Nimi: _____ Päivämäärä: _____ Pisteet: _____

WireGuard vs OpenVPN Tehtävämoniste

WireGuard- ja OpenVPN-protokollien, koodikantojen kokojen, nopeuden ja kryptografisten standardien vertailu

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 protokollien koodikannan monimutkaisuutta ja auditointinopeutta.
- Analysoi ytimen tilassa ajamisen suorituskykyhyötyjä.
- Vertaile OpenSSL-salauksia WireGuardin moderniin kryptografiaan.
- Määritä julkisten ja yksityisten avainten parit vertaisten kättelyjä varten.
- Reitittä VPN-liikenne TCP- ja UDP-palomuuriporttien kautta.

PROTOKOLLIEN VERTAILUN TEHTÄVÄMONISTE, OHJEET

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

WIREGUARD VS OPENVPN (JOHDANTO)

VPN-protokollan valinta edellyttää nopeuden ja asetusvaihtoehtojen tasapainottamista. OpenVPN on ollut standardi vuosikymmeniä ja tarjoaa joustavat TCP/UDP-asetukset. WireGuard on moderni korvaaja, joka toimii suoraan ydintilassa vain 4 000 koodirivillä. Protokollien erojen ymmärtäminen on avainasemassa suojattujen verkkojesi optimoinnissa.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. **1. Kuinka suuri on WireGuard-protokollan koodipohja likimäärin?**
   - A. Noin 70 000 riviä
   - B. Yli 100 000 riviä
   - C. Alle 1 000 riviä
   - D. Noin 4 000 riviä

2. **2. Missä käyttöjärjestelmän tilassa WireGuard toimii?**
   - A. Käyttäjätila
   - B. Ytimen tila
   - C. Sovellustila
   - D. Virtuaalitila

3. **3. Mihin salauskirjastoon OpenVPN ensisijaisesti nojaa?**
   - A. ChaCha20-Poly1305
   - B. OpenSSL-salauskirjasto
   - C. Noise-protokollakehys
   - D. Selväkielinen DES-koodaus

4. **4. Mikä on WireGuardin keskeinen suorituskykyetu OpenVPN:ään verrattuna?**
   - A. Nopeammat yhteyden kättelyt ja pienempi viive
   - B. Ohittamalla julkisten IP-osoitteiden tarve
   - C. Sisäänrakennettu natiivi tuki vanhoille puhelinmodeemiyhteyksille
   - D. Nolla akun lisäkuormaa mobiililaitteissa

5. **5. Miten WireGuard todentaa vertaisyhteydet?**
   - A. Vaihtamalla tavallisia käyttäjien salasanoja
   - B. Varmentamalla verkkotunnuksen rekisteröintitodistukset
   - C. Käyttämällä staattisia julkisten ja yksityisten avainten pareja
   - D. Tarkistamalla laitteiden sarjanumerot

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. WireGuardin kompakti koodipohja on merkittävästi helpompi auditoida.

○ Tosi ○ Epätosi

7 Kysymys 7

7. OpenVPN on yleensä nopeampi kuin WireGuard, koska se toimii ytimen tilassa.

○ Tosi ○ Epätosi

8 Kysymys 8

8. OpenVPN on erittäin muokattavissa ja tukee sekä UDP-että TCP-protokollia.

○ Tosi ○ Epätosi

9 Kysymys 9

9. WireGuard käyttää nykyaikaista kryptografiaa, kuten ChaCha20:tä, nopeaan paketinsalaukseen.

○ Tosi ○ Epätosi

10 Kysymys 10

10. WireGuard vaatii monimutkaiset varmennemyöntäjäasetukset todennukseen.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Moderni _____ **-protokolla toimii suoraan käyttöjärjestelmän ytimessä.**

2. Vanha _____ **-protokolla käyttää OpenSSL-kryptokirjastoa.**

3. Kontekstinvaihdon kuormaa vähentää koodin suorittaminen alueella, jonka nimi on _____ **.**

4. OpenVPN toimii alueella nimeltä _____ **ja reitittää paketit virtuaaliliitäntöjen kautta.**

5. WireGuardissa yhteyskumppanien tunnistamiseen käytetään julkisen ja yksityisen avaimen muodostamaa kokonaisuutta, jonka nimi on _____ **.**

