnelin suoraan reitittimeesi, oikea määritys on avain DNS-vuotojen estämiseen ja kaiken verkkoliikenteen suojaamiseen.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. **1. Mikä on helpoin tapa ottaa VPN käyttöön mobiililaitteissa?**
   - A. Lataamalla virallinen VPN-sovellus sovelluskaupasta
   - B. Muokkaamalla käyttöjärjestelmän ydintiedostoja käsin
   - C. Asentamalla mukautettu laiteohjelmisto laitteen rautaan
   - D. Yhdistämällä puhelin pöytätietokoneeseen USB:llä

2. **2. Mikä on etu VPN:n asentamisessa suoraan reitittimeen?**
   - A. Se lisää kaikkien paikallisten laitteiden yhteysnopeuksia
   - B. Se suojaa automaattisesti kaikki yhdistetyt verkkolaitteet
   - C. Se poistaa tarpeen paikallisen internetyhteyden tilausmaksuille
   - D. Se poistaa laitteistoreitittimien tarpeen kokonaan

3. **3. Mitä 'natiivi' VPN-määritys tarkoittaa?**
   - A. Yhteyden muodostaminen käyttöjärjestelmän omilla sisäänrakennetuilla asetuksilla
   - B. VPN:n käyttö vain omassa kotikaupungissa
   - C. Yhdistäminen vain paikallisen maan palvelimiin
   - D. Oman protokollan kirjoittaminen assembly-kielellä

4. **4. Mitä tarvitaan OpenVPN:n manuaaliseen ulkoiseen määritykseen?**
   - A. Mukautetun logon suunnittelu palvelinyhteydelle
   - B. Tuodaan .ovpn-profiili, joka sisältää varmenneavaimet
   - C. Kotireitittimen fyysisen sijainnin vaihtaminen
   - D. Käyttöjärjestelmän palomuurin poistaminen kokonaan käytöstä

5. **5. Miksi ylläpitäjä käyttäisi split tunnelingia määrityksessä?**
   - A. Estää kaiken internetliikenteen kokonaan
   - B. Antaa tiettyjen turvallisten sovellusten ohittaa suojatun tunnelin
   - C. Fyysisen reitittimen jakaminen kahdeksi erilliseksi yksiköksi
   - D. Salauksen poistamiseksi käytöstä ylläpidon valvontaa varten

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Reititin-VPN:n käyttöönotto on yksinkertainen prosessi, joka ei vaadi teknistä osaamista.

- ○ Tosi
- ○ Epätosi

7 Kysymys 7

7. Windowsissa ja macOS:ssä on natiivit asiakasohjelmat, jotka tukevat IKEv2:ta ja L2TP:tä.

- ○ Tosi
- ○ Epätosi

8 Kysymys 8

8. WireGuardin käyttöönotto edellyttää julkisten ja yksityisten avainten luomista.

- ○ Tosi
- ○ Epätosi

9 Kysymys 9

9. VPN-tunneli suojaa paikallisverkkosi tulostimet ja tulostustyöt.

- ○ Tosi
- ○ Epätosi

10 Kysymys 10

10. Älylukot, jotka eivät voi ajaa VPN-sovelluksia, tarvitsevat reititintason VPN:n ollakseen katettuja.

- ○ Tosi
- ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. VPN:n asentaminen verkon yhdyskäytävään eli _____ suojaa älytelevisiot ja pelikonsolit.

2. OpenVPN:n manuaalisessa määrityksessä tuodaan palvelimen asetukset sisältävä _____ .

3. Käyttöjärjestelmän sisäänrakennetut määritykset hyödyntävät järjestelmän omaa VPN-ratkaisua, jota kutsutaan nimellä _____ .

4. WireGuard-todennuksen perustana on kryptografinen julkinen ja yksityinen _____ .

5. Käyttäjäystävällisen asennuksen mahdollistaa palveluntarjoajan virallinen _____ .

6. Nimenselvityskyselyt eivät vuoda, kun käytetään VPN:n omia _____ -palvelimia.

SANASTON SANAPANKKI

AVAINPARI DNS NATIIVIASIAKAS OVPN-PROFIILI REITITIN TUNNELIN JAKO VPN-SOVELLUS YHTEYSLOKIT

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Verkkokäsitteiden yhdistäminen

