Nimi: _____ Päivämäärä: _____ Pisteet: _____

VPN.comin VPN-opas Tehtävämoniste

Käytännön harjoituksia verkkoprotokollista, tunneloinnista ja tietoturvakontrolleista.

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 datan tunneloinnin ja kapseloinnin käsite.
- Tunnista tavalliset protokollamääritykset ja kaistanleveysvaatimukset.
- Analysoi palomuurien ja maantieteellisen eston roolia internetin reitityksessä.
- Ymmärrä, miten palveluntarjoajat seuraavat salaamatonta selailua ja miten VPN estää sen.
- Erota toisistaan palvelimen sijainnin ja lainkäyttövallan toiminnalliset rajat.

VPN-OPAS, OHJEET

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

MIKÄ ON VPN? (JOHDANTO)

Virtuaalinen yksityisverkko on enemmän kuin pelkkä yksityisyyskytkin. Se on salattu tunneli, joka reitittää internetliikenteesi etäpalvelimen kautta. Tämä piilottaa IP-osoitteesi, estää internetoperaattoriasi kokoamasta lokeja verkkotoimistasi ja suojaa tietosi julkisissa verkoissa. Terminologian ymmärtäminen on olennaista digitaalisen turvallisuuden ylläpitämiseksi.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mikä on VPN-protokolla?

- A. Kaapelien liittämiseen käytettävä laite.
- B. Sääntöjoukko, joka määrittää, miten data salataan ja lähetetään.
- C. Selaimen laajennus, joka estää mainoksia.
- D. Internetpalveluntarjoajayritys.

2. Jos VPN-yhteytesi tuntuu hitaalta, mikä on todennäköisin syy?

- A. VPN-palvelin on liian kaukana tai ylikuormitettu.
- B. Näytön resoluutio on asetettu liian suureksi.
- C. Olet poistanut selaimen evästeet käytöstä.
- D. Näppäimistön asettelu on määritetty väärin.

3. Miksi VPN:n käyttöä suositellaan vahvasti julkiseen Wi-Fi-verkkoon yhdistettäessä?

- A. Se tekee Wi-Fi-yhteydestä ilmaisen.
- B. Se laajentaa reitittimen kantamaa.
- C. Se salaa liikenteen, jotta samassa verkossa olevat hakkerit eivät pääse siihen käsiksi.
- D. Se poistaa roskapostin automaattisesti.

4. Mikä seuraavista kuvaa maantieteellistä eston (geoblock)?

- A. Työkalu, joka mittaa fyysistä etäisyyttä palvelimeen.
- B. Rajoitus, joka estää pääsyn sivustolle sijainnin perusteella.
- C. Protokolla paikallista tiedostojen pakkaamista varten.
- D. Varmuuskopioiden tallennusmekanismi.

5. Mitä internetyhteyden tarjoajasi (ISP) näkee, kun käytät VPN:ää?

- A. Hakusanat ja katsomasi verkkosivujen sisältö.
- B. Että olet yhteydessä VPN:ään, mutta ei liikenteen yksityiskohtia.
- C. Ei mitään tietoa, ei edes sitä, että olet verkossa.
- D. Paikallisella kiintolevylläsi olevat tiedostot ja valokuvat.

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Sijainnin peittäminen

6. VPN peittää laitteesi julkisen IP-osoitteen, mikä estää kolmannen osapuolen verkkosivustoja tunnistamasta fyysistä sijaintiasi helposti.

○ Tosi ○ Epätosi

7 VPN:n vaikutus nopeuteen

7. VPN-yhteyden käyttöönotto tekee perusinternetnopeudestasi kaksi kertaa nopeamman kuin yhteytesi ilman VPN:ää.

○ Tosi ○ Epätosi

8 Julkisen Wi-Fin nuuskinta

8. Jos käytät suojaamatonta julkista Wi-Fi-verkkoa ilman VPN:ää, muut samassa verkossa olevat käyttäjät voivat mahdollisesti siepata salaamattoman liikenteesi.

