Nimi: _____ Päivämäärä: _____ Pisteet: _____

Välityspalvelin vai VPN Tehtävämoniste

Välityspalvelinten ja virtuaalisten erillisverkkojen vertailu, salauserot sekä sovelluskohtainen ja koko järjestelmän kattava reititys

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 sovellusvälityspalvelimia järjestelmänlaajuiseen VPN-salaukseen.
- Tunnista SOCKS5:n ominaisuudet verrattuna perus-HTTP-välityspalvelimiin.
- Analysoi, miten selainpohjaiset välityspalvelimet jättävät taustasovellukset suojaamattomiksi.
- Ymmärrä, miten palveluntarjoajat kirjaavat salaamatonta liikennettä välityspalvelintunneleissa.
- Valitse oikea reititystyökalu nopeus- ja tietoturvatarpeiden mukaan.

VÄLITYSPALVELINTEN VERTAILUN TEHTÄVÄMONISTE, OHJEET

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

VÄLITYSPALVELIN VAI VPN (JOHDANTO)

Välityspalvelimet ja VPN:t palvelevat eri digitaalisen yksityisyyden tehtäviä. Välityspalvelin toimii sovellustason uudelleenohjauksena, joka peittää IP-osoitteesi tietyissä ohjelmissa salaamatta dataa. VPN toimii verkkotasolla ja suojaa kaiken järjestelmäliikenteen salauksella. Oikean työkalun valinta riippuu tietoturvatarpeistasi.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1 **1. Millä OSI-mallin kerroksella tavallinen HTTP-välityspalvelin toimii?**

- A. Fyysinen kerros
- B. Verkkokerros
- C. Sovelluskerros
- D. Siirtoyhteyskerros

2 **2. Mikä on SOCKS5:n keskeinen protokollaetu tavallisiin HTTP-välityspalvelimiin verrattuna?**

- A. Se pakottaa hyötykuorman täyden salauksen
- B. Se tukee mitä tahansa TCP/UDP-liikenteen reititystä
- C. Se on immuuni DNS-vuodoille
- D. Se toimii suoraan ytimen tilassa

3 **3. Miksi VPN on yleensä turvallisempi kuin välityspalvelin?**

- A. Se toimii nopeammalla etälaitteistolla
- B. Se salaa kaiken verkkoliikenteen koko järjestelmässä
- C. Se ei vaadi paikallisia reititystaulukoita
- D. Se poistaa verkon viiveen kokonaan

4 **4. Minkä tyyppinen välityspalvelin ohjaa liikenteen uudelleen oletuksena ilman salausta?**

- A. Perus-HTTP-välityspalvelin
- B. Salattu HTTPS-välityspalvelin
- C. Suojattu WireGuard-asiakasohjelma
- D. Hämätty VPN-palvelin

5 **5. Mitä taustasovellusten liikenteelle tapahtuu, kun käytetään selaimen välityspalvelinta?**

- A. Se salataan automaattisesti
- B. Välityspalvelin estää sen
- C. Se reititetään välityspalvelimen tunnelin kautta
- D. Se ohittaa välityspalvelimen ja paljastaa IP-osoitteesi

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. SOCKS5-välityspalvelin salaa kaikkien palvelimen kautta kulkevien pakettien hyötykuorman.

○ Tosi ○ Epätosi

7 Kysymys 7

7. VPN toimii verkkokerroksella kaiken järjestelmäliikenteen suojaamiseksi.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Välityspalvelimet ovat yleensä nopeampia kuin VPN:t, koska ne tekevät syvän pakettisalauksen.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Välityspalvelimen määrittäminen edellyttää liikenteen uudelleenohjausten asettamista tiettyjen sovellusten sisällä.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Välityspalvelimen käyttö ei suojaa datalikennettäsi paikalliselta palveluntarjoajan seurannalta.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Sovellustason _____ ohjaa tiettyä selainliikennettä suojaamatta muita sovelluksia.

