Nama: _____ Tanggal: _____ Nilai: _____

Cara Memilih VPN Lembar Kerja

Menilai penyedia VPN, standar keamanan, audit, dan kebijakan log

GAMBARAN PEMBELAJARAN VPN

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 prinsip dasar Virtual Private Network (VPN). Anda akan mempelajari bagaimana terowongan terenkripsi mengamankan data Anda, bagaimana protokol jaringan bekerja, dan cara mengenali serta mencegah kebocoran privasi.

POS-POS LEMBAR KERJA

- [ ] **Bagian 1-4: Kuasai konsep dan protokol VPN.**
- [ ] **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 VPN.com

URL: https://www.vpn.com/id/vpn/

Peta Belajar VPN Anda

- Nilai yurisdiksi penyedia dan kebijakan tanpa log demi privasi.
- Bandingkan protokol tunneling seperti WireGuard dan OpenVPN dari sisi kecepatan.
- Analisis fitur keamanan seperti kill switch dan node server hanya-RAM.
- Kenali audit keamanan independen dan paket harga saat memilih.
- Pilih lokasi server sesuai kebutuhan kecepatan dan pembukaan blokir wilayah.

PETUNJUK LEMBAR KERJA PEMILIHAN

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 dalam memilih infrastruktur VPN yang aman. Akhiri dengan aktivitas bonus Berpikir Cepat.

MEMILIH VPN (PENGANTAR)

Memilih VPN yang tepat berarti tidak terkecoh promosi. Penyedia yang andal harus punya kebijakan tanpa log yang terbukti, protokol enkripsi yang aman, dan klien open source. Dengan menilai fitur keamanan, yurisdiksi, dan kecepatan, Anda dapat memilih VPN yang sesuai kebutuhan perlindungan digital Anda.

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

Pos 1: Tantangan Pilihan Ganda

1 **1. Apa faktor kunci saat memilih penyedia VPN yang aman?**

- A. Jumlah negara server
- B. Kebijakan tanpa log yang diaudit secara independen
- C. Harga bulanan termurah
- D. Sponsor iklan yang mencolok

2 **2. Protokol VPN mana yang paling seimbang antara kecepatan dan kemudahan audit?**

- A. PPTP (Lama)
- B. L2TP/IPSec
- C. OpenVPN lewat TCP saja
- D. WireGuard

3 **3. Mengapa VPN gratis sebaiknya dihindari untuk aktivitas sensitif?**

- A. Dilarang di Amerika Serikat
- B. Sering menjual riwayat penjelajahan Anda
- C. Tidak mendukung penjelajahan web dasar
- D. Memerlukan perangkat keras khusus

4 **4. Apa yang ditentukan oleh yurisdiksi hukum asal penyedia?**

- A. Kecepatan koneksi server
- B. Jenis perangkat yang didukung
- C. Hukum setempat soal retensi data dan surat perintah penggeledahan
- D. Tema tampilan aplikasi klien

5 **5. Apa fungsi utama fitur 'kill switch' pada klien VPN?**

- A. Memblokir akses internet jika koneksi VPN terputus
- B. Menghapus semua aplikasi di perangkat
- C. Menggandakan kecepatan koneksi server
- D. Memulai ulang sistem operasi saat menganggur

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. VPN melindungi perangkat Anda dari unduhan malware dan berkas virus.

Benar Salah

7 Pertanyaan 7

7. Audit independen dari firma seperti Deloitte memverifikasi klaim tanpa log.

Benar Salah

8 Pertanyaan 8

8. Hukum negara asal penyedia tidak memengaruhi privasi data pengguna.

Benar Salah

9 Pertanyaan 9

9. Kode WireGuard yang ringkas lebih mudah diaudit daripada OpenVPN.

Benar Salah

10 Pertanyaan 10

10. VPN gratis sering menjual iklan atau melacak pengguna untuk menutup biaya server.

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. Kebijakan tanpa _____ mewajibkan penyedia VPN untuk tidak mencatat riwayat online Anda.

