Nama: _____ Tanggal: _____ Nilai: _____

# VPN Perusahaan

Menerapkan akses jaringan Zero Trust, node gerbang khusus, dan kontrol admin perusahaan terpusat.

## GAMBARAN PEMBELAJARAN JARINGAN VPN PERUSAHAAN

**PELAJAR**
**STATUS SISWA**
Jalur Pembela Jaringan

**AMAN**
**STATUS KONEKSI**
Melindungi paket data

**AKTIF**
**PERLINDUNGAN KEBOCORAN**
Perlindungan kebocoran DNS & IPv6

**Selamat datang! Paket aktivitas ini memandu Anda mempelajari** jaringan VPN perusahaan. Anda akan mempelajari arsitektur Zero Trust, gerbang IP statis khusus, konsol administrator, penugasan lisensi, dan terowongan IPsec antarlokasi.

**POS-POS LEMBAR KERJA**

- [ ] **Bagian 1-4: Kuasai konfigurasi VPN dan keamanan jaringan.**
- [ ] **Bagian 5-7: Selesaikan teka-teki silang & pencarian kata.**
- [ ] **Bagian 8-9: Selesaikan studi kasus & tantangan sandi.**
- [ ] **Bagian 10: Pelajari halaman FAQ dasar & lanjutan.**
- [ ] **Bagian 11: Jelajahi 10 fakta menarik dari dunia nyata.**
- [ ] **Bonus: Tantangan Berpikir Cepat.**

**Buka Panduan VPN Terbaik VPN.com**

URL: https://www.vpn.com/vpn/best-vpn-for-business/enterprise/

# Peta Belajar Jaringan VPN Perusahaan Anda

- Terapkan kerangka Zero Trust Network Access (ZTNA).
- Atur alamat IP gerbang server khusus untuk filter daftar putih.
- Kelola panel admin perusahaan terpusat dan daftar kursi pengguna.
- Audit log akses jaringan dan riwayat koneksi pengguna.
- Atur aturan Single Sign-On (SSO) dan autentikasi multifaktor.
- Siapkan terowongan IPsec antarlokasi dari cabang ke cabang.

## PETUNJUK JARINGAN VPN PERUSAHAAN

Jawab soal pilihan ganda dan benar/salah, lengkapi kalimat rumpang dengan bank kata, cocokkan definisi, serta selesaikan teka-teki silang dan pencarian kata. Terapkan pengetahuan Anda tentang Zero Trust dan IPsec antarlokasi. Akhiri dengan aktivitas bonus Berpikir Cepat.

## ARSITEKTUR ZERO TRUST & GERBANG KHUSUS (PENGANTAR)

VPN perusahaan mengamankan aset korporat dengan beralih ke kerangka Zero Trust Network Access (ZTNA) dan memasukkan gerbang IP statis khusus ke daftar putih. Manajer TI memakai konsol admin terpusat untuk mengatur terowongan IPsec antarlokasi dan tautan single sign-on (SSO).

**BACA SETIAP POS DENGAN SAKSAMA DAN PILIH ATAU TULIS JAWABAN YANG BENAR.**

## Pos 1: Tantangan Pilihan Ganda

1. **1. Model keamanan apa yang menggantikan VPN perusahaan lama?**
   - A) Zero Trust
   - B) Multi-hop
   - C) Peer-to-peer
   - D) Gerbang tunggal

2. **2. Fitur apa yang diperlukan untuk membatasi akses basis data ke server perusahaan?**
   - A) IP khusus
   - B) Routing dinamis
   - C) Split tunnel
   - D) Proxy DNS

3. **3. Protokol apa yang menjadi standar terowongan antarlokasi perusahaan?**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **4. Alat pusat apa yang memungkinkan administrator mengelola kursi karyawan?**
   - A) Konsol admin
   - B) Kunci registry
   - C) Firmware router
   - D) Log sistem