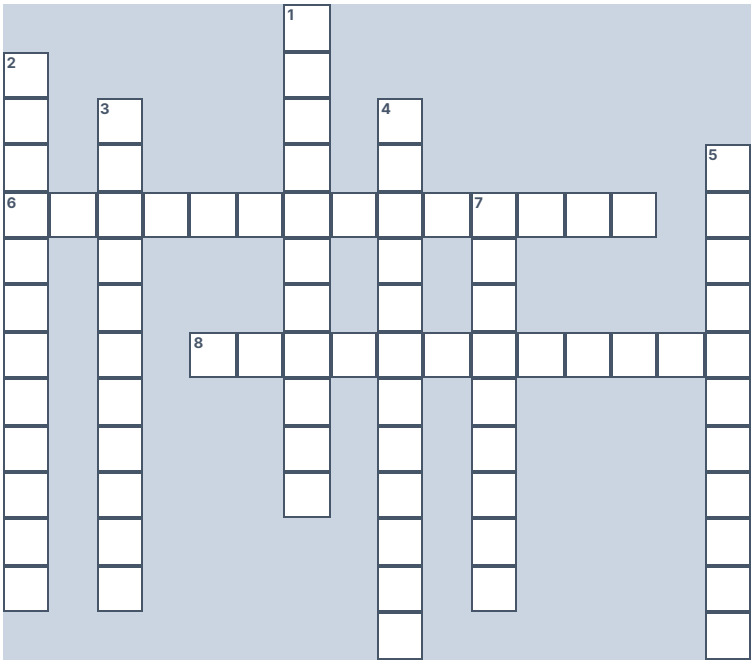
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. VPN-sovellus	A	Yhdyskäytävätason salaus, joka suojaa kaikkia paikallisverkon älylaitteita.
☐	2. Reitittimen VPN	B	Tilauspalvelun tarjoama ohjelmistopaketti helppoa yhden napsautuksen käyttöönottoa varten.
☐	3. Natiivi asiakasohjelma	C	Virhetulosteiden ja asiakkaan tilalokien tarkistaminen epäonnistuneiden asennusten vianmääritystä varten.
☐	4. .OVPN-PROFIILI	D	Liikennereittien erottaminen, jotta tietyt sovellukset voivat ohittaa salatun tunnelin.
☐	5. Avainpari	E	Liikenteen suojaaminen käyttöjärjestelmän omissa asetuksissa asentamatta sovelluksia.
☐	6. Jaettu tunnelointi	F	Verkon selvitysosoitteiden määrittäminen verkkotunnushakujen vuotojen estämiseksi.
☐	7. DNS-palvelimen määritys	G	Kryptografiset tunnisteet (julkinen/yksityinen), joita tarvitaan WireGuard-kättelyjen muodostamiseen.
☐	8. Yhteyslokit	H	OpenVPN-tiedostomuoto, joka sisältää palvelimet, porttiasetukset ja varmenneavaimet.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

6. Liikenteen suojaaminen käyttöjärjestelmän omissa asetuksissa ilman sovellusten asentamista (14)

8. Liikenteen reittien erottelu siten, että tietyt sovellukset ohittavat salatun tunnelin (12)

PYSTYSUORAAN

1. Yhdyskäytävätason salaus, joka suojaa kaikki paikallisverkon älylaitteet (11)

2. OpenVPN-tiedostomuoto, joka sisältää palvelimet, porttiasetukset ja varmenneavaimet (12)

3. Virhetulosteiden ja asiakasohjelman tilalokien tarkistaminen epäonnistuneiden asennusten selvittämiseksi (11)

4. Verkon nimipalvelinosoitteiden määrittäminen verkkotunnushakujen vuotojen estämiseksi (12)

5. Tilauspalvelun tarjoama ohjelmistopaketti helppoa yhden napsautuksen asennusta varten (11)

7. Kryptografiset tunnisteet (julkinen ja yksityinen), joita tarvitaan WireGuard-kättelyjen muodostamiseen (9)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

6 vaakasuoraan: Liikenteen suojaaminen käyttöjärjestelmän omissa asetuksissa ilman sovellusten asentamista (14 kirjainta):

8 vaakasuoraan: Liikenteen reittien erottelu siten, että tietyt sovellukset ohittavat salatun tunnelin (12 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Yhdyskäytävätason salaus, joka suojaa kaikki paikallisverkon älylaitteet (11 kirjainta):

2 pystysuoraan: OpenVPN-tiedostomuoto, joka sisältää palvelimet, porttiasetukset ja varmenneavaimet (12 kirjainta):

3 pystysuoraan: Virhetulosteiden ja asiakasohjelman tilalokien tarkistaminen epäonnistuneiden asennusten selvittämiseksi (11 kirjainta):

