Nimi: _____ Päivämäärä: _____ Pisteet: _____

# Etäkäyttö-VPN

Etätyöntekijöiden päätelaitteiden suojaaminen, monivaiheinen tunnistautuminen ja IPsec-tunnelien määritykset.

## ETÄKÄYTTÖ-VPN:IEN OPPIMISKATSAUS

**OPPIJA**
**OPISKELIJASTATUS**
Verkon puolustajan polku

**TURVALLINEN**
**YHTEYDEN TILA**
Datapakettien suojaaminen

**AKTIIVINEN**
**VUOTOSUOJA**
DNS- ja IPv6-vuodonesto

**Tervetuloa!** Tämä tehtäväpaketti käsittelee aihetta: etäkäyttö-VPN-verkot. Tutustut asiakas-palvelin-tunneleihin, monivaiheisiin kirjautumisiin, päätelaitteen tilatarkistuksiin, kaistanleveysrajoihin ja syslog-tietoturva-auditointiin.

**TEHTÄVÄMONISTEEN TARKISTUSPISTEET**

- [ ] **Osat 1–4: Hallitse VPN- ja verkkoturvallisuuden määritykset.**
- [ ] **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 parhaiden VPN-palvelujen opas**

URL: https://www.vpn.com/fi/vpn/paras-vpn-yrityksille/etakaytto/

# Oppimispolkusi: etäkäytön VPN

- Suojatut etätyöntekijöiden päätelaitteet, jotka käyttävät paikallisverkon solmuja.
- Määritä monivaiheisen todennuksen käytännöt etäkirjautumisia varten.
- Määritä asiakas-sivusto IPsec- ja OpenVPN-asetukset.
- Auditoi etäyhteyslokit käyttöoikeusrikkomusten varalta.
- Toteuta laitteen tilatarkistukset ennen verkkoyhteyksien myöntämistä.
- Optimoi palvelimen läpäisykyky, jotta etätyön kaistanleveys ei tukkeudu.

## ETÄKÄYTTÖ-VPN:IEN OHJEET

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

## CLIENT-TO-SITE-TUNNELIT JA PÄÄTELAITTEIDEN VAATIMUSTENMUKAISUUS (JOHDANTO)

Etäkäyttö-VPN:t muodostavat suojattuja asiakas-sivusto-tunneleita toimipisteen ulkopuolella työskenteleville. Näiden yhteyksien suojaaminen edellyttää monivaiheisen tunnistautumisen (MFA) kirjautumisten pakottamista, päätelaitteen tilan vaatimustenmukaisuustarkistuksia ja lokien auditointia keskitettyjen syslog-keräimien kautta.

**LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.**

## Tarkistuspiste 1: Monivalintahaaste

1. **1. Mitä todennusstandardia etäkäyttö-VPN-portaalien tulisi edellyttää?**
   - A) Monitekijäinen
   - B) Yksivaiheinen
   - C) Salaamaton
   - D) Paikallinen vieras

2. **2. Mikä protokolla on etätyön asiakas-toimipiste-yhteyksien suojaamisen standardi?**
   - A) OpenVPN
   - B) SOCKS5
   - C) PPTP
   - D) FTP

3. **3. Mikä tarkistus varmistaa, että etäkannettava on puhdas ennen yhdistämistä?**
   - A) Tilatarkistus
   - B) Nopeustesti
   - C) Ping-testi
   - D) Muistin määrä

4. **4. Missä etätyöntekijöiden yhteyslokit säilytetään tietoturvatarkastuksia varten?**
   - A) Syslog-palvelin
   - B) Rekisteriavain
   - C) Asiakkaan muisti
   - D) Verkkoselain

5. **5. Mikä ongelma syntyy, kun etätyöntekijöiden määrä ylittää yhdyskäytävän kaistanleveyskapasiteetin?**
   - A) Kaistanleveyden kuristus
   - B) DNS-vuoto
   - C) Kättelyn läpäisy
   - D) IP-osoitteen paljastuminen

## Tarkistuspiste 2: Tosi vai epätosi -haaste

### 6 Kysymys 6

6. Monivaiheinen tunnistautuminen lisää toisen vahvistustunnisteen etäkirjautumisten suojaamiseksi.

○ Tosi ○ Epätosi

### 7 Kysymys 7

7. Laitetilatarkastukset sallivat etälaitteiden, joiden palomuurit on poistettu käytöstä, pääsyn yksityisille palvelimille.