2. Vankka _____ kapseloi ja salaa kaikki laitteen datapaketit.

3. Protokolla _____ sijaitsee sovellus- ja kuljetuskerrosten välissä.

4. HTTP-välityspalvelimet toimivat OSI-mallin kerroksella, jonka nimi on _____ .

5. Tavallisilta välityspalvelimilta puuttuu sisällön _____ , mikä jättää datan haavoittuvaksi.

6. VPN tarjoaa kaikille verkkosovittimille suojauksen, jonka taso on _____ .

SANASTON SANAPANKKI

LAITETASO NÄKYVYYS SALAUS SOCKS5 SOVELLUSKERROS UDP-TUKI VPN-TUNNELI VÄLITYSPALVELIN

Kirjoita vastauksesi tähän:

1.
2.
3.
4.
5.
6.

Tarkistuspiste 4: Verkkokäsitteiden yhdistäminen

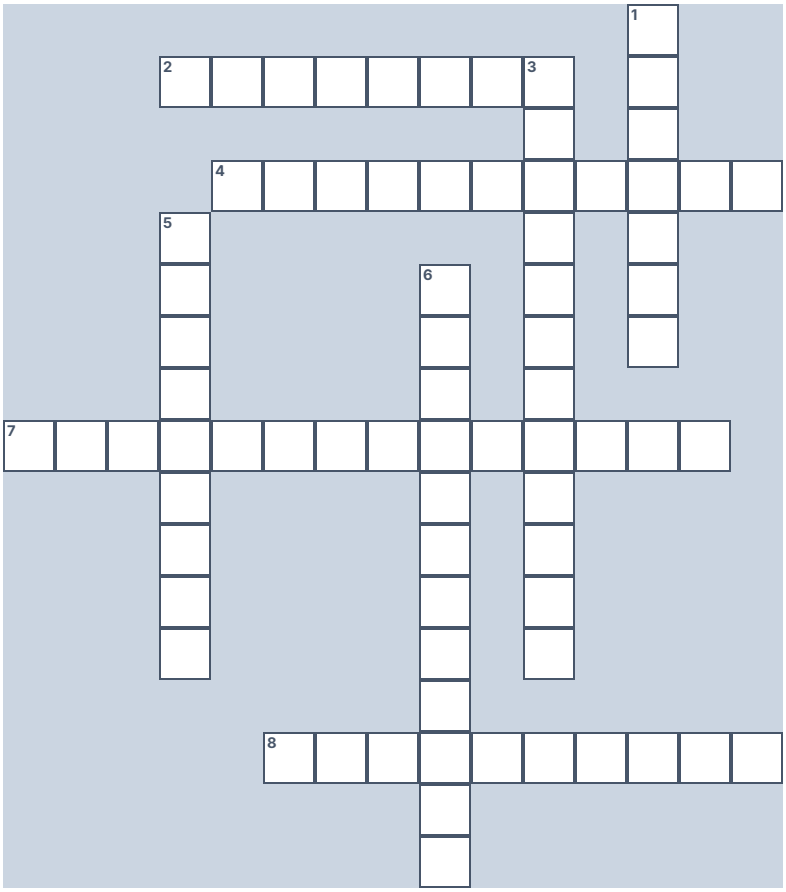
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. HTTP-välityspalvelin	A	Käyttöjärjestelmätason reititys, joka salaa kaiken sovellusliikenteen.
☐	2. SOCKS5-välityspalvelin	B	Sovelluskerros, jolla tavalliset web-välityspalvelimen protokollat toimivat.
☐	3. VPN-tunneli	C	SOCKS5:n kyky välittää UDP:tä sekä TCP:tä toisin kuin tavalliset HTTP-välityspalvelimet.
☐	4. Järjestelmänlaajuinen	D	Asiakaslaajennus, joka piilottaa liikenteen vain selaimen hiekkalaatikon sisällä.
☐	5. OSI-kerros 7	E	Salaus ja kapselointi, jotka kietovat laitteen kaiken taustaliikenteen.
☐	6. UDP-tuki	F	Liikenteen tila, jossa salaamaton välityspalvelimen data pysyy palveluntarjoajien nähtävissä.
☐	7. Selainvälityspalvelin	G	Sovelluskerroksen välityspalvelin, joka ohjaa tietyn verkkoselaimen liikennettä.
☐	8. Operaattorin näkyvyys	H	Välityspalvelinprotokolla sovellus- ja siirtokerroksen välissä, ilman salausta.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