2. Protokol modern _____ memberi kecepatan tinggi dengan kode yang sangat ringkas.

3. Fitur keamanan bernama _____ menghentikan semua lalu lintas jika koneksi VPN tiba-tiba gagal.

4. Menilai _____ hukum penyedia menentukan apakah mereka terikat perjanjian pengawasan.

5. Mengamankan server dengan disk _____ membantu mencegah data pengguna tertinggal setelah reboot.

6. Memverifikasi klaim tanpa pengetahuan memerlukan _____ keamanan pihak ketiga dari firma tepercaya.

BANK KATA KOSAKATA

AUDIT FIVE EYES HANYA-RAM KILL SWITCH TANPA LOG VPN GRATIS WIREGUARD YURISDIKSI

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Jaringan

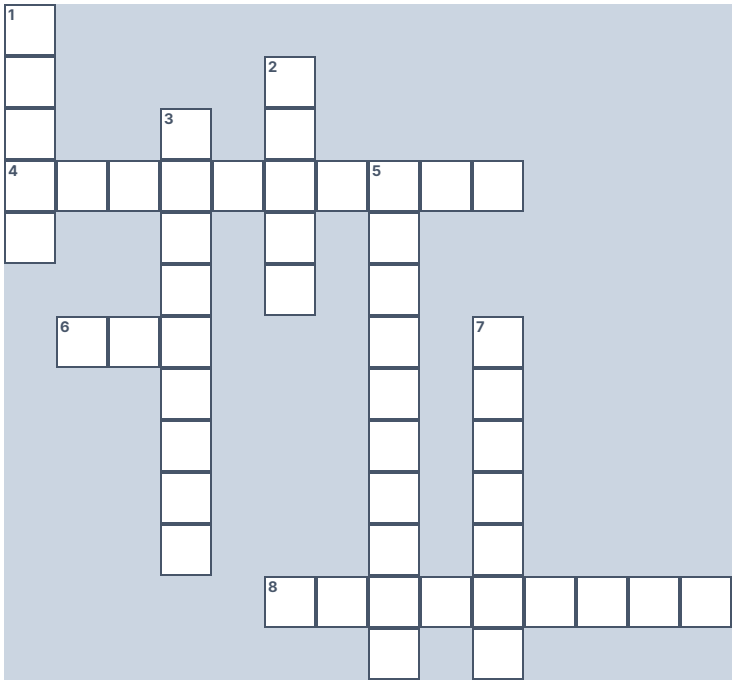
MENCOCOKKAN DEFINISI

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

☐	1. WireGuard	A	Layanan koneksi berisiko tinggi yang sering mencari untung dengan mencatat dan menjual data browser.
☐	2. Log Teraudit	B	Mekanisme pengaman yang memblokir perutean internet jika terowongan aman terputus.
☐	3. Yurisdiksi	C	Aliansi berbagi intelijen antara AS, Inggris, Kanada, Australia, dan Selandia Baru.
☐	4. Kill Switch	D	Infrastruktur perangkat keras yang berjalan di memori volatil, sehingga data tidak disimpan di disk.
☐	5. Five Eyes	E	Wilayah geografis yang menentukan kewajiban hukum penyedia VPN.
☐	6. VPN Gratis	F	Protokol modern dan cepat dengan sekitar 4.000 baris kode yang mudah diaudit.
☐	7. Server Hanya-RAM	G	Protokol open source yang matang dan telah banyak diaudit, dengan basis kode jauh lebih besar daripada WireGuard.
☐	8. OpenVPN	H	Klaim privasi yang diverifikasi firma keamanan siber pihak ketiga yang independen.

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

4. Wilayah geografis yang mengatur kewajiban hukum penyedia VPN (10)

6. Catatan aktivitas pengguna yang sebaiknya tidak disimpan penyedia VPN (3)

8. Laju koneksi yang perlu diuji sebelum memilih VPN (9)

PETUNJUK MENURUN

1. Harga langganan; VPN gratis sering menutupnya dengan mencatat dan menjual data penjelajahan (5)

2. Pemeriksaan oleh firma keamanan siber independen yang memverifikasi klaim privasi (5)

3. Protokol modern dan cepat dengan sekitar 4.000 baris kode yang mudah diaudit (9)

5. Mekanisme pengaman yang memblokir internet jika terowongan aman terputus (10)

7. Protokol open source matang yang banyak diaudit, dengan basis kode jauh lebih besar daripada WireGuard (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

4 mendatar: Wilayah geografis yang mengatur kewajiban hukum penyedia VPN (10 huruf):

6 mendatar: Catatan aktivitas pengguna yang sebaiknya tidak disimpan penyedia VPN (3 huruf):

8 mendatar: Laju koneksi yang perlu diuji sebelum memilih VPN (9 huruf):