○ Tosi ○ Epätosi

9 Palomuurit ja estetyt yhteydet

9. Verkonvalvojat voivat määrittää palomuurit havaitsemaan ja estämään lähtevät VPN-yhteystunnelit.

○ Tosi ○ Epätosi

10 Tiukat lokittomuuskäytännöt

10. Tiukka ”no-logs”-käytäntö tarkoittaa, että VPN-palveluntarjoaja on lain mukaan velvoitettu tallentamaan hakukyselysi ja vierailemasi linkit vähintään 30 päivän ajaksi.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Liikenteesi suojaamiseksi VPN käärii datapakettisi toisen protokollan sisään; prosessin nimi on _____ .

2. Jos suoratoiston aikana lataus on hidasta, syynä voi olla rajallinen verkon _____ .

3. Vain tietyssä maassa saatavilla oleva suoratoistopalvelu rajoittaa maailmanlaajuisia käyttäjiä esteellä, jonka nimi on _____ .

4. Salaus- ja yhteysparametrit määrittelevät yhteyssäännöt ovat VPN:n _____ .

5. Tietokoneesi paikallinen verkkoliikennettä valvova ja vaaralliset yhteydet estävä suojajärjestelmä on _____ .

6. Kun muodostat VPN-yhteyden, datasi reititetään etätietokoneen kautta julkisen IP-osoitteesi piilottamiseksi; tämä etätietokone on _____ .

SANASTON SANAPANKKI

ALUEESTO KAISTANLEVEYS OPERAATTORI PALOMUURI PALVELIN
PROTOKOLLA TUNNELOINTI YKSITYISYYS

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Verkkokäsitteiden yhdistäminen

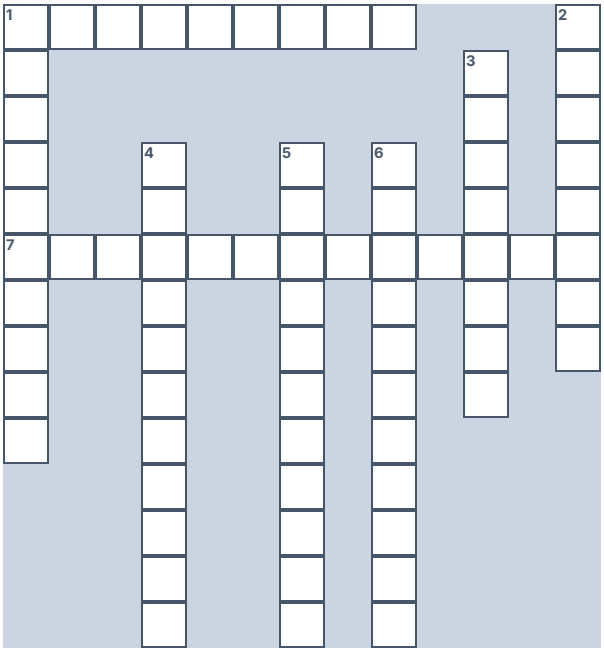
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. Tunnelointi	A	Sääntöjoukko, joka määrittää, miten tietoja siirretään verkossa.
☐	2. Protokolla	B	Tiedonsiirron suurin nopeus yhteyden yli.
☐	3. Kaista	C	Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella.
☐	4. Palvelin	D	Suojausjärjestelmä, joka valvoo ja estää luvattoman liikenteen.
☐	5. Maantieteellinen esto	E	Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi.
☐	6. Palomuuri	F	Tila, jossa ei ole seurannan tai julkisen valvonnan kohteena.
☐	7. Yksityisyys	G	Internetpalveluntarjoaja, joka kuljettaa liikennettäsi ja voi nähdä salaamattoman toiminnan.
☐	8. Internetoperaattori	H	Datapakettien kääriminen toisen paketin sisään turvallista siirtoa varten.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

1. Tietoturvajärjestelmä, joka valvoo ja estää luvattoman liikenteen (9)

7. Yhteyden suurin tiedonsiirtonopeus (13)

PYSTYSUORAAN

1. Sääntöjoukko, joka määrittää, miten dataa siirretään verkossa (10)

2. Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella (8)

3. Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi (8)