4 pystysuoraan: Verkon nimipalvelinosoitteiden määrittäminen verkkotunnushakujen vuotojen estämiseksi (12 kirjainta):

5 pystysuoraan: Tilauspalvelun tarjoama ohjelmistopaketti helppoa yhden napsautuksen asennusta varten (11 kirjainta):

7 pystysuoraan: Kryptografiset tunnisteet (julkinen ja yksityinen), joita tarvitaan WireGuard-kättelyjen muodostamiseen (9 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

VPNSOVELLUS, REITITINVPN, NATIIVIASIAKAS, OVPNPROFIILI, AVAINPARI, TUNNELINJAKO, DNSASETUKSET, YHTEYSLOKIT

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. VPNSOVELLUS**
- **B. REITITINVPN**
- **C. NATIIVIASIAKAS**
- **D. OVPNPROFIILI**
- **E. AVAINPARI**
- **F. TUNNELINJAKO**
- **G. DNSASETUKSET**
- **H. YHTEYSLOKIT**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Verkon nimipalvelinosoitteiden määrittäminen verkkotunnushakujen vuotojen estämiseksi.
2. Liikenteen reittien erottelu siten, että tietyt sovellukset ohittavat salatun tunnelin.
3. Yhdyskäytävätason salaus, joka suojaa kaikki paikallisverkon älylaitteet.
4. Kryptografiset tunnisteet (julkinen ja yksityinen), joita tarvitaan WireGuard-kättelyjen muodostamiseen.
5. Liikenteen suojaaminen käyttöjärjestelmän omissa asetuksissa ilman sovellusten asentamista.
6. Virhetulosteiden ja asiakasohjelman tilalokien tarkistaminen epäonnistuneiden asennusten selvittämiseksi.
7. OpenVPN-tiedostomuoto, joka sisältää palvelimet, porttiasetukset ja varmenneavaimet.
8. Tilauspalvelun tarjoama ohjelmistopaketti helppoa yhden napsautuksen asennusta varten.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. OEUPVLVLNSS
2. IAVTIANKASIASI
3. APNVAIIRA
4. EUSSTTESKDNA
5. VENIINITRPT
6. IPIIRLFOVOPN
7. NJETUIOAKNLN
8. KLTSTYYHIOE

Bonustehtävä: Nopeat vastaukset

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

1	Asioita, jotka tarkistat käyttöönoton jälkeen			
2	Laitteita, jotka voivat käyttää VPN:ää			
3	VPN-palveluja, jotka tunnet			
4	Syitä käyttää VPN:ää matkustaessa			
5	Virheitä, joita ihmiset tekevät käyttöönoton aikana			
6	Sanoja tästä tehtävämonisteesta, jotka haluat muistaa			
7	Asetuksia, jotka otat käyttöön ensin			
8	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
9	Vaiheita VPN:n käyttöönotossa			
10	Paikkoja, joissa käyttäisit VPN:ää			
11	Tapoja tunnistaa väärennetty Wi-Fi-verkko			
12	Asioita, jotka VPN voi piilottaa			
13	Asioita, jotka internetoperaattorisi näkee			
14	Paikkoja, joista löydät apua			
15	Asioita, joita tarvitset päästäksesi alkuun			

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 palvelinmääritysten koulutuksesi loppuun purkamalla tämä piilotettu viesti suojattujen tunnelien käyttöönotosta.

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	19	5	14	14	1		25	8	4	25	19	11	28	25	20	28	22	28

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

16	1	12	22	5	12	21	12	12	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, 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: Mitä tarvitsen aloittamiseen?

Tarvitset voimassa olevan VPN-tilauksen tai oman VPN-palvelimen, tuetun laitteen sekä joko palveluntarjoajan sovelluksen tai manuaalisen asennuksen tiedot: palvelimen osoitteen, protokollan sekä tunnuksesi, avaimesi tai varmenteesi. Useimmat asentavat vain virallisen sovelluksen, kirjautuvat sisään ja napauttavat yhdistä-painiketta.

Q3: Miten määritän VPN:n Windowsissa ilman sovellusta?

Avaa Asetukset > Verkko ja internet > VPN, valitse Lisää VPN ja anna palveluntarjoajan palvelimen nimi, VPN-tyyppi (kuten IKEv2 tai L2TP/IPsec) ja kirjautumistietosi. Valitse sitten Yhdistä.

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 otan macOS:n käyttöön?