PETUNJUK MENURUN

1 menurun: Harga langganan; VPN gratis sering menutupnya dengan mencatat dan menjual data penjelajahan (5 huruf):

2 menurun: Pemeriksaan oleh firma keamanan siber independen yang memverifikasi klaim privasi (5 huruf):

3 menurun: Protokol modern dan cepat dengan sekitar 4.000 baris kode yang mudah diaudit (9 huruf):

5 menurun: Mekanisme pengaman yang memblokir internet jika terowongan aman terputus (10 huruf):

7 menurun: Protokol open source matang yang banyak diaudit, dengan basis kode jauh lebih besar daripada WireGuard (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.

C R I G N R M O P X Q O C U S

T E A L J B A P B C A P X L K

H Y Y K X T K E D Q U M J D I

C N A N K Q P N G M D M Q R S

T T I T G Y C V S Q I O H W S

I B B W D U S P Z V T C Z I W

W F K H Z R D N K N D Q X R P

S C U B A I Z N E D K A D E O

L D F H I S D R C Q M E I G R

L Z S F Q D L V E F A A Q U O

I N P T X I O Q P K R U S A D

K N Y B F K G S A X W J A R R

Z Y Y L G S I M T R J M L D T

O H Q Q H I Z A A O V G U B Y

R Y B H L Z G J N O P N W C M

DAFTAR KOSAKATA

AUDIT YURISDIKSI WIREGUARD OPENVPN LOG KECEPATAN KILLSWITCH BIAYA

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. AUDIT
B. YURISDIKSI
C. WIREGUARD
D. OPENVPN
E. LOG
F. KECEPATAN
G. KILLSWITCH
H. BIAYA

DEFINISI & KOLOM PENCOCOKAN

1. Catatan aktivitas pengguna yang sebaiknya tidak disimpan penyedia VPN.
2. Pemeriksaan oleh firma keamanan siber independen yang memverifikasi klaim privasi.
3. Harga langganan; VPN gratis sering menutupnya dengan mencatat dan menjual data penjelajahan.
4. Laju koneksi yang perlu diuji sebelum memilih VPN.
5. Protokol open source matang yang banyak diaudit, dengan basis kode jauh lebih besar daripada WireGuard.
6. Mekanisme pengaman yang memblokir internet jika terowongan aman terputus.
7. Protokol modern dan cepat dengan sekitar 4.000 baris kode yang mudah diaudit.
8. Wilayah geografis yang mengatur kewajiban hukum penyedia VPN.

Pos 7: Tantangan Kata Acak

Susun ulang huruf di bawah ini untuk menemukan konsep dan istilah kunci VPN. Tulis jawaban Anda di kotak isian.

1. **IDATU** _____
2. **DWREIUAGR** _____
3. **GOL** _____
4. **WCSHLTIKIL** _____
5. **KDIUIISYSR** _____
6. **PEVONNP** _____
7. **AKANTEEPC** _____
8. **ABAYI** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Hal yang bisa disembunyikan VPN			
2	Hal yang lebih penting daripada harga			
3	Tempat membaca ulasan VPN			
4	Hal yang tidak bisa dicegah VPN			
5	Pertanyaan untuk penjual VPN			
6	Hal yang bisa dilihat penyedia internet Anda			
7	Hal di daftar periksa saat memilih VPN			
8	Tempat Anda akan memakai VPN			
9	Tanda bahaya pada penyedia VPN			
10	Kata yang berkaitan dengan privasi			
11	Hal yang pertama kali Anda uji			
12	Janji penyedia VPN yang baik			
13	Alasan memakai VPN saat bepergian			
14	Perangkat yang bisa memakai VPN			
15	Mitos tentang VPN			

Pos 8: Studi Kasus VPN

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

SARAH (MAHASISWI DI KEDAI KOPI)

👩‍💻 "Hai! Aku sedang di Coffee & Bytes. Ada jaringan publik tanpa pengamanan bernama 'Free_Wi-Fi_No_Password'. Aku ingin masuk ke email sekolah dan mengunggah tugas, tapi aku khawatir soal peretas. Apa risikonya memakai jaringan ini tanpa VPN, dan bagaimana VPN mengamankan dataku?"