5. **5. Standar autentikasi apa yang memungkinkan login melalui Okta atau Microsoft Entra ID?**
   - A) Single Sign-On
   - B) Rahasia bersama (shared secret)
   - C) Autentikasi EPP
   - D) Kunci WEP

## Pos 2: Tantangan Benar atau Salah

**6 Pertanyaan 6**

6. Zero Trust Network Access memberi akses jaringan hanya setelah kepercayaan perangkat diverifikasi terus-menerus.

Benar Salah

**7 Pertanyaan 7**

7. Gerbang IP khusus mengalirkan lalu lintas karyawan bersama pengguna publik acak.

Benar Salah

**8 Pertanyaan 8**

8. Konsol admin terpusat memungkinkan manajer TI mencabut kursi karyawan secara langsung.

Benar Salah

**9 Pertanyaan 9**

9. IPsec adalah protokol ringan yang tidak mendukung terowongan jaringan antarlokasi.

Benar Salah

**10 Pertanyaan 10**

10. Single Sign-On memungkinkan autentikasi karyawan yang aman memakai penyedia identitas perusahaan.

Benar Salah

## Pos 3: Mengisi Istilah Kunci

Baca setiap kalimat di bawah ini dan isi bagian yang kosong dengan istilah yang tepat dari Bank Kata.

1. Arsitektur keamanan modern menggantikan terowongan lama dengan akses _____ .
2. Untuk membatasi akses basis data, perusahaan mengatur alamat gerbang _____ .
3. Kantor cabang dihubungkan dengan aman memakai terowongan antarlokasi _____ .
4. Administrator TI mengalokasikan lisensi pengguna karyawan di dalam _____ pusat.
5. Integrasi Okta memungkinkan karyawan melakukan autentikasi lewat _____ perusahaan.
6. Untuk melindungi login, portal perusahaan mewajibkan autentikasi _____ .

**BANK KATA KOSAKATA**

GERBANG IPKHUSUS IPSEC KONSOL ADMIN MULTIFAKTOR PENYEDIAAN SINGLE SIGN-ON ZERO TRUST

**Tulis jawaban Anda di sini:**

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

# Pos 4: Pencocokan Istilah Kunci

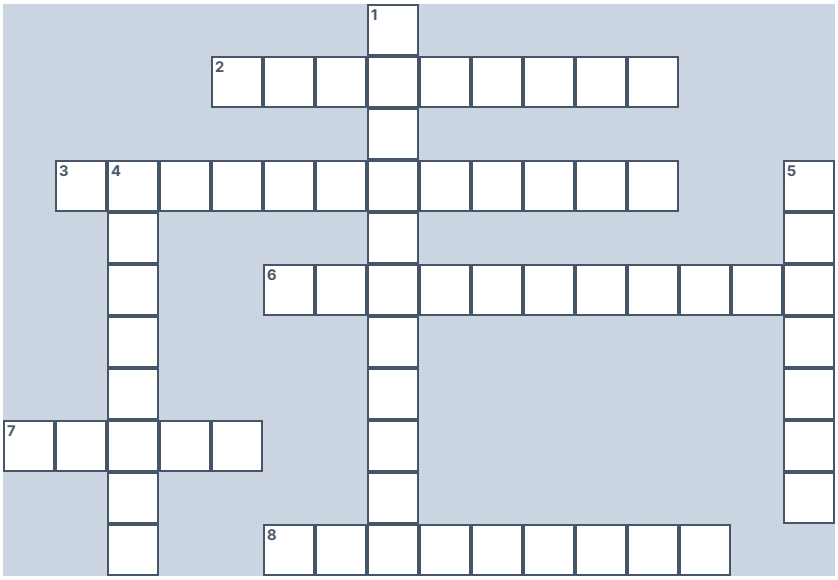
**MENCOCOKKAN DEFINISI**

Cocokkan setiap istilah di sebelah kiri dengan definisi yang benar di sebelah kanan dengan menulis huruf yang sesuai (A-H) di kotak isian.

