Nimi: _____ Päivämäärä: _____ Pisteet: _____

Yritys-VPN

Zero Trust -verkkokäytön, erillisten yhdyskäytäväsolmujen ja keskitettyjen yrityksen ylläpitäjän hallintatoimintojen käyttöönotto.

YRITYSTEN VPN-VERKOT: YLEISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: yritysten VPN-verkot. Tutustut Zero Trust -arkkitehtuureihin, erillisiin staattisiin IP-yhdyskäytäviin, ylläpitäjän konsoleihin, käyttöönottoon ja sivustojen välisiin IPsec-tunneleihin.

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/yritys/

Oppimispolkusi: yrityksen VPN-verkko

- Toteuta Zero Trust -verkkokäyttö (ZTNA) -viitekehykset.
- Määritä erillisten palvelinten yhdyskäytävien IP-osoitteet sallittujen luetteloiden suodattimia varten.
- Hallitse keskitettyjä yrityksen hallintapaneeleita ja käyttäjäpaikkaluetteloita.
- Auditoi verkkoyhteyksien käyttölokit ja käyttäjien yhteyshistoriat.
- Määritä kertakirjautumisen (SSO) ja monivaiheisen todennuksen säännöt.
- Määritä toimipisteiden väliset sivustojen väliset IPsec-tunnelit.

YRITYSTEN VPN-VERKKOJEN OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: Zero Trust ja sivustojen välinen IPsec. Lopuksi bonustehtävä Nopeat vastaukset.

ZERO TRUST -ARKKITEHTUURIT JA ERILLISET YHDYSKÄYTÄVÄT (JOHDANTO)

Yritysten VPN:t suojaavat yrityksen omaisuutta siirtymällä Zero Trust Network Access (ZTNA) -viitekehyksiin ja sallimalla vain omat kiinteät IP-yhdyskäytävät. IT-päälliköt käyttävät keskitettyjä hallintakonsoleita toimipisteiden välisten IPsec-tunnelien ja kertakirjautumislinkkien (SSO) ohjaamiseen.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. **1. Mikä turvallisuusmalli korvaa vanhat yritys-VPN:t?**
   - A) Nollaluottamus
   - B) Multi-hop
   - C) Vertaisverkko
   - D) Yksittäinen yhdyskäytävä

2. **2. Mikä ominaisuus vaaditaan tietokantakäytön rajaamiseksi yrityksen palvelimiin?**
   - A) Dedikoitu IP-osoite
   - B) Dynaaminen reititys
   - C) Jaettu tunneli
   - D) DNS-välityspalvelin

3. **3. Mikä protokolla on yritysten toimipisteiden välisten tunneleiden standardi?**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **4. Millä keskitetyllä työkalulla ylläpitäjät voivat hallita työntekijöiden käyttäjäpaikkoja?**
   - A) Hallintakonsoli
   - B) Rekisteriavain
   - C) Reitittimen laiteohjelmisto
   - D) Järjestelmäloki

5. **5. Mikä todennusstandardi mahdollistaa kirjautumisen Oktan tai Microsoft Entra ID:n kautta?**
   - A) Kertakirjautuminen
   - B) Jaettu salaisuus
   - C) EPP-todennus
   - D) WEP-avain

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Zero Trust Network Access myöntää pääsyn verkkoon vasta, kun laitteen luotettavuus on varmennettu jatkuvasti.

○ Tosi ○ Epätosi

7 Kysymys 7

7. Omat IP-yhdyskäytävät reitittävät työntekijöiden liikenteen satunnaisten julkisten kuluttajakäyttäjien liikenteen rinnalla.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Keskitetyt ylläpitokonsolit antavat IT-vastaaville mahdollisuuden perua yksittäisten työntekijöiden käyttäjäpaikat välittömästi.