6. Pieni koodikanta parantaa ohjelmiston tietoturvaa, koska se tekee koodista helpon tarkastaa; tätä ominaisuutta kuvaa termi _____ **.**

SANASTON SANAPANKKI

AVAINPARI KÄYTTÄJÄTILA OPENSSL OPENVPN TARKASTETTAVUUS TCP JA UDP WIREGUARD YDINTILA

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Verkkokäsitteiden yhdistäminen

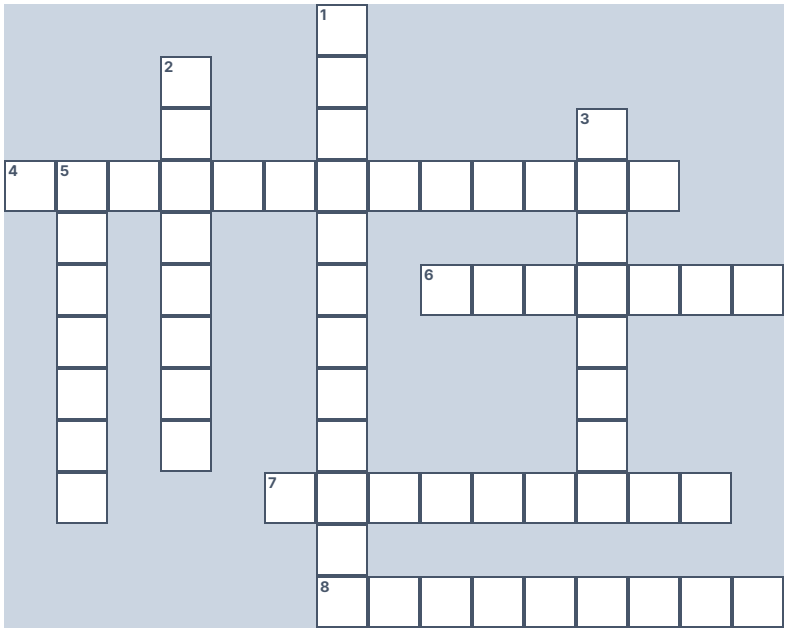
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. WireGuard	A	Suorituspiiri, jossa OpenVPN toimii ja joka aiheuttaa kontekstinvaihtokuormitusta.
☐	2. OpenVPN	B	WireGuardin koodikannan pieni koko, mikä tekee sen tarkastamisesta paljon helpompaa.
☐	3. Ydintila	C	Kryptografinen kirjasto, johon OpenVPN nojaa salausalgoritmien osalta.
☐	4. Käyttäjätila	D	Siirtoprotokollat, joita OpenVPN tukee; WireGuard itse toimii vain UDP:n päällä.
☐	5. 4 000 riviä	E	Käyttöjärjestelmän suoritusalue, jossa WireGuard toimii nopeuden vuoksi.
☐	6. OpenSSL	F	Epäsymmetriset avaimet, joilla WireGuard varmentaa vertaisyhteydet.
☐	7. Avainpari	G	Moderni VPN-protokolla, joka on suunniteltu nopeaksi ja helposti auditoitavaksi koodiltaan.
☐	8. TCP/UDP	H	Vankka vanha protokolla, jossa on suuri ja monimutkainen määrityskoodikanta.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

4. WireGuardin koodikannan pieni koko, joka tekee tarkastuksesta paljon helpompaa (13)

6. Vankka vanhempi protokolla, jonka asetuskoodikanta on laaja ja monimutkainen (7)

7. Moderni VPN-protokolla, joka on suunniteltu suurta nopeutta ja yksinkertaista koodin tarkastusta varten (9)

8. Epäsymmetriset tunnisteet, joilla WireGuard varmentaa vertaisyhteydet (9)

PYSTYSUORAAN

1. Suoritusalue, jossa OpenVPN toimii ja joka aiheuttaa kontekstinvaihdon kuormaa (12)

2. Kuljetusprotokollat, joita OpenVPN tukee; WireGuard itse toimii vain UDP:n päällä (8)

3. Käyttöjärjestelmän suoritusalue, jossa WireGuard toimii nopeuden vuoksi (8)

5. Kryptografinen kirjasto, johon OpenVPN nojaa salausalgoritmeissa (7)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

4 vaakasuoraan: WireGuardin koodikannan pieni koko, joka tekee tarkastuksesta paljon helpompaa (13 kirjainta):