| | | | |
|---|---|---|---|
| ☐ | 1. ZERO TRUST | A | Pengalokasian lisensi akses VPN karyawan. |
| ☐ | 2. IPKHUSUS | B | Penghubung identitas Okta dan Entra ID. |
| ☐ | 3. IPSEC | C | Keamanan login yang menuntut token tambahan. |
| ☐ | 4. KONSOL ADMIN | D | Alamat gerbang statis untuk daftar putih. |
| ☐ | 5. SINGLE SIGN-ON | E | Standar terowongan antarlokasi. |
| ☐ | 6. MULTIFAKTOR | F | Node routing pintu masuk jaringan. |
| ☐ | 7. GERBANG | G | Portal pusat manajer TI untuk mengelola kursi. |
| ☐ | 8. PENYEDIAAN | H | Kerangka verifikasi kepercayaan berkelanjutan. |

## Pos 5: Teka-Teki Silang

Selesaikan teka-teki silang dengan mengetik huruf di kotak putih yang aktif. Nomor-nomornya sesuai dengan petunjuk di bawah.



### PETUNJUK MENDATAR

**2. Kerangka verifikasi kepercayaan yang berkelanjutan (9)**

**3. Tautan identitas dengan Okta dan Entra ID (12)**

**6. Keamanan login yang meminta token tambahan (11)**

**7. Standar terowongan antarlokasi (site-to-site) (5)**

**8. Pembagian lisensi akses VPN kepada karyawan (9)**

### PETUNJUK MENURUN

**1. Portal pusat bagi manajer TI untuk mengelola kursi pengguna (11)**

**4. Alamat gerbang statis untuk daftar putih (8)**

**5. Node routing di pintu masuk jaringan (7)**

# Alternatif Pos 5: Petunjuk Teka-Teki Silang yang Aksesibel

Pengguna pembaca layar dan keyboard dapat mengetik jawaban teka-teki silang langsung di kolom teks di bawah ini.

## PETUNJUK MENDATAR

**2 mendatar: Kerangka verifikasi kepercayaan yang berkelanjutan (9 huruf):**

**3 mendatar: Tautan identitas dengan Okta dan Entra ID (12 huruf):**

**6 mendatar: Keamanan login yang meminta token tambahan (11 huruf):**

**7 mendatar: Standar terowongan antarlokasi (site-to-site) (5 huruf):**

**8 mendatar: Pembagian lisensi akses VPN kepada karyawan (9 huruf):**

## PETUNJUK MENURUN

**1 menurun: Portal pusat bagi manajer TI untuk mengelola kursi pengguna (11 huruf):**

**4 menurun: Alamat gerbang statis untuk daftar putih (8 huruf):**

**5 menurun: Node routing di pintu masuk jaringan (7 huruf):**

## Pos 6: Mencari Kata Tersembunyi

Temukan 8 istilah kunci yang tersembunyi dalam kisi di bawah ini. Kata dapat tersusun mendatar, menurun, atau diagonal.

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

**DAFTAR KOSAKATA**

ZEROTRUST IPKHUSUS IPSEC KONSOLADMIN SINGLESIGNON MULTIFAKTOR GERBANG PENUGASAN

# Alternatif Pos 6: Pencocokan Kosakata yang Aksesibel

Cocokkan kedelapan istilah dari Pencarian Kata dengan definisi yang benar dengan menulis hurufnya (A-H) di tempat kosong.

| ISTILAH KOSAKATA |
| --- |
| A. ZEROTRUST |
| B. IPKHUSUS |
| C. IPSEC |
| D. KONSOLADMIN |
| E. SINGLESIGNON |
| F. MULTIFAKTOR |
| G. GERBANG |
| H. PENUGASAN |

**DEFINISI & KOLOM PENCOCOKAN**

1. Alamat gerbang statis untuk daftar putih.
2. Node routing di pintu masuk jaringan.
3. Pembagian lisensi akses VPN kepada karyawan.
4. Keamanan login yang meminta token tambahan.
5. Standar terowongan antarlokasi (site-to-site).
6. Kerangka verifikasi kepercayaan yang berkelanjutan.
7. Tautan identitas dengan Okta dan Entra ID.
8. Portal pusat bagi manajer TI untuk mengelola kursi pengguna.