○ Tosi ○ Epätosi

9 Kysymys 9

9. IPsec on kevyt protokolla, joka ei tue toimipisteiden välisiä verkkotunneleita.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Single Sign-On mahdollistaa työntekijöiden turvallisen todennuksen yrityksen identiteettipalveluntarjoajien avulla.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Nykyaikaiset tietoturva-arkkitehtuurit korvaavat vanhat tunnelit _____ -mallilla.

2. Tietokantojen käytön rajaamiseksi yritykset määrittävät yhdyskäytävälle sallittujen luettelon osoitteen, jota kutsutaan nimellä _____ .

3. Toimipisteet yhdistetään turvallisesti toisiinsa toimipisteiden välisillä _____ -tunneleilla.

4. IT-ylläpitäjät jakavat työntekijöiden käyttölisenssit keskitetyssä työkalussa nimeltä _____ .

5. Okta-integraatio mahdollistaa työntekijöiden todennuksen yhdellä kirjautumisella; toiminto on nimeltään _____ .

6. Kirjautumisten suojaamiseksi yritysportaalit edellyttävät tunnistautumista, joka on luonteeltaan _____ .

SANASTON SANAPANKKI

HALLINTANÄYTTÖ IPSEC KERTAKIRJAUS KIINTEÄ IP LISENSOINTI MONIVAIHEINEN NOLLALUOTTAMUS YHDYSKÄYTÄVÄ

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Keskeisten käsitteiden yhdistäminen

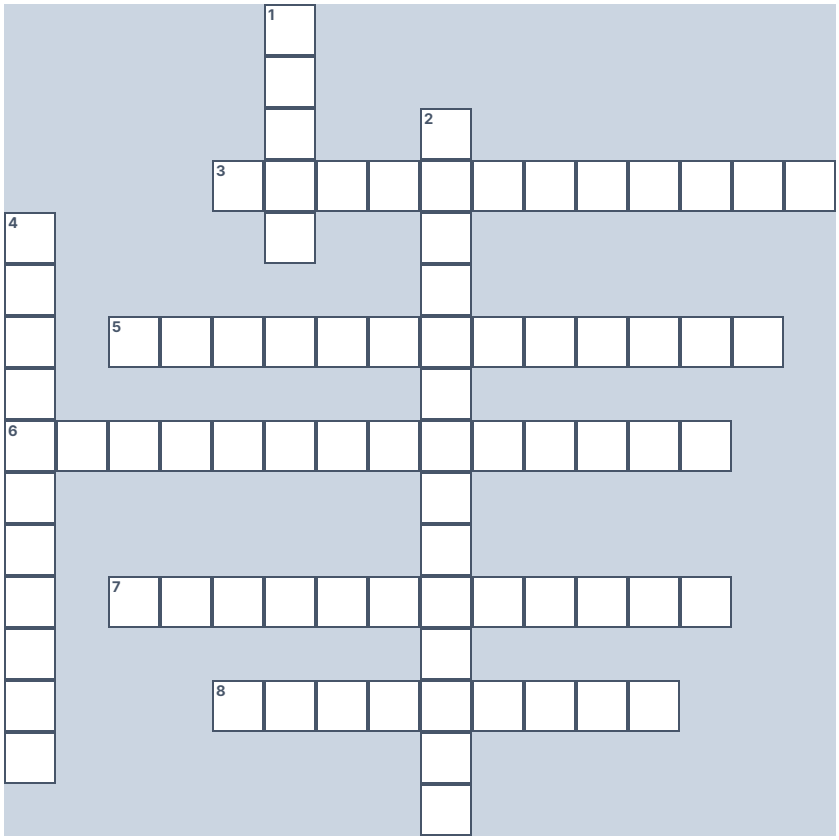
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. NOLLALUOTTAMUS	A	Työntekijöiden VPN-käyttölupien jakaminen.
☐	2. OMAIP	B	Oktan ja Entra ID:n identiteettiyhteys.
☐	3. IPSEC	C	Kirjautumisturva, joka vaatii lisätunnisteita.
☐	4. HALLINTAKONSOLI	D	Staattinen sallittujen luettelon yhdyskäytäväosoite.
☐	5. YHTEISKIRJAUTUMINEN	E	Sivustojen välisen tunnelin standardi.
☐	6. USEAN TEKIJÄN	F	Verkon sisääntulon reititysolmu.
☐	7. YHDYSKÄYTÄVÄ	G	Keskitetty IT-vastaavan käyttäjäpaikkojen portaali.
☐	8. VARAUS	H	Jatkuvan luottamuksen varmennuskehys.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