4. Tila, jossa ei ole seurantaa eikä julkista valvontaa (11)

5. Datapakettien käärimistä toisen paketin sisään turvallista siirtoa varten (11)

6. Internet-palveluntarjoaja, joka kirjaa liikenteesi lokiin, ellei sitä ole salattu (11)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

1 vaakasuoraan: Tietoturvajärjestelmä, joka valvoo ja estää luvattoman liikenteen (9 kirjainta):

7 vaakasuoraan: Yhteyden suurin tiedonsiirtonopeus (13 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Sääntöjoukko, joka määrittää, miten dataa siirretään verkossa (10 kirjainta):

2 pystysuoraan: Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella (8 kirjainta):

3 pystysuoraan: Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi (8 kirjainta):

4 pystysuoraan: Tila, jossa ei ole seurantaa eikä julkista valvontaa (11 kirjainta):

5 pystysuoraan: Datapakettien käärimistä toisen paketin sisään turvallista siirtoa varten (11 kirjainta):

6 pystysuoraan: Internet-palveluntarjoaja, joka kirjaa liikenteesi lokiin, ellei sitä ole salattu (11 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

TUNNELOINTI PROTOKOLLA KAISTANLEVEYS PALVELIN ALUEESTO
PALOMUURI YKSITYISYYS OPERAATTORI

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. TUNNELOINTI**
- **B. PROTOKOLLA**
- **C. KAISTANLEVEYS**
- **D. PALVELIN**
- **E. ALUEESTO**
- **F. PALOMUURI**
- **G. YKSITYISYYS**
- **H. OPERAATTORI**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Tila, jossa ei ole seurantaa eikä julkista valvontaa.
2. Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella.
3. Sääntöjoukko, joka määrittää, miten dataa siirretään verkossa.
4. Tietoturvajärjestelmä, joka valvoo ja estää luvattoman liikenteen.
5. Yhteyden suurin tiedonsiirtonopeus.
6. Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi.
7. Internet-palveluntarjoaja, joka kirjaa liikenteesi lokiin, ellei sitä ole salattu.
8. Datapakettien käärimistä toisen paketin sisään turvallista siirtoa varten.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. **EOTULITNNIN**
2. **YTAAIKENSE VLS**
3. **ELAESOTU**
4. **IYSYSTYSYKI**
5. **LKARTOOPLO**
6. **INVLPEAL**
7. **UPRIUOAML**
8. **OTIAEOAPRT R**

Bonustehtävä: Nopeat vastaukset

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

1	Asioita, jotka yhdistät sanaan "tunneli"			
2	Asioita, joita opettaisit perheellesi VPN:istä			
3	Asioita verkkosivustolla, jotka voivat seurata sinua			
4	Myyttejä VPN:istä			
5	Sanoja tästä tehtävämonisteesta, jotka haluat muistaa			
6	Laitteita, jotka voivat käyttää VPN:ää			
7	Asioita, joilta VPN ei voi suojata sinua			
8	Maita, joissa haluaisit "vierailla" verkossa			
9	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
10	Tapoja tunnistaa väärennetty Wi-Fi-verkko			
11	Kysymyksiä, joita sinulla on VPN:istä			
12	VPN-palveluja, jotka tunnet			
13	Yksityisyyteen liittyviä sanoja			
14	Asioita, jotka VPN voi piilottaa			
15	Syitä käyttää VPN:ää kahvilassa			

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

VPN salaa liikenteesi sen suojaamiseksi. Käytä alla olevaa kirjain–numero-avainta purkaaksesi kyberturvallisuusviestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Å=27 Ä=28 Ö=29

19	21	15	10	1	1									
25	11	19	9	20	25	9	19	25	25	20	5	19	9	
20	21	18	22	1	12	12	9	19	5	12	12	1		
20	21	14	14	5	12	9	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: 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: Onko VPN:n käyttö laillista?

VPN:n käyttö on laillista monissa maissa, mutta jotkin lainkäyttöalueet rajoittavat, sääntelevät tai estävät VPN-palveluja. Käyttäjien tulisi tarkistaa voimassa olevat paikalliset lait ennen käyttöä. Lisätietoja saat VPN.comin laillisuusoppaista.