○ Tosi ○ Epätosi

### 8 Kysymys 8

8. Etäkäyttö-VPN:n lokit ovat välttämättömiä luvattoman yrityksen verkkoon pääsyn jäljittämiseksi.

○ Tosi ○ Epätosi

### 9 Kysymys 9

9. OpenVPN ja IPsec ovat vanhentuneita protokollia, jotka eivät salaa etäasiakkaiden sisältöä.

○ Tosi ○ Epätosi

### 10 Kysymys 10

10. Yhdyskäytävän kaistapullonkaula syntyy, kun etäliikenne ylittää verkkokortin kapasiteetin.

○ Tosi ○ Epätosi

## Tarkistuspiste 3: Avainkäsitteiden täyttö

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

**1. Yrityksen portaalien suojaamiseksi etäkirjautumisten on edellytettävä tunnistautumista, joka on _____ .**

**2. Etäasiakkaat salaavat tunnelin tietosisällön vakioprotokollilla, kuten _____ .**

**3. Laitteiden on läpäistävä tietoturvatarkistus ennen verkkoyhteyttä; tarkistettavaa ominaisuutta kutsutaan nimellä _____ .**

**4. Tarkastettavat kirjautumislokit lähetetään jatkuvasti keskitettyyn _____ -palvelimeen.**

**5. Raskaan liikenteen aikana toimistoaikaan yhdyskäytävän _____ voi ruuhkautua.**

**6. Windowsin ja macOS:n virtuaaliset sovitinajurit hoitavat asiakkaan ja palvelinverkon välisessä yhteydessä tekniikkaa nimeltä _____ .**