3. Okta- ja Entra ID -identiteettiyhteys (12)

5. Kirjautumisen suojaus, joka vaatii lisätunnisteita (13)

6. Jatkuvan luottamuksen varmennuksen viitekehys (14)

7. Verkon sisäänkäynnin reitityssolmu (12)

8. Kiinteä, sallittujen luetteloon lisätty yhdyskäytävän osoite (9)

PYSTYSUORAAN

1. Toimipisteiden välisen tunnelin standardi (5)

2. IT-ylläpitäjän keskitetty hallintaportaali (14)

4. Työntekijöiden VPN-käyttöoikeuksien jakaminen (11)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

3 vaakasuoraan: Okta- ja Entra ID -identiteettiyhteys (12 kirjainta):

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

6 vaakasuoraan: Jatkuvan luottamuksen varmennuksen viitekehys (14 kirjainta):

7 vaakasuoraan: Verkon sisäänkäynnin reitityssolmu (12 kirjainta):

8 vaakasuoraan: Kiinteä, sallittujen luetteloon lisätty yhdyskäytävän osoite (9 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Toimipisteiden välisen tunnelin standardi (5 kirjainta):

2 pystysuoraan: IT-ylläpitäjän keskitetty hallintaportaali (14 kirjainta):

4 pystysuoraan: Työntekijöiden VPN-käyttöoikeuksien jakaminen (11 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

NOLLALUOTTAMUS KIINTEÄIP IPSEC HALLINTANÄYTTÖ KERTAKIRJAUS
MONIVAIHEINEN YHDYSKÄYTÄVÄ LISENSOINTI

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. NOLLALUOTTAMUS**
- **B. KIINTEÄIP**
- **C. IPSEC**
- **D. HALLINTANÄYTTÖ**
- **E. KERTAKIRJAUS**
- **F. MONIVAIHEINEN**
- **G. YHDYSKÄYTÄVÄ**
- **H. LISENSOINTI**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Kiinteä, sallittujen luetteloon lisätty yhdyskäytävän osoite.
2. Verkon sisäänkäynnin reitityssolmu.
3. Työntekijöiden VPN-käyttöoikeuksien jakaminen.
4. Kirjautumisen suojaus, joka vaatii lisätunnisteita.
5. Toimipisteiden välisen tunnelin standardi.
6. Jatkuvan luottamuksen varmennuksen viitekehys.
7. Okta- ja Entra ID -identiteettiyhteys.
8. IT-ylläpitäjän keskitetty hallintaportaali.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. A L O T U L O T M N U S A L

2. I C E S P

3. K E R I U J R K S A A T

4. V Y S D Ä Ä K Ä T Y H Y

5. Ä T I P E N K I I

6. N T Y I L T A T Ä H A N Ö L

7. I N H A M O E V N E N I I

8. N O I S S L N I T I E

Bonustehtävä: Nopeat vastaukset

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

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

Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: ZERO TRUST -SIIRTYMÄ

👷

Tilanne: Yritys haluaa suojata paikalliset palvelimensa tarkistamalla jatkuvasti laitteiden vaatimustenmukaisuusvarmenteet, palomuurin tilan ja käyttäjän sijainnin sen sijaan, että luottaisi kehenkään verkon sisällä.

Keskustelukysymys: Minkä kehyksen IT-tietoturvajohtajan tulisi ottaa käyttöön tämän saavuttamiseksi?