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. [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: 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 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 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: Voiko VPN ohittaa internetpalveluntarjoajan nopeuden rajoituksen?

Joskus. VPN voi auttaa, kun internetpalveluntarjoaja hidastaa valikoiden tunnistettavia toimintoja, mutta se ei ratkaise verkon ruuhkaa, datarajoituksia, tilikohtaisia nopeusrajoituksia tai heikkoa verkon laatua.

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. 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 ulkopuolisia auditoijia (kuten Cure53 tai PwC) tekemään riippumattomia koodikatselmuksia ja varmistamaan, etteivät ne kirjaa käyttäjien toimintaa.

5. 5-EYES-LIITTOUMAN ALKUPERÄ

Five Eyes -liittouma kasvoi vuoden 1946 UKUSA-signaalitiedustelusopimuksesta Yhdysvaltojen ja Britannian välillä, ja siihen liittyivät myöhemmin Kanada, Australia ja Uusi-Seelanti.

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. YRITYSKÄYTTÖ

Suuri osa yritysten työntekijöistä maailmanlaajuisesti käyttää suojattuja VPN-yhteyksiä kirjautuakseen sisäisiin tietokantoihin, mikä tekee siitä keskeisen tietoturvastandardin.

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 ja poistuminen) kautta, jolloin yksikään solmu ei tiedä molempia päitä.

10. TIETOVUOTOJEN KUSTANNUKSET

Nollaluottamusmallin mukaisen suojatun käyttöoikeusmallin käyttö VPN:n kanssa auttaa organisaatioita suojaamaan immateriaalioikeuksia ja lieventämään tietomurtojen taloudellisia vaikutuksia.

Tekniset viitteet ja lähteet

Tässä tehtävämonisteessa käytetyt lainatut julkaisut, salausmääritykset ja viralliset asiakirjastandardit.

AKATEEMINEN KIRJALLISUUS JA TIETOTURVASTANDARDIT

[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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.

https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

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

TEKNISTEN STANDARDIEN YHTEENVETO

- Kapselointistandardit: RFC 4301 määrittelee suojatun IPsec/L2TP-internetpakettien reitityksen.
- Palveluntarjoajan seuranta: DNS-kyselyjen reititys salatun VPN-tunnelin kautta voi vähentää paikallisen palveluntarjoajan näkyvyyttä DNS-liikenteeseen.
- Palomuurin hallintaprotokollat: hämärretyt stealth-paketit ohittavat syväpakettisuodattimet.

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

Oikea vastaus: B

OPETTAJALLE

VPN-protokolla määrittelee säännöt tunnelin rakentamiselle ja datan salaamiselle; muut vaihtoehdot kuvaavat kaapeleita, mainosten estäjiä ja internetoperaattoreita.

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

Etäisyys lisää viivettä, ja ylikuormitetulla palvelimella on vähemmän jaettavaa kapasiteettia; näytön tarkkuus, evästeet ja näppäimistöasettelu eivät vaikuta yhteysnopeuteen.

3 Kysymys 3

Oikea vastaus: C

OPETTAJALLE

Avoimissa verkoissa muut voivat siepata salaamattomia paketteja; VPN salaa liikenteen, joten siepattua dataa ei voi lukea.

4 Kysymys 4

Oikea vastaus: B

OPETTAJALLE

Maaesto yhdistää vierailijan julkisen IP-osoitteen sijaintitietokantaan ja estää pääsyn sallittujen alueiden ulkopuolelta.

5 Kysymys 5

Oikea vastaus: B

OPETTAJALLE

Internetoperaattori näkee, että lähetät salattua dataa VPN-palvelimelle, mutta ei sitä, millä sivustoilla vierailet tai mitä haet.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

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

OPETTAJALLE

Verkkosivustot näkevät sinun IP-osoitteesi sijaan VPN-palvelimen IP-osoitteen, mikä piilottaa likimääräisen sijaintisi niiltä.

7 **Kysymys 7** **Oikea vastaus: Epätosi**

OPETTAJALLE

Salaus ja ylimääräinen hyppy VPN-palvelimelle yleensä hidastavat nopeutta hieman; VPN ei voi kaksinkertaistaa perusyhteytesi nopeutta.