6 vaakasuoraan: Vankka vanhempi protokolla, jonka asetuskoodikanta on laaja ja monimutkainen (7 kirjainta):

7 vaakasuoraan: Moderni VPN-protokolla, joka on suunniteltu suurta nopeutta ja yksinkertaista koodin tarkastusta varten (9 kirjainta):

8 vaakasuoraan: Epäsymmetriset tunnisteet, joilla WireGuard varmentaa vertaisyhteydet (9 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Suoritusalue, jossa OpenVPN toimii ja joka aiheuttaa kontekstinvaihdon kuormaa (12 kirjainta):

2 pystysuoraan: Kuljetusprotokollat, joita OpenVPN tukee; WireGuard itse toimii vain UDP:n päällä (8 kirjainta):

3 pystysuoraan: Käyttöjärjestelmän suoritusalue, jossa WireGuard toimii nopeuden vuoksi (8 kirjainta):

5 pystysuoraan: Kryptografinen kirjasto, johon OpenVPN nojaa salausalgoritmeissa (7 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

WIREGUARD OPENVPN YDINTILA KÄYTTÄJÄTILA KOMPAKTIKOODI OPENSSL AVAINPARI TCPJAUDP

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. WIREGUARD**
- **B. OPENVPN**
- **C. YDINTILA**
- **D. KÄYTTÄJÄTILA**
- **E. KOMPAKTIKOODI**
- **F. OPENSSL**
- **G. AVAINPARI**
- **H. TCPJAUDP**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Kryptografinen kirjasto, johon OpenVPN nojaa salausalgoritmeissa.
2. Käyttöjärjestelmän suoritusalue, jossa WireGuard toimii nopeuden vuoksi.
3. Vankka vanhempi protokolla, jonka asetuskoodikanta on laaja ja monimutkainen.
4. Epäsymmetriset tunnisteet, joilla WireGuard varmentaa vertaisyhteydet.
5. Kuljetusprotokollat, joita OpenVPN tukee; WireGuard itse toimii vain UDP:n päällä.
6. WireGuardin koodikannan pieni koko, joka tekee tarkastuksesta paljon helpompaa.
7. Moderni VPN-protokolla, joka on suunniteltu suurta nopeutta ja yksinkertaista koodin tarkastusta varten.
8. Suoritusalue, jossa OpenVPN toimii ja joka aiheuttaa kontekstinvaihdon kuormaa.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. UGEIWARDR
2. NYADLITI
3. OKIOKDIMTA KOP
4. NIRIAPAVA
5. VNNEOPP
6. ATTIÄLÄKÄJ YT
7. OSSLPNE
8. JCAPTDUP

Bonustehtävä: Nopeat vastaukset

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

1	Syitä valita WireGuard			
2	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
3	Syitä valita OpenVPN			
4	Syitä käyttää VPN:ää matkustaessa			
5	Asioita, jotka internetoperaattorisi näkee			
6	Tapoja tunnistaa väärennetty Wi-Fi-verkko			
7	Myyttejä VPN:istä			
8	Paikkoja, joissa käyttäisit VPN:ää			
9	Nopeita asioita arjessa			
10	Asioita, joilta VPN ei voi suojata sinua			
11	Asioita, jotka helpottavat koodin tarkastamista			
12	Asioita, jotka VPN voi piilottaa			
13	Eroja WireGuardin ja OpenVPN:n välillä			
14	Yksityisyyteen liittyviä sanoja			
15	Salausnimiä, jotka tunnet			

Tarkistuspiste 8: VPN:n tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

SARAH (KAHVILAN OPISKELIJA)

👷 "Hei! Olen kahvilan Wi-Fi-verkossa, ja VPN-sovelluksessani voin valita WireGuardin tai OpenVPN:n. Videopuhelut katkeilevat, kun siirryn kahvilan verkosta puhelimeni hotspotiin ja takaisin. Kumman protokollan valitsen, ja miksi se selviäisi siirtymästä paremmin?"

ALEX (MATKAILIJAOPISKELIJA)

👷 "Olen ulkomailla hotellin verkossa, joka näyttää estävän suurimman osan VPN-liikenteestä. WireGuard ei yhdistä lainkaan, mutta minun pitää päästä käsiksi koulun resursseihin kotimaassani. Mitä todennäköisesti estetään, ja miten OpenVPN voisi auttaa pääsemään läpi?"