TAPAUSTUTKIMUS 2: YHDYSKÄYTÄVÄN RAJOITUS

👷

Tilanne: Yritys isännöi yksityisiä rahoitustietokantoja pilvessä. Se haluaa estää kaiken julkisen internetyhteyden ylläpitopaneeleihin ja sallia kirjautumiset vain vahvistetuista yrityksen päätelaitteista.

Keskustelukysymys: Mikä verkkomääritys tietokannan ylläpitäjän tulisi tehdä pilven palomuuriin?

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

14	15	12	12	1	12	21	15	20	20	1	13	21	19

20	1	18	11	9	19	20	1	1		11	1	9	11	11	9

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 yritystason VPN?

Yrityksille suunniteltu suojattu verkkotunneli, jonka avulla etätyöntekijät voivat käyttää yrityksen verkkoja keskitetyllä hallinnalla.

Q2: Miten Zero Trust eroaa perinteisistä VPN:istä?

Perinteiset VPN:t luottavat kaikkiin tunnelin sisällä oleviin, kun taas Zero Trust varmentaa jatkuvasti jokaisen laitteen ja käyttäjän yhteyden.

Q3: Mikä on Dedicated IP yritys-VPN:issä?

Yksinomaan yrityksellesi varattu kiinteä IP-osoite, jonka voit sallia suojattua pilvitietokannan käyttöä varten.

Q4: Miksi kertakirjautuminen (SSO) on tärkeää yritys-VPN:issä?

Single Sign-On (SSO) antaa työntekijöiden kirjautua turvallisesti sisään yrityksen tunnuksillaan (kuten Okta tai Microsoft Entra ID).

Q5: Mikä on sivustosta sivustoon -VPN?

Tunneli, joka yhdistää kaksi fyysistä toimistoa (kuten sivutoimiston ja pääkonttorin) julkisen internetin yli IPsecin avulla.

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

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

Q6: Mikä on hallintakonsolin tehtävä?

Hallintapaneeli IT-ylläpitäjille työntekijöiden paikkojen lisäämiseen tai poistamiseen, yhdyskäytävien määrittämiseen ja aktiivisten yhteyksien valvontaan.

Q7: Miten MFA suojaa yritys-VPN:iä?

Vaatimalla toisen koodin (kuten todennussovelluksen tunnuksen) luvattoman pääsyn estämiseksi, jos salasanat ovat vaarantuneet.

Q8: Voinko tarkastaa työntekijöiden yhteyshistoriaa?

Kyllä, yrityskäytön VPN-palvelut tallentavat yhteyksien aikaleimat, kestot ja annetut IP-osoitteet vaatimustenmukaisuuden auditointia varten.

Q9: Mitä ZTNA on?

Zero Trust Network Access, tietoturvamalli, joka myöntää pääsyn vain tiettyihin sovelluksiin koko verkon sijaan.

Q10: Mikä on yhdyskäytäväsolmujen tehtävä?

Ne toimivat etäliikenteen suojattuina sisääntulopisteinä ja reitittävät datan suoraan yksityisille yrityspalvelimille.

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

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

Q1: Miten IPsec suojaa toimipisteiden välisen yritysviestinnän?

IPsec salaa liikenteen verkkokerroksella käyttäen Encapsulating Security Payload (ESP) -protokollaa tietojen luottamuksellisuuden ja eheyden varmistamiseksi.

Q2: Miksi vanha kehäpohjainen tietoturva ei toimi etätyöntekijöille?

Koska työntekijät käyttävät dataa useista sijainneista ja laitteista, yksittäinen verkon palomuurin ulkoreuna on vanhentunut.

Q3: Miten IT-päälliköt toteuttavat automaattisen käyttöönoton?

Yhdistämällä SCIM-protokollat identiteettipalveluntarjoajien (Okta) ja VPN-hallintakonsolin välillä käyttäjähakemistojen synkronoimiseksi.