## Pos 7: Tantangan Kata Acak

Susun ulang huruf di bawah ini untuk menemukan konsep dan istilah kunci dari lembar kerja ini. Tulis jawaban Anda di kotak isian yang tersedia.

1. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. GEABNGR
5. USPSHIUK
6. ONLDIMKOANS
7. KIMUARTOLFT
8. NGAPUEASN

# Aktivitas Bonus: Berpikir Cepat

3 JAWABAN UNTUK SETIAP KATEGORI. ORANG PERTAMA YANG MELENGKAPI DAFTAR MENANG.

| | | | | |
|---|---|---|---|---|
| 1 | Alat yang dipakai perusahaan setiap hari | | | |
| 2 | Hal yang bisa disembunyikan VPN | | | |
| 3 | Peran di departemen TI | | | |
| 4 | Kata yang menggambarkan Zero Trust | | | |
| 5 | Cara masuk dengan aman | | | |
| 6 | Alasan memberi VPN kepada karyawan | | | |
| 7 | Hal yang dilakukan saat terjadi pembobolan | | | |
| 8 | Alasan memakai VPN saat bepergian | | | |
| 9 | Aturan kerja jarak jauh yang aman | | | |
| 10 | Data yang harus dilindungi perusahaan | | | |
| 11 | Hal yang mengganggu rapat video | | | |
| 12 | Perangkat yang bisa memakai VPN | | | |
| 13 | Program perkantoran yang Anda ketahui | | | |
| 14 | Tempat karyawan bekerja | | | |
| 15 | Perangkat yang dimiliki karyawan | | | |

# Pos 8: Studi Kasus VPN & Jaringan

Terapkan konsep yang telah Anda pelajari untuk menyelesaikan skenario nyata di bawah ini.

## STUDI KASUS 1: MIGRASI KE ZERO TRUST

👷

**Skenario: Sebuah perusahaan ingin mengamankan server lokalnya dengan memverifikasi** sertifikat kepatuhan perangkat, status firewall, dan lokasi pengguna secara terus-menerus, bukan memercayai siapa pun di dalam jaringan.

**Pertanyaan Diskusi: Kerangka apa yang harus diterapkan direktur keamanan TI untuk** mencapai hal ini?

## STUDI KASUS 2: PEMBATASAN GERBANG

👷

**Skenario: Sebuah perusahaan menyimpan basis data keuangan pribadi di cloud. Mereka ingin** memblokir semua akses internet publik ke panel admin dan hanya mengizinkan login dari endpoint perusahaan yang terverifikasi.

**Pertanyaan Diskusi: Konfigurasi jaringan apa yang harus disiapkan administrator basis data** pada firewall cloud?

# Pos 9: Memecahkan Sandi

Seorang insinyur jaringan mengamankan jalur routing dan terowongan klien. Gunakan kunci Huruf-ke-Angka di bawah untuk memecahkan pesan dengan menulis huruf yang sesuai di tempat kosong.

**KUNCI ENKRIPSI HURUF-KE-ANGKA**

**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**

| 22 | 5 | 18 | 9 | 6 | 9 | 11 | 1 | 19 | 9 | | 19 | 5 | 20 | 9 | 1 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | |
| 16 | 5 | 18 | 1 | 14 | 7 | 11 | 1 | 20 | | 19 | 5 | 2 | 5 | 12 | 21 | 13 |
| | | | | | | | | | | | | | | | | |
| | | 13 | 5 | 13 | 2 | 5 | 18 | 9 | | 1 | 11 | 19 | 5 | 19 | | |
| | | | | | | | | | | | | | | | | |

**Pesan yang dipecahkan:**

TIPS: SETIAP ANGKA MEWAKILI POSISI HURUF TERSEBUT DALAM ALFABET (MISALNYA 1 = A, 2 = B, 26 = Z).