2. Liikenteen tila, jossa salaamaton välityspalvelimen data pysyy internetoperaattoreiden nähtävissä (8)

4. Sovelluskerroksen välityspalvelin, joka ohjaa tiettyä verkkoselaimen liikennettä (11)

7. Sovelluskerros, jolla tavalliset verkkovälityspalvelinprotokollat toimivat (14)

8. Salaus ja kapselointi, joka kattaa kaiken laitteen taustaliikenteen (10)

PYSTYSUORAAN

1. SOCKS5:n kyky välittää UDP:tä TCP:n lisäksi, toisin kuin tavalliset HTTP-välityspalvelimet (7)

3. Asiakkaan laajennus, joka piilottaa liikenteen vain selaimen hiekkalaatikon sisällä (12)

5. Käyttöjärjestelmätason reititys, joka salaa kaiken sovellusliikenteen (9)

6. Välityspalvelinprotokolla sovellus- ja kuljetuskerrosten välillä, ilman salausta (12)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

2 vaakasuoraan: Liikenteen tila, jossa salaamaton välityspalvelimen data pysyy internetoperaattoreiden nähtävissä (8 kirjainta):

4 vaakasuoraan: Sovelluskerroksen välityspalvelin, joka ohjaa tiettyä verkkoselaimen liikennettä (11 kirjainta):

7 vaakasuoraan: Sovelluskerros, jolla tavalliset verkkovälityspalvelinprotokollat toimivat (14 kirjainta):

8 vaakasuoraan: Salaus ja kapselointi, joka kattaa kaiken laitteen taustaliikenteen (10 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: SOCKS5:n kyky välittää UDP:tä TCP:n lisäksi, toisin kuin tavalliset HTTP-välityspalvelimet (7 kirjainta):

3 pystysuoraan: Asiakkaan laajennus, joka piilottaa liikenteen vain selaimen hiekkalaatikon sisällä (12 kirjainta):

5 pystysuoraan: Käyttöjärjestelmätason reititys, joka salaa kaiken sovellusliikenteen (9 kirjainta):

6 pystysuoraan: Välityspalvelinprotokolla sovellus- ja kuljetuskerrosten välillä, ilman salausta (12 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

HTTPVÄLITYS, SOCKSVÄLITYS, VPNTUNNELI, LAITETASO, SOVELLUSKERROS, UDPTUKI, SELAINPROKSI, NÄKYVYYS

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. HTTPVÄLITYS**
- **B. SOCKSVÄLITYS**
- **C. VPNTUNNELI**
- **D. LAITETASO**
- **E. SOVELLUSKERROS**
- **F. UDPTUKI**
- **G. SELAINPROKSI**
- **H. NÄKYVYYS**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Sovelluskerros, jolla tavalliset verkkovälityspalvelinprotokollat toimivat.
2. SOCKS5:n kyky välittää UDP:tä TCP:n lisäksi, toisin kuin tavalliset HTTP-välityspalvelimet.
3. Sovelluskerroksen välityspalvelin, joka ohjaa tiettyä verkkoselaimen liikennettä.
4. Asiakkaan laajennus, joka piilottaa liikenteen vain selaimen hiekkalaatikon sisällä.
5. Salaus ja kapselointi, joka kattaa kaiken laitteen taustaliikenteen.
6. Käyttöjärjestelmätason reititys, joka salaa kaiken sovellusliikenteen.
7. Liikenteen tila, jossa salaamaton välityspalvelimen data pysyy internetoperaattoreiden nähtävissä.
8. Välityspalvelinprotokolla sovellus- ja kuljetuskerrosten välillä, ilman salausta.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. **VLYTÄIHTTSP**
2. **LTVPUINENN**
3. **SKOOSSERVULLRE**
4. **SRILPINKOSEA**
5. **OTLÄSCSIVSYK**
6. **STAATLEOI**
7. **UKUIDTP**
8. **YÄVSNYYK**