Q4: Mikä on jaetun tunneloinnin hyöty yritysympäristöissä?

Se reitittää paikallisen SaaS-liikenteen (kuten Microsoft 365:n) VPN-tunnelin ulkopuolelle ja säästää yrityksen yhdyskäytävän kaistaa yksityisille tietokannoille.

Q5: Miten laitteen tilatarkistukset validoivat päätelaitteen tietoturvan?

VPN-asiakasohjelma tarkistaa laitteen ennen yhdistämistä varmistaakseen, että palomuuri on aktiivinen, virustorjunta on käynnissä ja käyttöjärjestelmän päivitykset ovat ajan tasalla.

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

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

Q6: Mikä rooli NAT-läpikäynnillä on yritys-VPN-käyttöönotoissa?

NAT-T kapseloi IPsec-paketit UDP:hen, jotta ne pääsevät kotireitittimien ja palomuurien läpi ilman yhteyskatkoksia.

Q7: Miten yritykset estävät yhdyskäytävän kaistanleveyden tukkeutumisen?

Ottamalla käyttöön useita alueellisia yhdyskäytäväsolmuja ja tasaamalla saapuvaa käyttäjäliikennettä niiden kesken kuormantasaajilla.

Q8: Miksi kiinteät IP-sallintalistat ovat parempia kuin dynaamiset?

Staattiset sallittujen luettelot estävät luvattomia ulkoisia IP-osoitteita yrittämästä yhteyskättelyjä, mikä pienentää hyökkäyspinta-alaa dramaattisesti.

Q9: Mikä rooli varmennepohjaisella todennuksella on yritys-VPN:issä?

Se validoi yrityksen hallinnoimille laitteille asennetut yksilölliset digitaaliset varmenteet ja estää hallinnoimattomat henkilökohtaiset tietokoneet.

Q10: Miten ZTNA pienentää sivuttaisliikkumisen riskiä?

Eristämällä käyttäjäistunnot tiettyihin valtuutettuihin resursseihin, mikä estää hakkereita liikkumasta verkossa, jos yksi solmu murretaan.

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

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

1. VPN-OIVALLUS

Zero Trust -arkkitehtuurit varmentavat jatkuvasti jokaisen verkkoyhteyttä yrittävän laitteen tietoturvatilan.

2. VPN-OIVALLUS

Omat IP-yhdyskäytävät antavat yritysten lukita pilvitietokannat sallimalla vain kiinteät osoitteet.

3. VPN-OIVALLUS

IPsec on alan standardiprotokolla suojattujen toimipisteiden välisten verkkotunnelien määrittämiseen.

4. VPN-OIVALLUS

Hallintakonsolien avulla IT-osastot voivat ottaa käyttöön, hallita ja auditoida työntekijöiden VPN-käyttöpaikkoja.

5. VPN-OIVALLUS

Single Sign-On yhdistää VPN-käytön yrityksen identiteettipalveluntarjoajiin, kuten Oktaan ja Entra ID:hen.

6. VPN-OIVALLUS

Monivaiheinen tunnistautuminen estää luvattomat yhteysyritykset, jotka perustuvat varastettuihin salasanoihin.

7. VPN-TIETOA

Jaettu tunnelointi optimoi yrityksen kaistaa sulkemalla julkisen SaaS-liikenteen pois salatusta tunnelista.

8. VPN-TIETOA

Laitteen tilatarkistukset varmistavat paikalliset suojausasetukset ennen pääsyn myöntämistä yrityksen palvelimille.

9. VPN-TIETOA

SCIM-hakemistosynkronointi automatisoi työntekijöiden käyttöoikeuksien hallinnan työsuhteen alkaessa ja päättyessä.

10. VPN-OIVALLUS

Zero Trust Network Access rajoittaa käyttäjien pääsyn tiettyihin valtuutettuihin sovelluksiin ja estää liikkumisen sivusuunnassa verkossa.