# Pos 10: FAQ Dasar VPN (Bagian A)

Pelajari pertanyaan dan jawaban paling umum tentang Virtual Private Network (VPN) dan tunneling.

### Q1: Apa itu VPN perusahaan?

Terowongan jaringan aman untuk bisnis yang memungkinkan pekerja jarak jauh mengakses jaringan perusahaan dengan pengelolaan terpusat.

### Q2: Apa beda Zero Trust dengan VPN tradisional?

VPN tradisional memercayai siapa pun di dalam terowongan, sedangkan Zero Trust terus memverifikasi setiap perangkat dan koneksi pengguna.

### Q3: Apa itu IP khusus pada VPN bisnis?

Alamat IP statis yang khusus untuk bisnis Anda sehingga dapat dimasukkan ke daftar putih untuk akses basis data cloud yang aman.

### Q4: Mengapa SSO penting bagi VPN bisnis?

Single Sign-On memungkinkan karyawan menggunakan kredensial perusahaan (seperti Okta atau Microsoft Entra ID) untuk masuk dengan aman.

### Q5: Apa itu VPN antarlokasi?

Terowongan yang menghubungkan dua kantor fisik (misalnya cabang dan kantor pusat) melalui internet publik memakai IPsec.

# Pos 10: FAQ Dasar VPN (Bagian B)

Pelajari pertanyaan dan jawaban paling umum tentang Virtual Private Network (VPN) dan tunneling.

### Q6: Apa fungsi konsol admin?

Dasbor bagi administrator TI untuk menambah atau menghapus kursi karyawan, menetapkan gerbang, dan memantau koneksi aktif.

### Q7: Bagaimana MFA mengamankan VPN bisnis?

Dengan mewajibkan kode kedua (seperti token aplikasi autentikator) agar kata sandi yang bocor tidak cukup untuk masuk.

### Q8: Bisakah saya mengaudit riwayat koneksi karyawan?

Ya, VPN perusahaan mencatat stempel waktu koneksi, durasi, dan IP yang diberikan untuk audit kepatuhan.

### Q9: Apa itu ZTNA?

Zero Trust Network Access, model keamanan yang memberi akses hanya ke aplikasi tertentu, bukan ke seluruh jaringan.

### Q10: Apa peran node gerbang?

Node itu menjadi pintu masuk aman bagi lalu lintas jarak jauh dan meneruskan data langsung ke server perusahaan.

# Pos 10: FAQ Lanjutan VPN (Bagian C)

Jelajahi aspek teknis lanjutan dari protokol tunneling VPN, integrasi aplikasi seluler, dan penerapan di perusahaan.

### Q1: Bagaimana IPsec melindungi komunikasi antarlokasi perusahaan?

IPsec mengenkripsi lalu lintas di lapisan jaringan memakai Encapsulating Security Payload (ESP) untuk menjamin kerahasiaan dan keutuhan data.

### Q2: Mengapa keamanan berbasis perimeter gagal untuk tenaga kerja jarak jauh?

Karena karyawan mengakses data dari banyak lokasi dan perangkat sehingga perimeter firewall tunggal menjadi usang.

### Q3: Bagaimana manajer TI menerapkan penugasan otomatis?

Dengan memetakan protokol SCIM antara penyedia identitas (Okta) dan konsol admin VPN untuk menyinkronkan direktori pengguna.

### Q4: Apa manfaat split tunneling di lingkungan perusahaan?

Fitur ini merutekan lalu lintas SaaS lokal (seperti Microsoft 365) di luar tunnel VPN, sehingga bandwidth gerbang perusahaan tetap tersedia untuk database privat.

### Q5: Bagaimana pemeriksaan postur perangkat memvalidasi keamanan endpoint?

Aplikasi VPN memindai perangkat sebelum tersambung untuk memastikan firewall aktif, antivirus berjalan, dan patch sistem operasi terbaru.