8 **Kysymys 8** **Oikea vastaus: Tosi**

OPETTAJALLE

Suojaamattomassa Wi-Fi-verkossa pakettien nuuskintatyökalut voivat siepata salaamatonta liikennettä, kuten ilman HTTPS:ää lähetettyjä kirjautumistietoja.

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

OPETTAJALLE

Ylläpitäjät voivat estää tunnetut VPN-portit, kuten OpenVPN:n 1194, tai käyttää syväpakettitarkastusta VPN-liikenteen havaitsemiseen.

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

OPETTAJALLE

Lokittomuuskäytäntö on palveluntarjoajan lupaus olla säilyttämättä tietoja toiminnastasi; mikään laki ei velvoita VPN-palveluja tallentamaan hakuja 30 päiväksi.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

H 1. Tunnelointi	A 2. Protokolla	B 3. Kaista	E 4. Palvelin
C 5. Maantieteellinen esto	D 6. Palomuuri	F 7. Yksityisyys	G 8. Internetoperaattori

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 TUNNELOINTI	2 KAISTANLEVEYS	3 ALUEESTO	4 PROTOKOLLA
5 PALOMUURI	6 PALVELIN		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 G – YKSITYISYYS	2 E – ALUEESTO	3 B – PROTOKOLLA	4 F – PALOMUURI
5 C – KAISTANLEVEYS	6 D – PALVELIN	7 H – OPERAATTORI	8 A – TUNNELOINTI

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit Tunnelointi, Protokolla ja Kaista omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

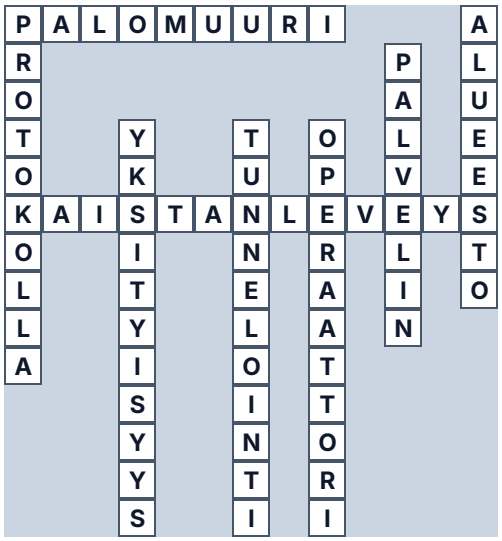
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



VAAKASUORAAN

1 vaakasuoraan: PALOMUURI Tietoturvajärjestelmä, joka valvoo ja estää luvattoman liikenteen (9 kirjainta)

7 vaakasuoraan: KAISTANLEVEYS Yhteyden suurin tiedonsiirtonopeus (13 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: PROTOKOLLA Sääntöjoukko, joka määrittää, miten dataa siirretään verkossa (10 kirjainta)

2 pystysuoraan: ALUEESTO Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella (8 kirjainta)

3 pystysuoraan: PALVELIN Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi (8 kirjainta)

4 pystysuoraan: YKSITYISYYS Tila, jossa ei ole seurantaa eikä julkista valvontaa (11 kirjainta)

5 pystysuoraan: TUNNELOINTI Datapakettien käärimistä toisen paketin sisään turvallista siirtoa varten (11 kirjainta)

6 pystysuoraan: OPERAATTORI Internet-palveluntarjoaja, joka kirjaa liikenteesi lokiin, ellei sitä ole salattu (11 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. EOTULITNNIN — **TUNNELOINTI**
2. YTAAIKENSEVLS — **KAISTANLEVEYS**
3. ELAESOTU — **ALUEESTO**
4. IYSYSTYSYKI — **YKSITYISYYS**
5. LKARTOOPLO — **PROTOKOLLA**
6. INVLPEAL — **PALVELIN**
7. UPRIUOAML — **PALOMUURI**
8. OTIAEOAPRTR — **OPERAATTORI**

SALAKIRJOITUSHAASTEEN AVAIN

"SUOJAA YKSITYISYYTESI TURVALLISELLA TUNNELILLA"

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.