Tarkistuspiste 9: Salakirjoituksen purkaminen

Suorita protokollien auditointikoulutuksesi loppuun purkamalla tämä piilotettu viesti ydintilan suorituksesta.

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	28	9	22	9	20	28	15	16	5	14	22	16	14	
14	15	16	5	1	13	16	1	1	14	20	21	14	14	5	12	9	9	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, 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 protokollilla on merkitystä?

Protokolla määrittää, miten VPN rakentaa tunnelinsa, mikä kryptografia suojaa tietojasi ja kuinka nopeasti se yhdistää ja yhdistää uudelleen. WireGuard ja OpenVPN ovat kaksi avoimen lähdekoodin protokollaa, joita useimmat VPN-sovellukset tarjoavat, ja niissä tehdään erilaisia kompromisseja yksinkertaisuuden, nopeuden ja muokattavuuden välillä.

Q3: Onko jompikumpi niistä yksityisempi kuin toinen?

Kumpikaan protokolla ei tee sinusta anonyymia. Molemmat salaavat tunnelin liikenteen vahvoilla salauksilla; yksityisyytesi riippuu pääosin siitä, mitä VPN-palveluntarjoaja kirjaa ja miten se hallitsee avaimia, tilejä ja palvelimia.

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: Ovatko molemmat avointa lähdekoodia?

Kyllä. WireGuard ja OpenVPN:n yhteisöversio julkaisevat lähdekoodinsa, joten riippumattomat tutkijat voivat tarkastaa ne. WireGuardin pieni koodikanta tekee täydellisestä tarkastuksesta paljon nopeamman.

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

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

Q6: Kumpi on nopeampi?

WireGuard on yleensä nopeampi: se toimii ytimessä, käyttää kevyttä ChaCha20-Poly1305-salausta ja suorittaa kättelyt nopeasti. OpenVPN:n lisäkuormitus on suurempi, mutta todelliset nopeudet riippuvat myös palvelimen kuormasta ja etäisyydestä.

Q7: Voivatko molemmat toimia TCP:llä ja UDP:llä?

Ei. OpenVPN voi toimia UDP:n tai TCP:n yli, ja TCP-tila auttaa verkoissa, jotka estävät UDP:n. WireGuard lähettää pakettinsa vain UDP:n yli, joten se voi epäonnistua verkoissa, jotka sallivat vain TCP:n. [4]

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 WireGuardia ja OpenVPN:ää puhelimellani?

Kyllä. WireGuard on alustariippumaton, ja siihen on sovellukset Windowsille, macOS:lle, Linuxille, iOS:lle ja Androidille, ja OpenVPN-asiakkaat löytyvät samoille järjestelmille. Useimmissa VPN-sovelluksissa voit valita kumman tahansa. [1]

Q10: Miksi WireGuard on niin pieni?

WireGuard tukee yhtä kiinteää nykyaikaisten salausalgoritmien joukkoa monien vaihtoehtojen sijaan. Sen Linux-toteutus vaatii alle 4 000 koodiriviä, mikä tekee siitä helpommin auditoitavan kuin suuremmat VPN-koodipohjat. [3]

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 salausalgoritmeja WireGuard käyttää?

WireGuard käyttää salaukseen ChaCha20:tä ja Poly1305:tä, avaintenvaihtoon Curve25519:ää, tiivisteisiin BLAKE2s:ää ja kättelyyn Noise-kehystä. Salausneuvottelua ei ole, joten käyttäjät eivät voi valita heikkoa vaihtoehtoa. [2]

Q3: Mitä salausmenetelmiä ja kirjastoja OpenVPN voi käyttää?

OpenVPN on tiiviisti integroitu OpenSSL-kirjastoon ja käyttää TLS:ää avainten vaihtoon. Ylläpitäjät voivat valita datakanavan salaimia, kuten AES-256-GCM, mikä lisää joustavuutta mutta myös heikkojen asetusten mahdollisuutta. [4]

Q4: Miten kukin protokolla todentaa vertaiset?

WireGuard-vertaiset tunnistavat toisensa staattisten julkisten avainten avulla, aivan kuten SSH-avaimia vaihdettaessa, ja jokainen avain vastaa sallittuja tunneli-IP-osoitteita. OpenVPN tukeutuu yleensä varmennemyöntäjään ja X.509-varmenteisiin, usein yhdistettynä käyttäjätunnukseen ja salasanaan.