# Pos 10: FAQ Lanjutan VPN (Bagian D)

Jelajahi aspek teknis lanjutan dari protokol tunneling VPN, integrasi aplikasi seluler, dan penerapan di perusahaan.

### Q6: Apa peran NAT traversal dalam penyiapan VPN bisnis?

NAT-T membungkus paket IPsec dalam UDP agar dapat melewati router rumah dan firewall tanpa koneksi terputus.

### Q7: Bagaimana bisnis mencegah bandwidth gerbang tersendat?

Dengan menyebar beberapa node gerbang regional dan menyeimbangkan lalu lintas masuk memakai penyeimbang beban.

### Q8: Mengapa daftar putih IP statis lebih disukai daripada yang dinamis?

Daftar putih statis mencegah IP luar tanpa izin mencoba jabat tangan koneksi sehingga permukaan serangan jauh berkurang.

### Q9: Apa peran autentikasi berbasis sertifikat pada VPN perusahaan?

Autentikasi ini memvalidasi sertifikat digital unik pada perangkat yang dikelola perusahaan dan memblokir komputer pribadi yang tidak dikelola.

### Q10: Bagaimana ZTNA mengurangi risiko pergerakan lateral?

Dengan mengisolasi sesi pengguna ke sumber daya tertentu yang diizinkan sehingga peretas tidak dapat menjelajah jaringan jika satu node ditembus.

## Bagian 11: 10 Fakta & Wawasan VPN di Dunia Nyata

Pelajari fakta nyata tentang kecepatan enkripsi VPN, audit protokol, konektivitas seluler, dan kerja jarak jauh di perusahaan.

**1. WAWASAN VPN**

Arsitektur Zero Trust terus memverifikasi status keamanan setiap perangkat yang mencoba terhubung ke jaringan.

**2. WAWASAN VPN**

Gerbang IP khusus memungkinkan bisnis mengunci basis data cloud dengan memasukkan alamat statis ke daftar putih.

**3. WAWASAN VPN**

IPsec adalah protokol standar industri untuk menyiapkan terowongan antarkantor yang aman.

**4. WAWASAN VPN**

Konsol admin memungkinkan departemen TI menugaskan, mengelola, dan mengaudit kursi akses VPN karyawan.

**5. WAWASAN VPN**

Single Sign-On mengintegrasikan akses VPN dengan penyedia identitas perusahaan seperti Okta dan Entra ID.

**6. WAWASAN VPN**

Autentikasi multifaktor memblokir upaya koneksi tanpa izin yang berasal dari kata sandi curian.

**7. WAWASAN VPN**

Split tunneling mengoptimalkan bandwidth perusahaan dengan mengeluarkan lalu lintas SaaS publik dari terowongan terenkripsi.

**8. WAWASAN VPN**

Pemeriksaan postur perangkat memverifikasi pengaturan keamanan lokal sebelum memberi akses ke server perusahaan.

**9. WAWASAN VPN**

Sinkronisasi direktori SCIM mengotomatiskan kontrol akses saat karyawan masuk dan keluar.

**10. WAWASAN VPN**

Zero Trust Network Access membatasi akses pengguna ke aplikasi tertentu yang diizinkan sehingga mencegah pergerakan lateral di jaringan.

# Referensi & Sumber Teknis

Panduan belajar dan teka-teki interaktif ini disusun berdasarkan standar teknis, spesifikasi, dan kerangka regulasi global.

## REFERENSI AKADEMIK & INDUSTRI

[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/

## Kunci Jawaban: Pos 1 - Pilihan Ganda

**1** **Zero Trust** MODEL ZTNA **Jawaban Benar: A**

### CATATAN PENGAJAR

Model Zero Trust terus memverifikasi kepatuhan perangkat sebelum masuk ke jaringan.

**2** **IP Khusus** IP STATIS **Jawaban Benar: A**

### CATATAN PENGAJAR

Alamat IP khusus memungkinkan gerbang masuk daftar putih untuk memblokir lalu lintas publik.