Bonustehtävä: Nopeat vastaukset

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

1	Eroja välityspalvelimen ja VPN:n välillä			
2	Asioita, jotka jäävät salaamatta ilman VPN:ää			
3	Tapoja tunnistaa väärennetty Wi-Fi-verkko			
4	Asioita, joita välikäsi tekee arjessa			
5	Tilanteita, joissa välityspalvelin riittää			
6	Laitteita, jotka voivat käyttää VPN:ää			
7	Välityspalvelintyyppejä, jotka tunnet			
8	Asioita, jotka VPN voi piilottaa			
9	Myyttejä VPN:istä			
10	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
11	Asioita, joilta VPN ei voi suojata sinua			
12	Sanoja tästä tehtävämonisteesta, jotka haluat muistaa			
13	Syitä käyttää VPN:ää matkustaessa			
14	Tilanteita, joissa haluat VPN:n			
15	Paikkoja, joissa käyttäisit VPN:ää			

Tarkistuspiste 8: VPN:n tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

SARAH (KAHVILAN OPISKELIJA)

👷 "Hei! Olen Coffee & Bytes -kahvilassa avoimessa verkossa nimeltä 'Free_Wi-Fi_No_Password'. Minun pitää kirjautua koulun sähköpostiin, ja kaverini mukaan ilmainen selainvälityspalvelin riittää pitämään minut turvassa. Suojaisiko välityspalvelin kirjautumiseni ja tiedostoni, vai tarvitsenko VPN:n?"

ALEX (MATKAILIJAOPISKELIJA)

👷 "Olen ulkomailla, ja kotimaassani isännöity biologiadokumentti sanoo 'Tämä video ei ole saatavilla nykyisessä sijainnissasi.' Luokkatoverini käyttää välityspalvelinta, ja minulla on VPN. Miksi minut on estetty, ja kumpi työkalu toimisi paremmin?"

Tarkistuspiste 9: Salakirjoituksen purkaminen

Suorita välityspalvelinten vertailukoulutuksesi loppuun purkamalla tämä salainen viesti suojatusta tunneloinnista.

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

15	8	10	1	1		12	9	9	11	5	14	20	5	5	19	9
22	28	12	9	20	25	19	16	1	12	22	5	12	9	13	5	14
11	1	21	20	20	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: Mikä on välityspalvelin?

Välityspalvelin on välittäjä, joka välittää pyynnöt sovelluksesi ja kohdepalvelimen välillä. Verkkosivusto näkee välityspalvelimen IP-osoitteen omasi sijaan, mutta vain välityspalvelimen käyttöön määritettyjen sovellusten liikenne ohjataan sen kautta, eikä perusvälityspalvelin salaa tätä liikennettä.

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 välityspalvelin VPN?

Ei. Välityspalvelin välittää tiettyjen sovellusten liikennettä, yleensä ilman salausta. VPN rakentaa verkkotasolle salatun tunnelin, joka kuljettaa kaiken laitteen liikenteen, taustasovellukset mukaan lukien.

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 välityspalvelinta?

Voit, mutta ilmaisia välityspalvelimia ylläpitävät usein tuntemattomat toimijat. Koska perusvälityspalvelin ei salaa liikennettä, sen ylläpitäjä voi nähdä ja jopa muokata salaamattomia sivuja. Tarkista, kuka palvelua ylläpitää, ennen käyttöä.

Q7: Tallentaako välityspalvelin lokeja?

Se voi. Välityspalvelin käsittelee jokaisen välittämänsä pyynnön, joten sen ylläpitäjä voi tallentaa IP-osoitteesi, vierailemasi sivustot ja ajankohdat. Tarkista, kuka sitä ylläpitää ja mitä sen tietosuojakäytäntö sanoo.