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/

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Zero Trust** ZTNA-MALLI **Oikea vastaus: A**

OPETTAJALLE

Zero Trust -mallit varmentavat laitteen vaatimustenmukaisuuden jatkuvasti ennen verkkoon pääsyä. Lähde: NIST Zero Trust.

2 **Oma IP-osoite** STAATTINEN IP **Oikea vastaus: A**

OPETTAJALLE

Omat IP-osoitteet mahdollistavat yhdyskäytävien sallittujen luetteloiden käytön julkisen liikenteen estämiseksi. Lähde: Dedicated IP Guide.

3 **IPsec-standardi** IPSEC-TUNNELI **Oikea vastaus: A**

OPETTAJALLE

IPsec on vakioprotokolla, jota käytetään sivutoimipisteiden välisissä tunneleissa. Lähde: IPsec Tunneling.

4 **IT-resurssien jako** HALLINTAKONSOLI **Oikea vastaus: A**

OPETTAJALLE

Keskitetyt ylläpidon ohjauspaneelit antavat IT-vastaaville mahdollisuuden jakaa käyttäjälisenssejä. Lähde: CISA Guidelines.

5 **Kysymys 5** **Oikea vastaus: A**

OPETTAJALLE

Mikä todennusstandardi mahdollistaa kirjautumisen Oktan tai Microsoft Entra ID:n kautta? → Kertakirjautuminen

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Zero Trust** ZTNA-TARKISTUKSET **Oikea vastaus: Tosi**

OPETTAJALLE

Zero Trust -mallit varmentavat laitteen vaatimustenmukaisuuden jatkuvasti ennen verkkoon pääsyä. Lähde: NIST Zero Trust.

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

OPETTAJALLE

Omat IP-osoitteet on varattu yhdelle yritykselle, joten sen liikennettä ei sekoiteta muiden käyttäjien kanssa.

8 **IT-resurssien jako** IT-YLLÄPITÄJÄN PAIKKA **Oikea vastaus: Tosi**

OPETTAJALLE

Keskitetyt ylläpidon ohjauspaneelit antavat IT-vastaaville mahdollisuuden jakaa käyttäjälisenssejä. Lähde: CISA Guidelines.

9 **IPsec-standardi** SIVUSTOSTA SIVUSTOON **Oikea vastaus: Epätosi**

OPETTAJALLE

IPsec on vakioprotokolla, jota käytetään sivutoimipisteiden välisissä tunneleissa. Lähde: IPsec Tunneling.

10 **Okta SSO -linkki** SSO-KIRJAUTUMINEN **Oikea vastaus: Tosi**

OPETTAJALLE

Single Sign-On yhdistää VPN-kirjautumiset yrityksen hakemistoihin, kuten Oktaan. Lähde: Okta SSO.

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. NOLLALUOTTAMUS	D 2. OMAIP	E 3. IPSEC	G 4. HALLINTAKONSOLI
B 5. YHTEISKIRJAUTUMINEN	C 6. USEAN TEKIJÄN	F 7. YHDYSKÄYTÄVÄ	A 8. VARAUS

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 NOLLALUOTTAMUS	2 KIINTEÄ IP	3 IPSEC	4 HALLINTANÄYTTÖ
5 KERTAKIRJAUS	6 MONIVAIHEINEN		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 B – KIINTEÄIP	2 G – YHDYSKÄYTÄVÄ	3 H – LISENSOINTI	4 F – MONIVAIHEINEN
5 C – IPSEC	6 A – NOLLALUOTTAMUS	7 E – KERTAKIRJAUS	8 D – HALLINTANÄYTTÖ

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit NOLLALUOTTAMUS, OMAIP ja IPSEC omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