ALEX (MAHASISWA YANG SEDANG BEPERGIAN)

👩‍💻 "Aduh! Aku sedang ke luar negeri untuk sebuah proyek dan ingin menonton dokumenter biologi yang ada di server di negaraku. Tapi situsnya bilang 'Video ini tidak tersedia di lokasi Anda saat ini.' Kenapa aku diblokir, dan bagaimana VPN bisa membantuku menontonnya?"

Pos 9: Memecahkan Sandi

Untuk menuntaskan latihan panduan memilih ini, pecahkan pesan tersembunyi tentang memilih infrastruktur yang aman. Pesan yang dipecahkan:

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

2 1 14 4 9 14 7 11 1 14 12 1 16 15 18 1 14

4 5 14 7 1 14 19 9 19 20 5 13 25 1 14 7

1 13 1 14

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 penggunaan virtual private network.

Q1: Apa itu VPN dan bagaimana cara kerjanya?

Virtual Private Network (VPN) mengenkripsi koneksi internet Anda dan meneruskan lalu lintas melalui server jarak jauh yang aman. Ini menyamarkan alamat IP publik Anda dan membatasi apa yang dapat dilihat pengamat jaringan lokal dan ISP Anda tentang lalu lintas yang melewati terowongan VPN.

Q2: Mengapa saya harus menggunakan VPN?

VPN melindungi privasi digital Anda, mengamankan koneksi di Wi-Fi publik (seperti kedai kopi atau bandara), dapat mengurangi pelambatan berdasarkan aktivitas karena ISP tidak dapat mengenali jenis lalu lintas terenkripsi, menembus pembatasan geografis untuk mengakses konten global, dan membantu mengamankan sumber daya kerja jarak jauh.

Q3: Apakah VPN membuat saya sepenuhnya anonim di internet?

Tidak. Meskipun VPN menyembunyikan alamat IP dan mengenkripsi lalu lintas, Anda tetap bisa dilacak melalui cookie browser, akun yang aktif (seperti Google atau Facebook), sidik jari browser, atau jika penyedia VPN mencatat data Anda.

Q4: Apakah VPN akan memperlambat internet saya?

Ya, sedikit. Proses enkripsi dan jarak fisik ke server VPN menambah latensi dan beban. Dampaknya bergantung pada penyedia, protokol, jarak server, perangkat, dan kondisi jaringan.

Q5: Bagaimana VPN tersebut menghasilkan uang?

Periksa model bisnisnya. Langganan, tingkatan freemium, dan penjualan data semuanya memengaruhi seberapa jauh Anda dapat memercayai VPN, dan layanan yang tidak pernah mengumpulkan data Anda tidak dapat menjualnya. Baca kebijakan privasinya terlebih dahulu. [1]

Pos 10: FAQ Dasar VPN (Bagian B)

Pelajari pertanyaan dan jawaban paling umum tentang penggunaan virtual private network.

Q6: Bolehkah saya memakai VPN gratis?

VPN gratis mungkin mengandalkan iklan, fitur terbatas, analitik penggunaan, batas data, atau model monetisasi lain. Pengguna sebaiknya memeriksa kebijakan privasi, kepemilikan, audit, dan model bisnis penyedia sebelum menggunakannya.

Q7: Apa itu kebijakan "tanpa log"?

Kebijakan tanpa log menjelaskan data aktivitas dan koneksi mana yang menurut penyedia tidak disimpan. Cakupannya berbeda-beda, jadi pembaca sebaiknya memeriksa kebijakan tersebut dan hasil audit independen.

Q8: Bagaimana cara memilih VPN terbaik?

Carilah kebijakan tanpa log yang sudah diaudit, protokol yang kuat (WireGuard, OpenVPN), lokasi server yang aman, kecepatan tinggi, server khusus RAM, fitur kill switch, dan yurisdiksi di luar aliansi berbagi intelijen (seperti 5/9/14 Eyes).

Q9: Bisakah saya memakai VPN di ponsel dan smart TV?

Ya. Penyedia VPN modern menyediakan aplikasi khusus untuk iOS, Android, macOS, Windows, Linux, dan smart TV, serta pengaturan router untuk melindungi semua perangkat di jaringan rumah Anda.

Q10: Apa itu Kill Switch?

Kill Switch adalah fitur keamanan yang otomatis memutus perangkat Anda dari internet jika koneksi VPN terputus. Ini mencegah data yang tidak terenkripsi atau alamat IP asli Anda bocor.

Pos 10: FAQ Lanjutan VPN (Bagian C)

Jelajahi aspek teknis dan struktural dari virtual private network dan protokol tunneling yang aman.