Q8: Milloin välityspalvelin riittää?

Välityspalvelin voi riittää vähäriskisiin tehtäviin, kuten yhden selaimen näennäisen sijainnin muuttamiseen. Pankkiasioinnissa, julkisessa Wi-Fi-verkossa tai laitteen kaikkien sovellusten suojaamisessa VPN on turvallisempi valinta, koska se salaa kaiken liikenteen.

Q9: Voiko välityspalvelin suojata kaikki puhelimeni sovellukset?

Ei. Vain sovellukset, jotka noudattavat välityspalvelinasetusta, käyttävät sitä; muut yhdistävät suoraan. VPN-sovellus reitittää sen sijaan kaikki puhelimen sovellukset salatun tunnelinsa kautta.

Q10: Mikä on SOCKS5-välityspalvelin?

SOCKS5, joka on määritelty RFC 1928:ssa, on välityspalvelinprotokolla, joka sijaitsee sovellus- ja kuljetuskerrosten välissä. Se voi välittää TCP-yhteyksiä ja UDP-datagrammeja ja tukee todennusta, mutta siinä ei ole sisäänrakennettua salausta. [1]

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

Tutustu virtuaalisten yksityisverkkojen ja suojattujen tunnelointiprotokollien teknisiin ja rakenteellisiin puoliin.

Q1: Millä verkkokerroksilla välityspalvelimet ja VPN:t toimivat?

HTTP-välityspalvelin toimii sovelluskerroksella (kerros 7) ja ymmärtää verkkopyynnöt. SOCKS5 sijaitsee sovellus- ja siirtokerroksen välissä. VPN-protokollat, kuten IPsec tai WireGuard, toimivat verkkokerroksella, joten ne voivat kuljettaa kaiken laitteen IP-liikenteen.

Q2: Pysyykö HTTPS-sivusto salattuna välityspalvelimen kautta?

Kyllä. Kun avaat HTTPS-sivuston välityspalvelimen kautta, TLS-salaus toimii päästä päähän selaimesi ja sivuston välillä, joten välityspalvelin näkee verkkotunnuksen mutta ei sivun sisältöä. Pelkät HTTP-sivut pysyvät luettavissa.

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: Mikä on läpinäkyvä välityspalvelin ja kuka sitä käyttää?

Läpinäkyvä välityspalvelin sieppaa liikenteen ilman mitään määrityksiä käyttäjän laitteessa. Koulut, yritykset ja internetoperaattorit käyttävät niitä välimuistitukseen tai sisällönsuodatukseen. Käyttäjät eivät usein tiedä sellaisen olevan käytössä, eikä se anna heille yksityisyyttä.

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: Miksi välityspalvelin voi tuntua nopeammalta kuin VPN-yhteys?

Perusvälityspalvelin jättää salauksen pois ja käsittelee vain yhden sovelluksen liikennettä, joten se lisää vähemmän käsittelyä. VPN salaa jokaisen laitteen paketin. Nykyaikaisilla protokollilla ero on usein pieni, ja välityspalvelin tarjoaa paljon heikomman suojan.

Q8: Voivatko verkkosivustot havaita, että käytän välityspalvelinta tai VPN:ää?

Usein kyllä. Monet sivustot tarkistavat IP-osoitteita tunnettujen välityspalvelin- ja VPN-palvelinluetteloiden avulla, ja HTTP-välityspalvelimet voivat lisätä otsikoita, kuten Via tai X-Forwarded-For. Suoratoistopalvelut estävät yleensä molemmat.

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 välityspalvelin pysäyttää internetpalveluntarjoajan nopeuden rajoituksen?

Harvoin. Tavallinen välityspalvelin ei salaa liikennettä, joten palveluntarjoaja näkee silti, millaista toimintaa se on. VPN piilottaa liikennetyypit, mutta kumpikaan työkalu ei korjaa ruuhkaa tai datarajoja.