Asenna palveluntarjoajan macOS-sovellus tai avaa System Settings > VPN, lisää VPN-määritys, valitse IKEv2, L2TP IPSecin yli tai Cisco IPSec ja anna palveluntarjoajaltasi saatu palvelimen osoite ja tunnistetiedot.

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: Miten käytän .ovpn-tiedostoa?

Asenna OpenVPN-asiakas, tuo .ovpn-profiili palveluntarjoajaltasi tai ylläpitäjältäsi ja yhdistä. Tiedosto sisältää palvelimen osoitteen, portin, UDP- tai TCP-asetuksen ja usein myös varmenteet ja avaimet.

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: Miten otan WireGuardin käyttöön manuaalisesti?

Luo avainpari komennoilla wg genkey ja wg pubkey, jaa julkinen avaimesi palvelimelle ja kirjoita määritystiedosto, jossa on yksityinen avaimesi, vastapuolen julkinen avain, sallitut IP-osoitteet ja päätepiste. Työkalu wg-quick käynnistää yhteyden. [2]

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: Miten määritän VPN:n kotireitittimeeni turvallisesti?

Tarkista, että reitittimesi tukee VPN-asiakastilaa, kirjaudu sen hallintasivulle ja lataa palveluntarjoajan OpenVPN- tai WireGuard-tiedosto. Jotkin reitittimet tarvitsevat ensin laiteohjelmistopäivityksen; sen jälkeen kaikki verkon laitteet käyttävät tunnelia.

Q5: Miten obfuskointi ohittaa VPN-estot?

Hämäys (eli "Stealth VPN") naamioi VPN-liikenteen tavalliseksi HTTPS-liikenteeksi (portti 443). Tämä voi 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 voin tarkistaa, että uusi VPN-määritykseni toimii?

Muodosta yhteys ja avaa IP-osoitteen tarkistussivusto: sen pitäisi näyttää VPN-palvelimen IP-osoite ja sijainti. Suorita DNS- ja WebRTC-vuototestit ja katkaise yhteys hetkeksi varmistaaksesi, että kill switch estää liikenteen.

Q8: Mitä minun pitäisi tarkistaa, jos VPN ei yhdistä asennuksen jälkeen?

Tarkista kirjautumistietosi tai avaimesi, palvelimen osoite sekä se, ettei valittua porttia ja protokollaa ole estetty. Kokeile vaihtaa UDP:n ja TCP:n välillä tai toiseen palvelimeen ja lue sovelluksen yhteyslokeista virheet.

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: Pitäisikö VPN:n käynnistyä automaattisesti?

Yleensä kyllä. Useimmat sovellukset voivat käynnistyä käynnistyksen yhteydessä ja yhdistää automaattisesti tai epäluotettavassa Wi-Fi-verkossa, joten olet suojattu ennen kuin muut sovellukset alkavat lähettää dataa.

Osa 11: 10 mielenkiintoista VPN-faktaa ja tosielämän havaintoa

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

1. NATIIVIASIAKKAAT

Windowsissa ja macOS:ssä on molemmissa sisäänrakennetut VPN-asiakasohjelmat, jotka tukevat IKEv2:ta ja L2TP/IPsecia, joten monet yhteydet voi määrittää ilman erillistä sovellusta.

2. AVAINTEN LUONTI

WireGuardin pika-aloituksessa luodaan yksityinen avain komennolla wg genkey ja johdetaan siitä julkinen avain komennolla wg pubkey. [2]

3. WIREGUARD-VALLANKUMOUS

WireGuardin koodipohja on erittäin virtaviivainen ja suunniteltu tehokkuutta silmällä pitäen, minkä vuoksi sen tietoturvahaavoittuvuudet on helpompi auditoida kuin perinteisten protokollien. [1]

4. PROFIILITIEDOSTOT

.ovpn-profiili niputtaa palvelimen osoitteen, portin, protokollan ja varmenteet, joten yksi tuonti määrittää OpenVPN-yhteyden.

5. OLETUSPORTIT

OpenVPN käyttää yleensä porttia 1194, kun taas WireGuardin viralliset esimerkit käyttävät UDP-porttia 51820; palomuureissa ja reitittimissä nämä portit voi olla tarpeen sallia, jotta tunneli yhdistää.

6. SYVÄ PAKETTITARKASTUS

Syväpakettitarkastus (DPI) voi tunnistaa ja estää tavallisia VPN-protokollia; vaihtaminen OpenVPN:ään TCP-portin 443 kautta tai hämärrettyyn tilaan voi auttaa.