**SANASTON SANAPANKKI**

KAISTA LAITEKUNTO MONIVAIHEINEN OPENVPN PALOMUURI SALAUS SYSLOG TUNNELOINTI

**Kirjoita vastauksesi tähän:**

**1.** **2.**

**3.** **4.**

**5.** **6.**

# Tarkistuspiste 4: Keskeisten käsitteiden yhdistäminen

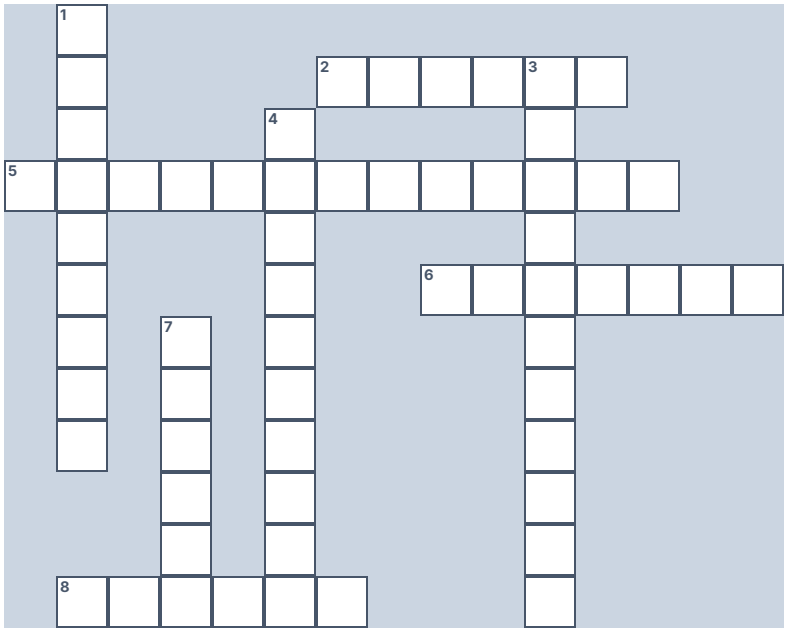
**MÄÄRITELMIEN YHDISTÄMINEN**

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

| | | | |
|---|---|---|---|
| ☐ | 1. USEAN TEKIJÄN | A | Datan kapselointi suojattuun reittiin. |
| ☐ | 2. OPENVPN | B | Keskitetty tietoturvalokien kerääjä. |
| ☐ | 3. LAITETILA | C | Verkon tiedonsiirtokapasiteetin raja. |
| ☐ | 4. SYSLOG | D | Vakiomuotoinen asiakas-sivusto-protokolla. |
| ☐ | 5. KAISTA | E | Etälaitteen kunnon validointi. |
| ☐ | 6. SALAUS | F | Liikenteen suodatusjärjestelmän säännöt. |
| ☐ | 7. TUNNELOINTI | G | Pakettien kryptografinen sekoittaminen. |
| ☐ | 8. PALOMUURI | H | Kirjautumisturva, joka vaatii lisätunnisteita. |

# Tarkistuspiste 5: Ristikko

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




## VAAKASUORAAN

**2. Verkon datakapasiteetin raja (6)**

**5. Kirjautumisen suojaus, joka vaatii lisätunnisteita (13)**

**6. Asiakkaan ja palvelinverkon välinen vakioprotokolla (7)**

**8. Keskitetty tietoturvalokien kerääjä (6)**

## PYSTYSUORAAN

**1. Liikennettä suodattavan järjestelmän säännöt (9)**

**3. Datan kapselointi suojattuun reittiin (11)**

**4. Etälaitteen terveyden tarkistus (10)**

**7. Pakettien kryptografinen sekoittaminen (6)**

# Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

## VAAKASUORAAN

**2 vaakasuoraan: Verkon datakapasiteetin raja (6 kirjainta):**

**5 vaakasuoraan: Kirjautumisen suojaus, joka vaatii lisätunnisteita (13 kirjainta):**

**6 vaakasuoraan: Asiakkaan ja palvelinverkon välinen vakioprotokolla (7 kirjainta):**

**8 vaakasuoraan: Keskitetty tietoturvalokien kerääjä (6 kirjainta):**

## PYSTYSUORAAN

**1 pystysuoraan: Liikennettä suodattavan järjestelmän säännöt (9 kirjainta):**

**3 pystysuoraan: Datan kapselointi suojattuun reittiin (11 kirjainta):**

**4 pystysuoraan: Etälaitteen terveyden tarkistus (10 kirjainta):**

**7 pystysuoraan: Pakettien kryptografinen sekoittaminen (6 kirjainta):**

## Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

**SANASTOLISTA**

MONIVAIHEINEN OPENVPN LAITEKUNTO SYSLOG KAISTA SALAUS
TUNNELOINTI PALOMUURI

# Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

**SANASTOTERMIT**

- **A. MONIVAIHEINEN**
- **B. OPENVPN**
- **C. LAITEKUNTO**
- **D. SYSLOG**
- **E. KAISTA**
- **F. SALAUS**
- **G. TUNNELOINTI**
- **H. PALOMUURI**

**MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT**

1. Keskitetty tietoturvalokien kerääjä.
2. Liikennettä suodattavan järjestelmän säännöt.
3. Datan kapselointi suojattuun reittiin.
4. Pakettien kryptografinen sekoittaminen.
5. Asiakkaan ja palvelinverkon välinen vakioprotokolla.
6. Verkon datakapasiteetin raja.
7. Etälaitteen terveyden tarkistus.
8. Kirjautumisen suojaus, joka vaatii lisätunnisteita.

## Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi tämän monisteen keskeiset käsitteet. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. INEEAOHIMNNVI
2. TTLAEOUNKI
3. KISATA
4. OTILNENITUN
5. VNNEOPP
6. OLSSGY
7. USASLA
8. IMRPOAUUL

# Bonustehtävä: Nopeat vastaukset

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

| | | | | |
|---|---|---|---|---|
| 1 | Myyttejä VPN:istä | | | |
| 2 | Sanoja, jotka kuvaavat Zero Trustia | | | |
| 3 | Toimisto-ohjelmia, jotka tunnet | | | |
| 4 | Sääntöjä turvalliseen etätyöhön | | | |
| 5 | Asioita, jotka internetoperaattorisi näkee | | | |
| 6 | VPN-palveluja, jotka tunnet | | | |
| 7 | Paikkoja, joista työntekijät työskentelevät | | | |
| 8 | Työkaluja, joita yritys käyttää joka päivä | | | |
| 9 | Rooleja IT-osastolla | | | |
| 10 | Laitteita, joita työntekijällä voi olla | | | |
| 11 | Tietoja, jotka yrityksen on suojattava | | | |
| 12 | Asioita, joita teet tietoturvaloukkauksen jälkeen | | | |
| 13 | Asioita, jotka voivat häiritä videopalaveria | | | |
| 14 | Tapoja kirjautua turvallisesti | | | |
| 15 | Syitä antaa työntekijöille VPN | | | |

# Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

## TAPAUSTUTKIMUS 1: MFA:N PAKOTTAMINEN



**Tilanne:** Liiketoiminta-analyytikko yrittää kirjautua yrityksen tietokantaan etätyön aikana. Hän syöttää oikean käyttäjätunnuksen ja salasanan, mutta VPN-portaali estää pääsyn ja vaatii fyysisen tunnuskoodin.

**Keskustelukysymys: Mikä tietoturvakäytäntö pakottaa tämän kaksinkertaisen todennusvaiheen?**

## TAPAUSTUTKIMUS 2: SUOJAUSTASON VAATIMUSTENMUKAISUUS



**Tilanne:** Alihankkija yhdistää henkilökohtaisen kannettavansa yrityksen etäverkkoon. VPN-asiakasohjelma katkaisee yhteyden heti ja ilmoittaa käyttäjälle, että hänen virustorjuntansa määritykset ovat vanhentuneet.

**Keskustelukysymys:** Mikä erikoistunut VPN-yhdyskäytävän tarkistus esti tämän yhteysyrityksen?

# Tarkistuspiste 9: Salakirjoituksen purkaminen

Verkkoinsinööri suojaa reititysreittejä ja asiakastunneleita. Käytä alla olevaa kirjain–numero-avainta purkaaksesi viestin 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

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 20 | 28 | 25 | 8 | 20 | 5 | 25 | 19 | | 22 | 16 | 14 | | 19 | 21 | 15 | 10 | 1 | 1 |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | 25 | 18 | 9 | 20 | 25 | 11 | 19 | 5 | 14 | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | 16 | 28 | 28 | 20 | 5 | 12 | 1 | 9 | 20 | 20 | 5 | 5 | 20 | | |
| | | | | | | | | | | | | | | | | | | | |

**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 virtuaalisista yksityisverkoista (VPN) ja tunneloinnista.

### Q1: Mikä on etäkäyttö-VPN?

Suojattu yhteystapa, jonka avulla toimipisteen ulkopuolella työskentelevät työntekijät voivat yhdistää suoraan yrityksen yksityisiin palvelimiin.

### Q2: Miksi asiakkaasta sivustoon -yhteys eroaa sivustosta sivustoon -yhteydestä?

Client-to-site yhdistää yksittäisiä käyttäjälaitteita, kun taas site-to-site yhdistää kokonaisia fyysisiä toimipisteitä.