**3** **Standar IPsec** TEROWONGAN IPSEC **Jawaban Benar: A**

### CATATAN PENGAJAR

IPsec adalah protokol standar untuk terowongan antarlokasi cabang.

**4** **Alokasi TI** KONSOL ADMIN **Jawaban Benar: A**

### CATATAN PENGAJAR

Dasbor admin terpusat memungkinkan manajer TI mengalokasikan lisensi kursi.

**5** **Soal 5** **Jawaban Benar: A**

### CATATAN PENGAJAR

Standar autentikasi apa yang memungkinkan login melalui Okta atau Microsoft Entra ID? → Single Sign-On

## Kunci Jawaban: Pos 2 - Benar atau Salah

**6** **Zero Trust** PEMERIKSAAN ZTNA — Jawaban Benar: Benar

### CATATAN PENGAJAR

Model Zero Trust terus memverifikasi kepatuhan perangkat sebelum masuk ke jaringan.

**7** **Soal 7** — Jawaban Benar: Salah

### CATATAN PENGAJAR

IP khusus dicadangkan untuk satu perusahaan, sehingga lalu lintasnya tidak bercampur dengan pengguna lain.

**8** **Alokasi TI** KURSI ADMIN TI — Jawaban Benar: Benar

### CATATAN PENGAJAR

Dasbor admin terpusat memungkinkan manajer TI mengalokasikan lisensi kursi.

**9** **Standar IPsec** ANTARLOKASI — Jawaban Benar: Salah

### CATATAN PENGAJAR

IPsec adalah protokol standar untuk terowongan antarlokasi cabang.

**10** **Tautan SSO Okta** LOGIN SSO — Jawaban Benar: Benar

### CATATAN PENGAJAR

Single Sign-On memadukan login VPN dengan direktori perusahaan seperti Okta.

# Kunci Kosakata & Rubrik Penilaian

**Rubrik Penilaian Pengajar: Berikan 1 poin untuk setiap pencocokan yang benar (total 8 poin) dan setiap istilah konteks yang benar (total 6 poin).**

## POS 4: KUNCI PENCOCOKAN KONSEP

| | | | |
|---|---|---|---|
| H 1. ZERO TRUST | D 2. IPKHUSUS | E 3. IPSEC | G 4. KONSOL ADMIN |
| B 5. SINGLE SIGN-ON | C 6. MULTIFAKTOR | F 7. GERBANG | A 8. PENYEDIAAN |

## POS 3: KUNCI ISTILAH KUNCI

| | | | |
|---|---|---|---|
| 1 ZERO TRUST | 2 IPKHUSUS | 3 IPSEC | 4 KONSOL ADMIN |
| 5 SINGLE SIGN-ON | 6 MULTIFAKTOR | | |

## ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

| | | | |
|---|---|---|---|
| 1 B – IPKHUSUS | 2 G – GERBANG | 3 H – PENUGASAN | 4 F – MULTIFAKTOR |
| 5 C – IPSEC | 6 A – ZEROTRUST | 7 E – SINGLESIGNON | 8 D – KONSOLADMIN |

## CATATAN DISKUSI UNTUK PENGAJAR

**Istilah Kunci:**
Pastikan siswa dapat menjelaskan ZERO TRUST, IPKHUSUS, dan IPSEC dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

**Studi Kasus:**
Minta siswa mendukung rekomendasi mereka dengan fakta dari lembar kerja, bukan asumsi.

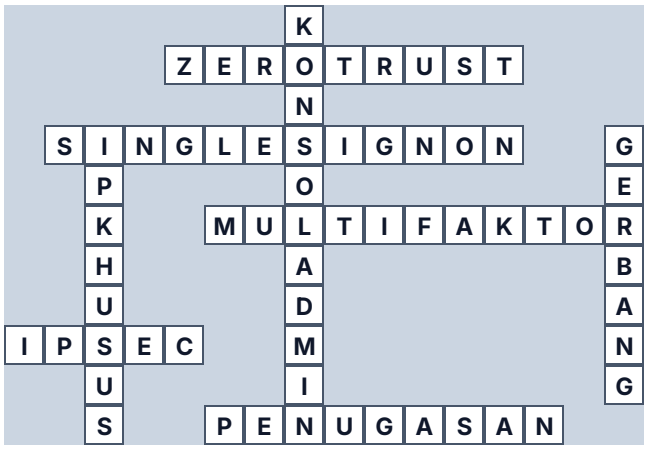
**Evaluasi Sumber:**
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