Osa 11: 10 mielenkiintoista VPN-faktaa ja tosielämän havaintoa

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

1. SOCKS-STANDARDI

IETF julkaisi SOCKS-protokollan version 5 RFC 1928 -dokumenttina maaliskuussa 1996, ja se on yhä viitemäärittely SOCKS5-välityspalvelimille, joita selaimet ja sovellukset käyttävät nykyään. [1]

2. SHIM-KERROS

RFC 1928 kuvaa SOCKSin välikerroksena sovellus- ja kuljetuskerroksen välillä, joten se ei voi välittää verkkokerroksen liikennettä, kuten ICMP:tä. [1]

3. UDP-RELE

SOCKS5 lisäsi UDP ASSOCIATE -komennon, jonka ansiosta välityspalvelin voi välittää UDP-datagrammeja TCP-yhteyksien lisäksi, mitä tavalliset HTTP-välityspalvelimet eivät käsittele. [1]

4. SOCKSIN OLETUSPORTTI

SOCKS5-asiakkaat yhdistävät välityspalvelimeen oletuksena TCP-portissa 1080, kuten RFC 1928 määrittelee; monet välityspalvelut antavat käyttäjien valita muita portteja. [1]

5. HTTP-VÄLIKÄDET

HTTP-standardi (RFC 9110) määrittelee välityspalvelimen asiakkaan valitsemaksi viestejä välittäväksi agentiksi, joka välittää pyynnöt eteenpäin alkuperäispalvelimelle.

6. SYVÄ PAKETTITARKASTUS

Syväpakettitarkastus (DPI) tutkii pakettien sisältöä ja liikennemalleja; salaamaton välityspalvelinliikenne näkyy sille täysin, kun taas VPN-liikenne paljastaa paljon vähemmän.

7. VERKKOKERROKSEN VPN:T

NIST SP 800-77:ssä kuvattu IPsec suojaa liikennettä verkkokerroksella, joten jokaisen sovelluksen IP-paketit voidaan suojata ilman sovelluskohtaisia asetuksia. [2]

8. VAIN SELAIMEEN RAJATTU KATTAVUUS

Yhteen selaimeen asetettu välityspalvelin vaikuttaa vain kyseiseen selaimeen; sähköpostiohjelmat, pelit ja järjestelmäpäivitykset käyttävät edelleen laitteen tavallista yhteyttä.

9. TOR VS. VÄLITYSPALVELIMET

Tor lähettää liikenteen kolmen vapaaehtoisen välityssolmun (guard, middle ja exit) kautta ja siihen päästään yleensä paikallisen SOCKS-välityspalvelimen kautta, mikä lisää kerroksia, joita yksittäinen välityspalvelin ei tarjoa.

10. NOPEUDEN KOMPROMISSI

Välityspalvelimet voivat vaikuttaa nopeammilta, koska ne ohittavat salauksen, mutta nykyaikaiset VPN-protokollat, kuten WireGuard, lisäävät vain vähän kuormaa ja suojaavat samalla kaiken laitteen liikenteen.

Tekniset viitteet ja lähteet

Tässä tehtävämonisteessa käytetyt lainatut julkaisut, salausmääritykset ja viralliset asiakirjastandardit.

TIETEELLISET JA ALAN VIITTEET

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Vastausavain: välityspalvelinten ja virtuaalisten erillisverkkojen vertailu, salauksen erot sekä sovellus- ja järjestelmätason reititys

1 Välityspalvelimen OSI-kerros

PROTOKOLLAT

Oikea vastaus: C

OPETTAJALLE

Tavalliset HTTP/HTTPS-välityspalvelimet toimivat sovellustasolla (taso 7) ja ohjaavat uudelleen tiettyä selainliikennettä. Niiltä puuttuu järjestelmänlaajuinen verkkoreititys. Lähde: Tor Project Foundation.