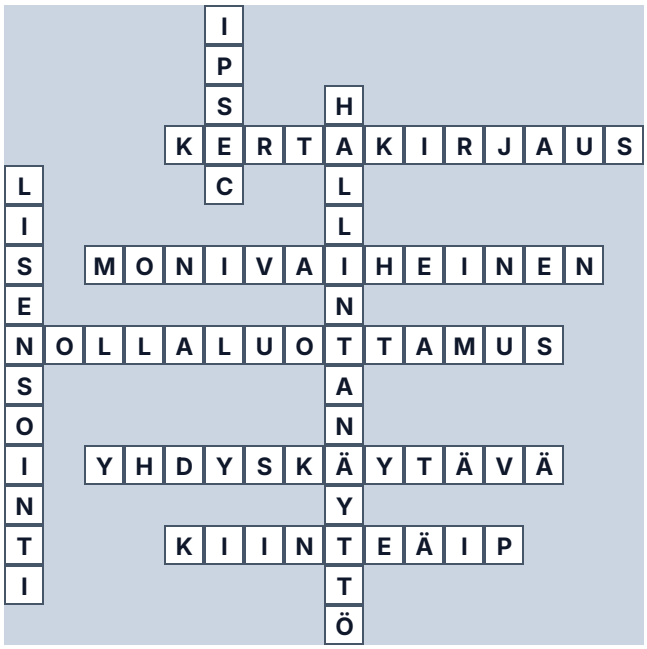
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

3 vaakasuoraan: KERTAKIRJAUS Okta- ja Entra ID -identiteettiyhteys (12 kirjainta)

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

6 vaakasuoraan: NOLLALUOTTAMUS Jatkuvan luottamuksen varmennuksen viitekehys (14 kirjainta)

7 vaakasuoraan: YHDYSKÄYTÄVÄ Verkon sisäänkäynnin reitityssolmu (12 kirjainta)

8 vaakasuoraan: KIINTEÄIP Kiinteä, sallittujen luetteloon lisätty yhdyskäytävän osoite (9 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: IPSEC Toimipisteiden välisen tunnelin standardi (5 kirjainta)

2 pystysuoraan: HALLINTANÄYTTÖ IT-ylläpitäjän keskitetty hallintaportaali (14 kirjainta)

4 pystysuoraan: LISENSOINTI Työntekijöiden VPN-käyttöoikeuksien jakaminen (11 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. ALOTULOTMNUSAL — **NOLLALUOTTAMUS**
2. ICESP — **IPSEC**
3. KERIUJRKSAAT — **KERTAKIRJAUS**
4. VYSDÄÄKÄTYHY — **YHDYSKÄYTÄVÄ**
5. ÄTIPENKII — **KIINTEÄIP**
6. NTYILTATÄHANÖL — **HALLINTANÄYTTÖ**
7. INHAMOEVNENII — **MONIVAIHEINEN**
8. NOISSLNITIE — **LISENSOINTI**

SALAKIRJOITUSHAASTEEN AVAIN

"NOLLALUOTTAMUS TARKISTAA KAIKKI LAITTEET"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Zero Trust -siirtymä

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yritys haluaa suojata paikalliset palvelimensa tarkistamalla jatkuvasti laitteiden vaatimustenmukaisuusvarmenteet, palomuurin tilan ja käyttäjän sijainnin sen sijaan, että luottaisi kaikkiin verkon sisällä oleviin.
- Suositeltu strategia ja ratkaisu: Johtajan tulisi siirtyä Zero Trust Network Access (ZTNA) -malliin, joka pakottaa jatkuvat kontekstipohjaiset turvatarkistukset.

B Tapaustutkimus 2: Yhdyskäytävän rajoitus

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yritys isännöi yksityisiä talouden tietokantoja pilvessä. Se haluaa estää kaiken julkisen internetyhteyden hallintapaneeleihin ja sallia kirjautumiset vain varmennetuista yrityksen päätelaitteista.
- Suositeltu strategia ja ratkaisu: Ylläpitäjän tulee määrittää yritys-VPN:ään Dedicated IP -yhdyskäytävä ja lisätä tämä staattinen osoite pilvitietokannan palomuurin sallittujen listalle.