### Q3: Mikä on laitteen tilatarkistus?

Tarkistus, joka selvittää etälaitteen suojaustilan (virustorjunta, käyttöjärjestelmän päivitystaso) ennen käyttöoikeuden myöntämistä.

### Q4: Miksi OpenVPN:ää käytetään etäkäyttöön?

Sen vahvan tietoturvaprotokollan, alustojen välisen yhteensopivuuden ja yksittäisten yhteyksien käsittelykyvyn vuoksi.

### Q5: Miten MFA suojaa etäkäyttöä?

Se lisää toissijaisen todennustunnisteen, joka estää pääsyn, vaikka työntekijöiden salasanat vuotaisivat tai varastettaisiin.

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

Tutustu yleisimpiin kysymyksiin ja vastauksiin virtuaalisista yksityisverkoista (VPN) ja tunneloinnista.

### Q6: Mikä on syslog-palvelin?

Keskitetty lokitietovarasto, joka tallentaa yhteystapahtumat, kirjautumiset ja järjestelmähälytykset vaatimustenmukaisuustarkastuksia varten.

### Q7: Mikä aiheuttaa kaistanleveyden tukkeutumisen?

Kun etätyöntekijöiden yhteenlasketut kaistanleveystarpeet ylittävät yrityksen yhdyskäytävän internetnopeuden ylärajan.

### Q8: Voinko yhdistää kotitietokoneeni työn VPN:ään?

Vain jos laite läpäisee yrityksen laitetilatarkastukset ja IT-ylläpitäjät ovat valtuuttaneet sen.

### Q9: Mitä verkon kapselointi on?

Datapakettien kääriminen siirron aikana salattujen protokollaotsikoiden sisään siirron suojaamiseksi.

### Q10: Miten jaettu tunnelointi optimoi etäkäyttöä?

Se antaa työntekijöiden käyttää paikallista palveluntarjoajaansa tavalliseen selaamiseen ja reitittää työhön liittyvät tiedostot VPN:n kautta.

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

Tutustu VPN-tunnelointiprotokollien, mobiiliasiakasohjelmien integraatioiden ja yrityskäyttöönoton edistyneisiin teknisiin puoliin.

### Q1: Miten varmennepohjainen todennus parantaa etäkäyttöä?

Se sitoo yhteysoikeudet valmiiksi asennettuihin paikallisiin digitaalisiin varmenteisiin ja estää hallinnoimattomat tai luvattomat laitteet.

### Q2: Mikä on jaetun tunneloinnin tietoturvariski etätyössä?

Se luo mahdollisen sillan, jonka kautta vaarantunut paikallinen laite voi reitittää ulkoisia uhkia yksityiseen verkkoon.

### Q3: Miten laitteen tilatarkistukset tarkastavat rekisteriasetuksia?

VPN-asiakasohjelma suorittaa paikallisia komentosarjoja, jotka kyselevät rekisteripolkuja sen tarkistamiseksi, onko yrityksen tietoturvaohjelmisto aktiivisesti käynnissä.

### Q4: Miksi syslogit käyttävät oletuksena UDP-porttia 514?

Lokien lähettämiseksi nopeasti mahdollisimman pienellä kuormalla, vaikka turvalliset asennukset edellyttävät nykyään TLS-kapselointia TCP:n päällä.

### Q5: Miten yritykset ratkaisevat yhdyskäytävän kaistanleveyden pullonkaulat?

Ottamalla käyttöön kuormantasaajia ja jakamalla etäliikenne alueellisten palvelinsolmujen kesken.

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

Tutustu VPN-tunnelointiprotokollien, mobiiliasiakasohjelmien integraatioiden ja yrityskäyttöönoton edistyneisiin teknisiin puoliin.

### Q6: Mikä on virtuaalisten TAP/TUN-sovittimien tehtävä etäasiakkailla?

Ne toimivat virtuaalisina verkkokortteina ja reitittävät laitetason TCP/IP-liikenteen suoraan salattuun VPN-tunneliin.