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 tapahtuu, kun vaihdan Wi-Fi-yhteydestä mobiiliverkkoon?

WireGuard on yhteydetön: se lähettää paketit uudesta osoitteesta ja tunneli jatkuu nopean kättelyn jälkeen. OpenVPN ylläpitää istuntotilaa, joten verkon vaihtuminen voi vaatia uudelleenyhdistämisen, joka kestää hieman kauemmin.

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: Onko OpenVPN edelleen hyvä valinta, jos WireGuard on nopeampi?

Kyllä. OpenVPN on kypsä ja laajasti käytössä, toimii TCP:n yli, kun UDP on estetty, ja tukee varmennepohjaisia yritysasennuksia. Monet palveluntarjoajat tarjoavat molempia protokollia, jotta käyttäjät voivat vaihtaa, jos toinen on estetty tai hidas.

Q9: Mitä portteja ne käyttävät?

OpenVPN:n vakioportti on 1194, mutta se voidaan siirtää mihin tahansa UDP- tai TCP-porttiin, myös porttiin 443. WireGuard kuuntelee määrityksissä asetettua UDP-porttia; 51820 on sen virallisissa esimerkeissä käytetty portti.

Q10: Kumpi protokolla on helpompi määrittää käsin?

WireGuard on yleensä yksinkertaisempi: luo avainpari, vaihda julkiset avaimet ja luettele sallitut IP-osoitteet. OpenVPN tarvitsee varmenteita, varmennemyöntäjän ja enemmän asetuksia, vaikka .ovpn-profiilit niputtavat ne yhteen tiedostoon.

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:n (Point-to-Point Tunneling Protocol) kehitti toimittajaryhmä, johon kuuluivat muun muassa Microsoft, ja se julkaistiin RFC 2637:nä heinäkuussa 1999 etäkäyttö-VPN-yhteyksien tukemiseksi. [6]

2. KAKSI KULJETUSTAPAA

OpenVPN voi kuljettaa tunnelinsa UDP:n tai TCP:n yli, ja TLS-tilassa sen ohjaus- ja datakanava jakavat yhden portin. [4]

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. MODERNI KRYPTOGRAFIA

WireGuard yhdistää ChaCha20:n, Poly1305:n, Curve25519:n, BLAKE2s:n, SipHash24:n ja HKDF:n Noise-protokollakehyksessä, eikä käyttäjille jää salausvalintoja, joissa voisi erehtyä. [2]

5. OPENSSL OPENVPN:N SISÄLLÄ

OpenVPN on tiiviisti integroitu OpenSSL-kirjastoon ja saa siitä monet salausominaisuutensa, myös avainten vaihdossa käytettävän TLS:n. [4]

6. SYVÄ PAKETTITARKASTUS

Syväpakettitarkastus (DPI) tutkii pakettien sisältöä ja liikennemalleja, ei vain otsikoita, ja jotkin palomuurit käyttävät sitä tavallisten VPN-protokollien tunnistamiseen ja estämiseen.

7. SSH-TYYPPISET AVAIMET

WireGuard-yhteydet muodostetaan vaihtamalla yksinkertaisia julkisia avaimia, aivan kuten SSH-avaimia vaihdetaan, eikä varmennemyöntäjää tarvita. [1]

8. ALUSTARIIPPUMATON

WireGuard julkaistiin ensin Linuxin ytimelle, ja se on nyt saatavilla Windowsille, macOS:lle, BSD:lle, iOS:lle ja Androidille, joten sama protokolla toimii useimmilla laitteilla. [1]

9. ETEENPÄINSALAUS

WireGuard toistaa Noise_IK-kättelynsä muutaman minuutin välein symmetristen istuntoavainten vaihtamiseksi, mikä antaa täydellisen eteenpäin suuntautuvan salassapidon, vaikka pitkäaikainen avain myöhemmin vuotaisi. [2]

10. TUN/TAP-LIITÄNNÄT

OpenVPN on suunniteltu toimimaan TUN/TAP-virtuaaliverkkoliittymän kanssa, joka on saatavilla useimmilla alustoilla ja kuljettaa tunnelin paketit. [4]

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.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.

https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Vastausavain: WireGuard- ja OpenVPN-protokollien, koodikantojen koon ja nopeuden vertailu sekä salausstandardit

1 **WireGuardin koodin koko** PROTOKOLLAT — **Oikea vastaus: D**

OPETTAJALLE

WireGuard on erittäin kompakti ja toimii noin 4 000 koodirivillä. Tämä pitää hyökkäyspinta-alan pienenä ja helpottaa auditointia. Lähde: WireGuard Project.