2 Kysymys 2

Oikea vastaus: B

OPETTAJALLE

SOCKS5 välittää TCP- ja UDP-liikennettä sovellus- ja siirtokerroksen välillä mutta ei salaa oletuksena, kun taas HTTP-välityspalvelimet käsittelevät verkkopyyntöjä.

3 VPN-järjestelmäsalaus

WI-FI-TURVALLISUUS

Oikea vastaus: B

OPETTAJALLE

VPN kapseloi ja salaa kaiken käyttöjärjestelmän liikenteen koko järjestelmässä, kun taas välityspalvelin ohjaa liikennettä vain tietyille määritetyille sovelluksille. Lähde: Deloitte Advisory.

4 Välityspalvelimen salauksen puute

REITITYKSEN HALLINTA

Oikea vastaus: A

OPETTAJALLE

HTTP-välityspalvelimet välittävät selaimen liikennettä sovelluskerroksella salaamatta pakettien hyötykuormaa, joten verkon ylläpitäjä tai palveluntarjoajasi voi silti jäljittää sisältöliikennettäsi. Lähde: IETF Proxy Vulnerabilities.

5 Ohituksen haavoittuvuus

YKSITYISYYS

Oikea vastaus: D

OPETTAJALLE

Selainvälityspalvelimet soveltavat sääntöjä vain itse verkkoselaimeen. Taustasovellukset, käyttöjärjestelmäpäivitykset ja sähköpostiohjelmat ohittavat välityspalvelimen ja paljastavat oman IP-osoitteesi. Lähde: W3C Consortium.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

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

OPETTAJALLE

SOCKS5 välittää liikennettä sovellus- ja siirtokerroksen välillä mutta ei suorita oletuksena salausta, joten pakettien sisältö pysyy luettavana siirron aikana.

7 **Verkkokerroksen tunnelit** NOPEUDET — **Oikea vastaus: Tosi**

OPETTAJALLE

Toimimalla verkkokerroksella VPN reitittää ja salaa laitteestasi lähtevän liikenteen, mikä auttaa suojaamaan liikennettä koko järjestelmässä. Lähde: Deloitte Advisory.

8 **Välityspalvelimen salausrajoitus** NUUSKINTARISKI — **Oikea vastaus: Epätosi**

OPETTAJALLE

Välityspalvelimet voivat joskus olla nopeampia, mutta se johtuu siitä, että ne EIVÄT salaa dataa. Salauksen puute jättää datan alttiiksi tarkastukselle. Lähde: IETF Proxy Vulnerabilities.

9 **Sovellustason uudelleenohjaus** PALOMUURIT — **Oikea vastaus: Tosi**

OPETTAJALLE

Toisin kuin koko järjestelmän kattavat VPN:t, välityspalvelimet vaativat manuaalisen määrityksen selaimen asetuksissa tai sovelluskohtaisissa välityspalvelinkentissä. Lähde: W3C Consortium.

10 **Palveluntarjoajan seurantariski** LOKITON — **Oikea vastaus: Tosi**

OPETTAJALLE

Koska tavalliset HTTP/SOCKS5-välityspalvelimet eivät salaa hyötykuormaa, paikallinen internetyhteyden tarjoajasi näkee kaiken verkkotoimintasi. Lähde: EDRi Retention Guidelines.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

G 1. HTTP-välityspalvelin	H 2. SOCKS5-välityspalvelin	E 3. VPN-tunneli	A 4. Järjestelmänlaajuinen
B 5. OSI-kerros 7	C 6. UDP-tuki	D 7. Selainvälityspalvelin	F 8. Operaattorin näkyvyys

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 VÄLITYSPALVELIN	2 VPN-TUNNELI	3 SOCKS5	4 SOVELLUSKERROS
5 SALAUS	6 LAITETASO		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 E – SOVELLUSKERROS	2 F – UDPTUKI	3 A – HTTPVÄLITYS	4 G – SELAINPROKSI
5 C – VPNTUNNELI	6 D – LAITETASO	7 H – NÄKYVYYS	8 B – SOCKSVÄLITYS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit HTTP-välityspalvelin, SOCKS5-välityspalvelin ja VPN-tunneli omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