### Q7: Miten IKEv2 MOBIKE tukee etätyöntekijöiden liikkuvuutta?

Se päivittää dynaamisesti IP-osoitesidonnat ja pitää VPN:n aktiivisena, kun käyttäjä siirtyy Wi-Fi-verkosta matkapuhelindataan.

### Q8: Mikä on jaetun ja täyden tunnelin reitityksen ero?

Täysi reititys pakottaa kaiken laitteen internetliikenteen VPN:n kautta, kun taas jaettu reititys lähettää vain yrityksen kohde-IP-osoitteet.

### Q9: Miten NAT-laitteet käsittelevät etä-VPN-yhteyksiä?

Yhdistämällä paikalliset porttialueet julkisiin yhdyskäytävän IP-osoitteisiin palaavien salattujen datapakettien reitittämiseksi.

### Q10: Mitkä vaatimustenmukaisuusstandardit edellyttävät etäkäytön tarkastusta?

Standardit, kuten HIPAA, SOC 2 ja PCI DSS, edellyttävät kaikkien etäyhteysistuntojen kirjaamista ja valvontaa.

# Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

Tutustu todellisiin tosiasioihin VPN-salauksen nopeuksista, protokollien auditoinneista, mobiiliyhteyksistä ja yritysten etätyöstä.

**1. VPN-OIVALLUS**

Etäkäyttö-VPN:t muodostavat suojattuja asiakas-sivusto-tunneleita toimipisteen ulkopuolella työskenteleville.

**2. VPN-OIVALLUS**

Vaatimustenmukaisuussäännöt edellyttävät monivaiheista tunnistautumista yritysten etäportaalien suojaamiseksi.

**3. VPN-OIVALLUS**

Laitetilatarkastukset varmistavat paikallisen asiakkaan tietoturva-asetukset ennen yksityisverkkoon pääsyn myöntämistä.

**4. VPN-OIVALLUS**

Syslog-palvelimet kokoavat yhteyslokeja luvattomien pääsyyritysten tarkastamiseksi ja havaitsemiseksi.

**5. VPN-OIVALLUS**

Yhdyskäytävän kaistapullonkaulat syntyvät, kun etäliikenteen yhteenlaskettu kysyntä ylittää palvelimen internetyhteyden rajat.

**6. VPN-OIVALLUS**

Virtuaaliset verkkosovittimet kapseloivat käyttöjärjestelmän verkkokyselyt suojattuihin protokolliin.

**7. VPN-TIETOA**

MOBIKE-tuki sallii etäasiakkaiden vaihtaa verkkoa VPN-tunnelin katkeamatta.

**8. VPN-TIETOA**

Täysi tunnelireititys suojaa kaiken työntekijöiden internetliikenteen mutta lisää yrityksen yhdyskäytävän kuormitusta.

**9. VPN-TIETOA**

Varmennetodennus sitoo VPN-yhteyden valtuutuksen suoraan yrityksen hallinnoimaan laitteistoon.

**10. VPN-OIVALLUS**

SOC 2:n ja PCI DSS:n kaltaiset viitekehykset edellyttävät etäkäyttöistuntojen lokitusta ja valvontaa.

# Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista teknisistä standardeista, määrittelyistä ja sääntelykehyksistä.

## TIETEELLISET JA ALAN VIITTEET

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

## Vastausavain: Tarkistuspiste 1 – Monivalinta

**1** **Kirjautumistunnisteet** MFA-TURVALLISUUS — **Oikea vastaus: A**

### OPETTAJALLE

Monivaiheinen tunnistautuminen vaatii kirjautumisille toissijaisen vahvistuksen. Lähde: MFA Implementation.