2 **Ydintilan nopeus** VIIVE — **Oikea vastaus: B**

OPETTAJALLE

Suorittamalla suoraan ytimen tilassa WireGuard välttää kontekstinvaihdon kuormituksen, mikä mahdollistaa suuren läpäisykyvyn. Lähde: WireGuard Project.

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

OPETTAJALLE

OpenVPN on tiiviisti integroitu OpenSSL:ään, joka tarjoaa salausalgoritmeja, kuten AES-GCM:n, ja tekee siitä erittäin muokattavan mutta monimutkaisemman.

4 **Protokollan suorituskyky** REITITYKSEN HALLINTA — **Oikea vastaus: A**

OPETTAJALLE

WireGuard muodostaa kättelyt millisekunneissa ja reagoi välittömästi verkon vaihtumiseen (esim. siirtyminen Wi-Fistä matkapuhelinverkkoon). Lähde: Microsoft Native Gateway, Apple Support.

5 **Epäsymmetrinen salaus** YKSITYISYYS — **Oikea vastaus: C**

OPETTAJALLE

WireGuard käyttää Cryptokey Routing -menetelmää, joka yhdistää julkiset avaimet sallittuihin tunneli-IP-osoitteisiin, samaan tapaan kuin SSH-määrityksissä. Lähde: WireGuard Project.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

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

OPETTAJALLE

WireGuardin Linux-toteutus on alle 4 000 riviä, joten tietoturvatiimit voivat tarkastaa sen paljon nopeammin kuin paljon suuremmat VPN-koodikannat, kuten OpenVPN:n.

7 **Käyttäjätilan viive** NOPEUDET **Oikea vastaus: Epätosi**

OPETTAJALLE

OpenVPN toimii käyttäjätilassa ja siirtää paketteja edestakaisin ytimen virtuaaliliittymän kautta, mikä lisää kontekstinvaihdon kuormaa (ellei käytetä ytimen kuormansiirtoa, kuten OpenVPN DCO:ta). Lähde: DD-WRT custom firmware.

8 **OpenVPN-määritys** NUUSKINTARISKI **Oikea vastaus: Tosi**

OPETTAJALLE

OpenVPN voi toimia TCP:n (luotettavuuteen ja palomuurin ohittamiseen) tai UDP:n (nopeuteen) yli, minkä ansiosta se sopii monimutkaisiin yrityspalomuureihin. Lähde: IETF Cryptographic Protocols.

9 **Moderni salaustekniikka** PALOMUURIT **Oikea vastaus: Tosi**

OPETTAJALLE

WireGuard hylkää vanhat salausalgoritmit ja käyttää nykyaikaisia, turvallisia perusrakenteita kuten ChaCha20:tä ja Poly1305:tä, jotka toimivat nopeasti mobiilisuorittimilla. Lähde: WireGuard Project.

10 **Avainparin yksinkertaistaminen** LOKITON **Oikea vastaus: Epätosi**

OPETTAJALLE

WireGuard ei käytä varmenteita tai monimutkaisia varmennemyöntäjähierarkioita, vaan tukeutuu vertaisten välillä vaihdettaviin yksinkertaisiin julkisen ja yksityisen avaimen pareihin. Lähde: WireGuard Project.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

G 1. WireGuard	H 2. OpenVPN	E 3. Ydintila	A 4. Käyttäjätila
B 5. 4 000 riviä	C 6. OpenSSL	F 7. Avainpari	D 8. TCP/UDP

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 WIREGUARD	2 OPENVPN	3 YDINTILA	4 KÄYTTÄJÄTILA
5 AVAINPARI	6 TARKASTETTAVUUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 F – OPENSSL	2 C – YDINTILA	3 B – OPENVPN	4 G – AVAINPARI
5 H – TCPJAUDP	6 E – KOMPAKTIKOODI	7 A – WIREGUARD	8 D – KÄYTTÄJÄTILA