# Kunci Teka-Teki & Catatan Pengajar

## JAWABAN PENCARIAN KATA

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

## JAWABAN TEKA-TEKI SILANG




## PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

### PETUNJUK MENDATAR

**2 mendatar: ZEROTRUST** Kerangka verifikasi kepercayaan yang berkelanjutan (9 huruf)

**3 mendatar: SINGLESIGNON** Tautan identitas dengan Okta dan Entra ID (12 huruf)

**6 mendatar: MULTIFAKTOR** Keamanan login yang meminta token tambahan (11 huruf)

**7 mendatar: IPSEC** Standar terowongan antarlokasi (site-to-site) (5 huruf)

**8 mendatar: PENUGASAN** Pembagian lisensi akses VPN kepada karyawan (9 huruf)

### PETUNJUK MENURUN

**1 menurun: KONSOLADMIN** Portal pusat bagi manajer TI untuk mengelola kursi pengguna (11 huruf)

**4 menurun: IPKHUSUS** Alamat gerbang statis untuk daftar putih (8 huruf)

**5 menurun: GERBANG** Node routing di pintu masuk jaringan (7 huruf)

# Kunci Jawaban Kata Acak & Sandi

Kunci penilaian untuk aktivitas menyusun kata acak dan Tantangan Sandi Rahasia.

## KUNCI KATA ACAK

| | | | | | |
|---|---|---|---|---|---|
| 1. | RTOEZUSTR | ZEROTRUST | 5. | USPSHIUK | IPKHUSUS |
| 2. | ICESP | IPSEC | 6. | ONLDIMKOANS | KONSOLADMIN |
| 3. | SIISOGNENLNG | SINGLESIGNON | 7. | KIMUARTOLFT | MULTIFAKTOR |
| 4. | GEABNGR | GERBANG | 8. | NGAPUEASN | PENUGASAN |

### KUNCI TANTANGAN SANDI RAHASIA

**"VERIFIKASI SETIAP PERANGKAT SEBELUM MEMBERI AKSES"**

# Kunci Jawaban Studi Kasus

## A Studi Kasus 1: Migrasi ke Zero Trust

Jawaban Pengajar

### PEDOMAN PENILAIAN

**Jawaban siswa harus mencakup poin-poin berikut:**

- Analisis Skenario: Perusahaan ingin mengamankan server lokalnya dengan memverifikasi sertifikat kepatuhan perangkat, status firewall, dan lokasi pengguna secara terus-menerus, bukan memercayai siapa pun di dalam jaringan.
- Strategi & Solusi yang Disarankan: Direktur itu sebaiknya bermigrasi ke model Zero Trust Network Access (ZTNA), yang menerapkan pemeriksaan keamanan berbasis konteks secara terus-menerus.

## B Studi Kasus 2: Pembatasan Gerbang

Jawaban Pengajar

### PEDOMAN PENILAIAN

**Jawaban siswa harus mencakup poin-poin berikut:**

- Analisis Skenario: Perusahaan menyimpan basis data keuangan pribadi di cloud dan ingin memblokir semua akses internet publik ke panel admin, hanya mengizinkan login dari endpoint perusahaan yang terverifikasi.
- Strategi & Solusi yang Disarankan: Administrator sebaiknya menyiapkan gerbang IP khusus pada VPN perusahaan dan memasukkan alamat statis itu ke daftar putih firewall basis data cloud.