7. REITITTIMEN TUKI

Reitittimessä oleva VPN suojaa kaikkia sen takana olevia laitteita, myös pelikonsoleita ja älytelevisioita, joissa ei voi ajaa VPN-sovellusta, ilman että mitään asennetaan jokaiselle laitteelle.

8. YHTEYDEN YLLÄPITOVIESTIT

NAT:n tai palomuurin takana WireGuardin PersistentKeepalive-asetus, yleensä 25 sekuntia, pitää tunnelin tavoitettavana. [2]

9. TUN/TAP-AJURIT

OpenVPN on suunniteltu toimimaan TUN/TAP-virtuaaliverkkoliittymän kanssa, joka on saatavilla useimmilla alustoilla ja otetaan käyttöön asiakasohjelmaa asennettaessa. [3]

10. JAETTU TUNNELOINTI

Asennuksen aikana jaettu tunnelointi antaa sinun jättää valitut sovellukset tai osoitteet VPN:n ulkopuolelle, mikä auttaa paikallisten tulostimien tai VPN-IP-osoitteita estävien sovellusten kanssa.

Tekniset viitteet ja lähteet

Tässä tehtävämonisteessa käytetyt lainatut julkaisut, salausmääritykset ja viralliset asiakirjastandardit.

TIETEELLISET JA ALAN VIITTEET

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[2] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

[3] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[4] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Vastausavain: VPN:ien määrittäminen Windowsissa, macOS:ssä, Androidissa, iOS:ssä, Linuxissa ja reitittimissä

1 Kysymys 1

Oikea vastaus: A

OPETTAJALLE

Mikä on helpoin tapa ottaa VPN käyttöön mobiililaitteissa? → Lataamalla virallinen VPN-sovellus sovelluskaupasta

2 Reitittimen yhdyskäytäväasetukset

VIIVE

Oikea vastaus: B

OPETTAJALLE

Reitittimen VPN salaa liikenteen yhdyskäytävässä ja suojaa IoT-laitteita, konsoleita ja älylaitteita, joihin ei voi asentaa VPN-sovellusta. Lähde: DD-WRT OpenVPN Clients, Linksys Router Config.

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Windowsissa ja macOS:ssä on sisäänrakennetut asiakasohjelmat protokolliin, kuten IKEv2 ja L2TP/IPsec, joten yhteyden voi määrittää asentamatta lisäohjelmistoja.

4 OpenVPN-profiilin tuonti

REITITYKSEN HALLINTA

Oikea vastaus: B

OPETTAJALLE

Manuaaliset määritykset vaativat.ovpn-profiiliavainten lataamista, jotka sisältävät kohdepalvelimen portit, protokollaparametrit (UDP/TCP) ja salausvarmenteet. Lähde: DD-WRT OpenVPN Clients.

5 Jaetun tunnelin reititys

YKSITYISYYS

Oikea vastaus: B

OPETTAJALLE

Jaetun tunneloinnin avulla käyttäjät voivat reitittää arkaluonteiset työsovellukset salatun tunnelin kautta ja antaa paikallisen suoratoiston tai pelien yhdistää suoraan ilman VPN-kuormaa. Lähde: IETF IKEv2 RFC.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

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

OPETTAJALLE

Reitittimen asetuksissa kirjaudutaan ylläpitosivulle, tarkistetaan VPN-tuki ja ladataan määritystiedostot.

7 **Natiivi käyttöjärjestelmäintegraatio** NOPEUDET — **Oikea vastaus: Tosi**

OPETTAJALLE

Suuret käyttöjärjestelmät sisältävät natiivin protokollatuen, joka varmistaa sujuvan suojatun yhteyden määrityksen. Lähde: Microsoft Native Gateway, Apple Support Profiles.

8 **WireGuardin avainparit** NUUSKINTARISKI — **Oikea vastaus: Tosi**

OPETTAJALLE

WireGuard käyttää epäsymmetrisiä avaimia turvallisten P2P-kättelyjen muodostamiseen salasanojen tai varmenneketjujen sijaan. Lähde: WireGuard CLI Specifications.

9 **Paikallisen liikenteen estot** PALOMUURIT — **Oikea vastaus: Epätosi**

OPETTAJALLE

VPN:t reitittävät yleensä julkista internetliikennettä, ja ne voivat joskus estää pääsyn paikallisverkon tulostimiin, ellei toisin määritetä. Lähde: Microsoft Native Gateway.