**2** **OpenVPN-tunneli** ASIAKAS–VERKKOON — **Oikea vastaus: A**

### OPETTAJALLE

OpenVPN on vakioprotokolla asiakas–sivusto-tunnelien suojaamiseen. Lähde: OpenVPN Client.

**3** **Laitetilatarkastukset** LAITETARKISTUS — **Oikea vastaus: A**

### OPETTAJALLE

Laitetilatarkastukset tarkistavat, että päätelaitteilla on aktiiviset palomuurit ja virustorjuntatyökalut. Lähde: Posture Compliance.

**4** **Lokien kokooja** SYSLOG-PALVELIN — **Oikea vastaus: A**

### OPETTAJALLE

Syslog-palvelimet keräävät tietoturvatapahtumalokeja pääsyrikkomusten valvontaa varten. Lähde: Syslog Standard.

**5** **Kortin ylivuoto** YHDYSKÄYTÄVÄN KAISTAPULLONKAULA — **Oikea vastaus: A**

### OPETTAJALLE

Yhdyskäytävän kaistapullonkaula syntyy, kun käyttäjien liikenne ylittää palvelimen rajat. Lähde: Capacity Planning.

## Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

**6** **Kirjautumistunnisteet** MFA-TARKISTUKSET — **Oikea vastaus: Tosi**

### OPETTAJALLE

Monivaiheinen tunnistautuminen vaatii kirjautumisille toissijaisen vahvistuksen. Lähde: MFA Implementation.

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

### OPETTAJALLE

Tilatarkistukset estävät laitteet, joiden palomuuri tai virustorjunta on pois päältä, joten tällaisilta laitteilta pääsy evätään.

**8** **Lokien kokooja** SYSLOG-PALVELIN — **Oikea vastaus: Tosi**

### OPETTAJALLE

Syslog-palvelimet keräävät tietoturvatapahtumalokeja pääsyrikkomusten valvontaa varten. Lähde: Syslog Standard.

**9** **Kysymys 9** — **Oikea vastaus: Epätosi**

### OPETTAJALLE

OpenVPN ja IPsec ovat nykyisiä protokollia, jotka salaavat etäasiakkaiden liikenteen.

**10** **Kortin ylivuoto** YHDYSKÄYTÄVÄN KAISTAPULLONKAULA — **Oikea vastaus: Tosi**

### OPETTAJALLE

Yhdyskäytävän kaistapullonkaula syntyy, kun käyttäjien liikenne ylittää palvelimen rajat. Lähde: Capacity Planning.

# 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. USEAN TEKIJÄN | D 2. OPENVPN | E 3. LAITETILA | B 4. SYSLOG |
| C 5. KAISTA | G 6. SALAUS | A 7. TUNNELOINTI | F 8. PALOMUURI |

## TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

| | | | |
|---|---|---|---|
| 1 MONIVAIHEINEN | 2 OPENVPN | 3 LAITEKUNTO | 4 SYSLOG |
| 5 KAISTA | 6 TUNNELOINTI | | |

## TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

| | | | |
|---|---|---|---|
| 1 D – SYSLOG | 2 H – PALOMUURI | 3 G – TUNNELOINTI | 4 F – SALAUS |
| 5 B – OPENVPN | 6 E – KAISTA | 7 C – LAITEKUNTO | 8 A – MONIVAIHEINEN |

## KESKUSTELUMUISTIINPANOT OPETTAJILLE

**Avaintermit:**
Tarkista, osaavatko oppilaat selittää termit USEAN TEKIJÄN, OPENVPN ja LAITETILA omin sanoin ja antaa jokaisesta esimerkin.