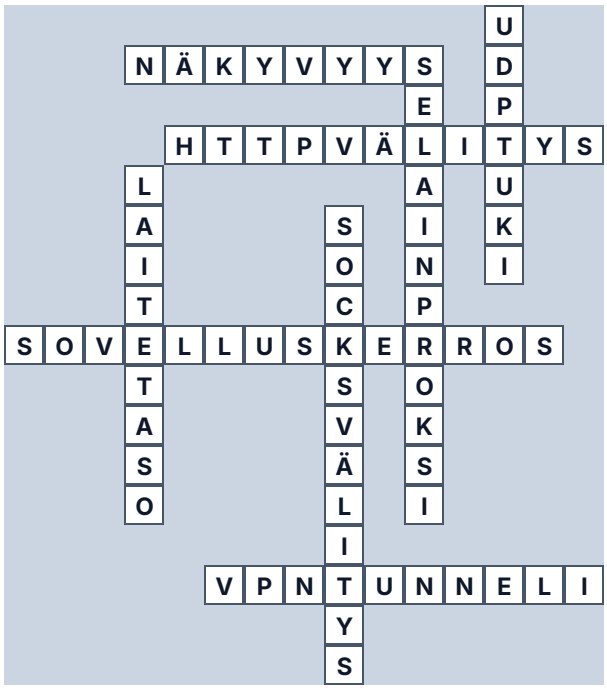
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: NÄKYVYYS Liikenteen tila, jossa salaamaton välityspalvelimen data pysyy internetoperaattoreiden nähtävissä (8 kirjainta)

4 vaakasuoraan: HTTPVÄLITYS Sovelluskerroksen välityspalvelin, joka ohjaa tiettyä verkkoselaimen liikennettä (11 kirjainta)

7 vaakasuoraan: SOVELLUSKERROS Sovelluskerros, jolla tavalliset verkkovälityspalvelinprotokollat toimivat (14 kirjainta)

8 vaakasuoraan: VPNTUNNELI Salaus ja kapselointi, joka kattaa kaiken laitteen taustaliikenteen (10 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: UDPTUKI SOCKS5:n kyky välittää UDP:tä TCP:n lisäksi, toisin kuin tavalliset HTTP-välityspalvelimet (7 kirjainta)

3 pystysuoraan: SELAINPROKSI Asiakkaan laajennus, joka piilottaa liikenteen vain selaimen hiekkalaatikon sisällä (12 kirjainta)

5 pystysuoraan: LAITETASO Käyttöjärjestelmätason reititys, joka salaa kaiken sovellusliikenteen (9 kirjainta)

6 pystysuoraan: SOCKSVÄLITYS Välityspalvelinprotokolla sovellus- ja kuljetuskerrosten välillä, ilman salausta (12 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. VLYTÄIHTTSP — **HTTPVÄLITYS**
2. LTVPUINENN — **VPNTUNNELI**
3. SKOOSSERVULLRE — **SOVELLUSKERROS**
4. SRILPINKOSEA — **SELAINPROKSI**
5. OTLÄSCSIVSYK — **SOCKSVÄLITYS**
6. STAATLEOI — **LAITETASO**
7. UKUIDTP — **UDPTUKI**
8. YÄVSNYYK — **NÄKYVYYS**

SALAKIRJOITUSHAASTEEN AVAIN

"OHJAA LIIKENTEESI VÄLITYSPALVELIMEN KAUTTA"

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.
- Välityspalvelin vai VPN: tavallinen selaimen välityspalvelin ei salaa hänen liikennettään. VPN salaa kaiken laitteella, jolloin siepatut paketit ovat paikallisille nuuskijoille lukukelvottomia.

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.
- Kumpi toimii paremmin: Molemmat antavat hänelle kotimaan IP-osoitteen, mutta välityspalvelin kattaa vain määritetyn sovelluksen, kun taas VPN salaa myös kaiken hänen laitteensa liikenteen.