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit WireGuard, OpenVPN ja Ydintila omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

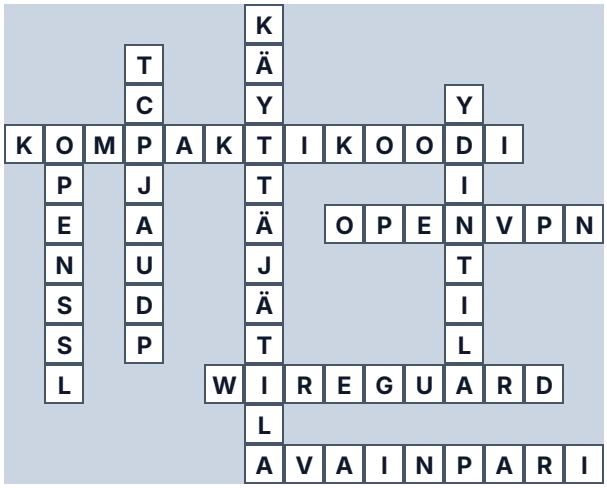
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

4 vaakasuoraan: KOMPAKTIKOODI WireGuardin koodikannan pieni koko, joka tekee tarkastuksesta paljon helpompaa (13 kirjainta)

6 vaakasuoraan: OPENVPN Vankka vanhempi protokolla, jonka asetuskoodikanta on laaja ja monimutkainen (7 kirjainta)

7 vaakasuoraan: WIREGUARD Moderni VPN-protokolla, joka on suunniteltu suurta nopeutta ja yksinkertaista koodin tarkastusta varten (9 kirjainta)

8 vaakasuoraan: AVAINPARI Epäsymmetriset tunnisteet, joilla WireGuard varmentaa vertaisyhteydet (9 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: KÄYTTÄJÄTILA Suoritusalue, jossa OpenVPN toimii ja joka aiheuttaa kontekstinvaihdon kuormaa (12 kirjainta)

2 pystysuoraan: TCPJAUDP Kuljetusprotokollat, joita OpenVPN tukee; WireGuard itse toimii vain UDP:n päällä (8 kirjainta)

3 pystysuoraan: YDINTILA Käyttöjärjestelmän suoritusalue, jossa WireGuard toimii nopeuden vuoksi (8 kirjainta)

5 pystysuoraan: OPENSSL Kryptografinen kirjasto, johon OpenVPN nojaa salausalgoritmeissa (7 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. UGEIWARDR — **WIREGUARD**
2. NYADLITI — **YDINTILA**
3. OKIOKDIMTAKOP — **KOMPAKTIKOODI**
4. NIRIAPAVA — **AVAINPARI**
5. VNNEOPP — **OPENVPN**
6. ATTIÄLÄKÄJYT — **KÄYTTÄJÄTILA**
7. OSSLPNE — **OPENSSL**
8. JCAPTDUP — **TCPJAUDP**

SALAKIRJOITUSHAASTEEN AVAIN

"PÄIVITÄ OPENVPN NOPEAMPAAN TUNNELIIN"

Tapaustutkimusten vastausavain

A Tilanne A: Protokollan valinta

NUUSKINTA JA SALAUS | Sarahin dilemma

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Suositus: WireGuard. Sen kevyt, yhteydetön rakenne antaa tunnelin toipua nopeasti, kun hänen verkkonsa vaihtuu, ja ChaCha20-Poly1305 pitää salauksen nopeana.
- Tietoturva: Molemmat protokollat salaavat hänen liikenteensä kahvilan Wi-Fi-verkossa, joten kumpikin suojaa hänen kirjautumisiaan oikein määritettynä; valinta vaikuttaa lähinnä nopeuteen ja vakauteen.

B Tilanne B: VPN-estojen ohittaminen

MAANTIETEELLISET ESTOT JA IP-OSOITTEET | Alexin dilemma

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Miksi estetty: WireGuard käyttää vain UDP:tä, ja hotellin palomuuri todennäköisesti estää UDP:n tai tunnistaa WireGuard-paketit suodatuksella tai syvällä pakettitarkastuksella (DPI).
- Miten OpenVPN auttaa: Se voi toimia TCP:n yli, myös HTTPS:n käyttämän portin 443 kautta, jota hotellien palomuurit harvoin estävät kokonaan, koska verkkoselaus riippuu siitä.