**Tapaustutkimukset:**
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

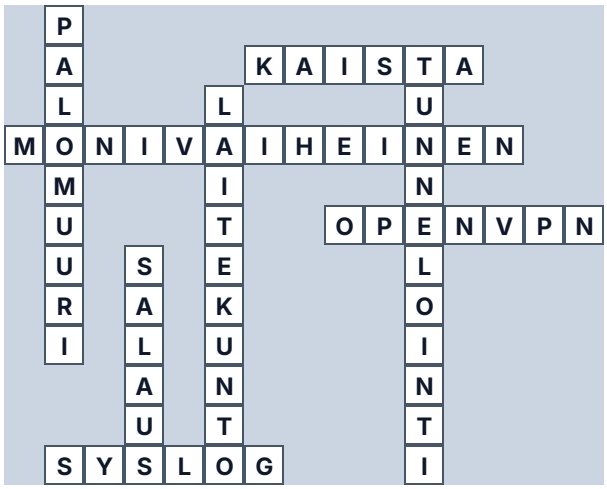
**Lähteiden arviointi:**
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

# Tehtäväavaimet ja opettajan muistiinpanot

## SANAHAUN RATKAISU

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

## RISTIKON RATKAISU




## OPETTAJAN OPAS RISTIKON RATKAISUIHIN

### VAAKASUORAAN

**2 vaakasuoraan: KAISTA** Verkon datakapasiteetin raja (6 kirjainta)

**5 vaakasuoraan: MONIVAIHEINEN** Kirjautumisen suojaus, joka vaatii lisätunnisteita (13 kirjainta)

**6 vaakasuoraan: OPENVPN** Asiakkaan ja palvelinverkon välinen vakioprotokolla (7 kirjainta)

**8 vaakasuoraan: SYSLOG** Keskitetty tietoturvalokien kerääjä (6 kirjainta)

### PYSTYSUORAAN

**1 pystysuoraan: PALOMUURI** Liikennettä suodattavan järjestelmän säännöt (9 kirjainta)

**3 pystysuoraan: TUNNELOINTI** Datan kapselointi suojattuun reittiin (11 kirjainta)

**4 pystysuoraan: LAITEKUNTO** Etälaitteen terveyden tarkistus (10 kirjainta)

**7 pystysuoraan: SALAUS** Pakettien kryptografinen sekoittaminen (6 kirjainta)

# Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

## SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. INEEAOHIMNNVI — **MONIVAIHEINEN**
2. TTLAEOUNKI — **LAITEKUNTO**
3. KISATA — **KAISTA**
4. OTILNENITUN — **TUNNELOINTI**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. USASLA — **SALAUS**
8. IMRPOAUUL — **PALOMUURI**

## SALAKIRJOITUSHAASTEEN AVAIN

**"ETÄYHTEYS VPN SUOJAA YRITYKSEN PÄÄTELAITTEET"**

# Tapaustutkimusten vastausavain

## A Tapaustutkimus 1: MFA:n pakottaminen

Opettajan ratkaisu

### ARVIOINTIOHJE

**Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:**

- Tilanneanalyysi: Liike-elämän analyytikko yrittää kirjautua yrityksen tietokantaan etätyössä. Hän syöttää oikean käyttäjätunnuksen ja salasanan, mutta VPN-portaali estää pääsyn ja vaatii fyysisen tunnistekoodin.
- Suositeltu strategia ja ratkaisu: Yrityksen VPN-portaali pakottaa tiukan monivaiheisen tunnistautumisen (MFA) käytännön etäkirjautumisten suojaamiseksi.

## B Tapaustutkimus 2: Suojaustason vaatimustenmukaisuus

Opettajan ratkaisu

### ARVIOINTIOHJE

**Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:**

- Tilanneanalyysi: Urakoitsija yhdistää henkilökohtaisen kannettavansa etäyritysverkkoon. VPN-asiakasohjelma katkaisee yhteyden heti ja ilmoittaa käyttäjälle, että hänen virustorjuntansa määrittelyt ovat vanhentuneet.
- Suositeltu strategia ja ratkaisu: Etäyhteyden yhdyskäytävä teki päätelaitteen tilatarkistuksen ja esti laitteen vanhentuneiden suojausasetusten vuoksi.