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

OPETTAJALLE

Älylukot, jotka eivät voi ajaa VPN-sovelluksia, tarvitsevat reititintason VPN:n ollakseen katettuja.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

B 1. VPN-sovellus	A 2. Reitittimen VPN	E 3. Natiivi asiakasohjelma	H 4. .OVPN-PROFIILI
G 5. Avainpari	D 6. Jaettu tunnelointi	F 7. DNS-palvelimen määritys	C 8. Yhteyslokit

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 REITITIN	2 OVPN-PROFIILI	3 NATIIVIASIAKAS	4 AVAINPARI
5 VPN-SOVELLUS	6 DNS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 G – DNSASETUKSET	2 F – TUNNELINJAKO	3 B – REITITINVPN	4 E – AVAINPARI
5 C – NATIIVIASIAKAS	6 H – YHTEYSLOKIT	7 D – OVPNPROFIILI	8 A – VPNSOVELLUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit VPN-sovellus, Reitittimen VPN ja Natiivi asiakasohjelma omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

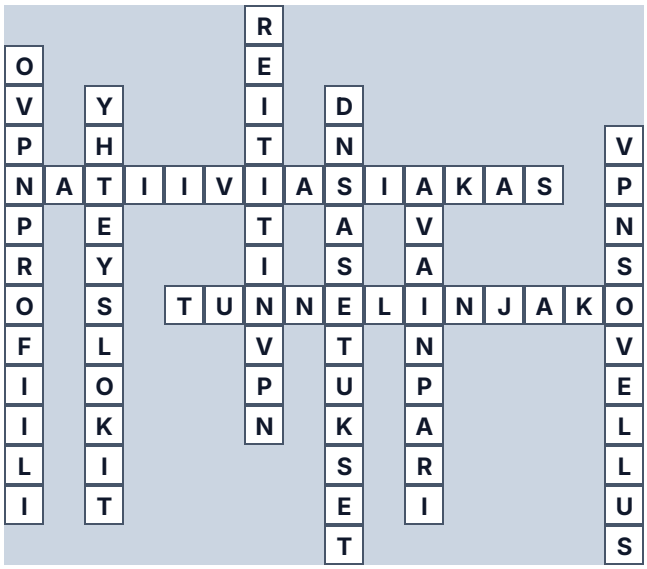
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

6 vaakasuoraan: NATIIVIASIAKAS Liikenteen suojaaminen käyttöjärjestelmän omissa asetuksissa ilman sovellusten asentamista (14 kirjainta)

8 vaakasuoraan: TUNNELINJAKO Liikenteen reittien erottelu siten, että tietyt sovellukset ohittavat salatun tunnelin (12 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: REITITINVPN Yhdyskäytävätason salaus, joka suojaa kaikki paikallisverkon älylaitteet (11 kirjainta)

2 pystysuoraan: OVPNPROFIILI OpenVPN-tiedostomuoto, joka sisältää palvelimet, porttiasetukset ja varmenneavaimet (12 kirjainta)

3 pystysuoraan: YHTEYSLOKIT Virhetulosteiden ja asiakasohjelman tilalokien tarkistaminen epäonnistuneiden asennusten selvittämiseksi (11 kirjainta)

4 pystysuoraan: DNSASETUKSET Verkon nimipalvelinosoitteiden määrittäminen verkkotunnushakujen vuotojen estämiseksi (12 kirjainta)

5 pystysuoraan: VPNSOVELLUS Tilauspalvelun tarjoama ohjelmistopaketti helppoa yhden napsautuksen asennusta varten (11 kirjainta)

7 pystysuoraan: AVAINPARI Kryptografiset tunnisteet (julkinen ja yksityinen), joita tarvitaan WireGuard-kättelyjen muodostamiseen (9 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. OEUPVLVLNSS — **VPNSOVELLUS**
2. IAVTIANKASIASI — **NATIIVIASIAKAS**
3. APNVAIIRA — **AVAINPARI**
4. EUSSTTESKDNA — **DNSASETUKSET**
5. VENIINITRPT — **REITITINVPN**
6. IPIIRLFOVOPN — **OVPNPROFIILI**
7. NJETUIOAKNLN — **TUNNELINJAKO**
8. KLTSTYYHIOE — **YHTEYSLOKIT**

SALAKIRJOITUSHAASTEEN AVAIN

"ASENNA YHDYSKÄYTÄVÄ TURVALLISELLA PALVELULLA"

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.