Q1: Apa perbedaan WireGuard, OpenVPN, dan IKEv2?

WireGuard adalah protokol modern dan ringan (hanya sekitar 4.000 baris kode) yang menawarkan kecepatan tinggi dan koneksi cepat. OpenVPN adalah protokol open source yang sangat aman dan sudah teruji. IKEv2 sangat cocok untuk perangkat seluler karena dapat tersambung kembali dengan cepat saat berpindah jaringan.

Q2: Apa itu double VPN atau routing Multi-Hop?

Multi-Hop merutekan lalu lintas Anda melalui dua atau lebih server VPN secara berurutan. Ini menambahkan lapisan enkripsi kedua dan membantu menyembunyikan alamat IP asli Anda dari hop kedua jika salah satu server disusupi.

Q3: Apa itu kebocoran WebRTC dan bagaimana VPN mencegahnya?

WebRTC adalah protokol browser yang dapat mengungkap alamat IP lokal dan publik asli Anda meskipun VPN aktif. VPN premium memblokir atau memalsukan permintaan WebRTC di aplikasi desktop/seluler dan ekstensi browser mereka.

Q4: Apa itu server khusus RAM dan mengapa penting?

Server tradisional menulis data ke hard drive, yang dapat disita atau disusupi. Server khusus RAM (tanpa disk) berjalan sepenuhnya di memori volatil (RAM). Saat server di-reboot atau dimatikan, data yang tersimpan di memori terhapus.

Q5: Bagaimana Obfuscation menembus pemblokiran VPN?

Obfuscation (atau "Stealth VPN") menyamarkan paket lalu lintas VPN agar terlihat seperti lalu lintas web HTTPS biasa (port 443). Ini membantu melewati Deep Packet Inspection (DPI) yang digunakan pemerintah atau jaringan sekolah/kantor untuk memblokir VPN.

Pos 10: FAQ Lanjutan VPN (Bagian D)

Jelajahi aspek teknis dan struktural dari virtual private network dan protokol tunneling yang aman.

Q6: Apa itu Split Tunneling dan kapan sebaiknya digunakan?

Split Tunneling memungkinkan Anda memilih aplikasi mana yang dirutekan melalui tunnel VPN terenkripsi dan mana yang terhubung langsung ke internet. Gunakan fitur ini untuk merutekan aplikasi perbankan yang sensitif melalui VPN sementara game lokal terhubung langsung, sehingga terhindar dari latensi tambahan akibat VPN.

Q7: Bagaimana cara kerja Forward Secrecy (Perfect Forward Secrecy)?

PFS memastikan kunci enkripsi sementara yang unik dibuat untuk setiap sesi. Meskipun kunci privat dibobol di masa depan, kunci itu tidak dapat digunakan untuk membuka sesi sebelumnya atau berikutnya karena setiap sesi memakai kunci tersendiri.

Q8: Apa itu aliansi 5/9/14 Eyes dan mengapa saya perlu peduli?

Yurisdiksi dapat memengaruhi proses hukum yang mungkin dihadapi penyedia, tetapi risiko privasi yang nyata juga bergantung pada data yang disimpan penyedia, arsitektur teknisnya, kepemilikan, laporan transparansi, dan riwayat auditnya.

Q9: Apa itu perlindungan kebocoran DNS?

Perlindungan kebocoran DNS memaksa perangkat Anda mengirim permintaan pencarian situs (kueri DNS) melalui server DNS pribadi VPN yang terenkripsi, bukan server ISP Anda. Ini mencegah ISP melacak situs yang Anda kunjungi.

Q10: Mengapa perlu memeriksa siapa yang menjalankan dan mendukung sebuah VPN?

Reputasi itu penting. Telusuri pemilik dan pimpinan perusahaan, cari audit pihak ketiga yang dipublikasikan, dan periksa pendapat pakar keamanan independen serta media sebelum Anda memercayainya. [1]

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

Pelajari fakta dan wawasan nyata yang sangat berharga tentang sejarah, pasar, dan teknologi VPN.

1. PROTOKOL VPN PERTAMA

PPTP (Point-to-Point Tunneling Protocol), protokol VPN awal dari kelompok yang dipimpin Microsoft pada 1990-an, kini dianggap tidak aman, sehingga VPN modern menggunakan WireGuard atau OpenVPN. [1]

2. NILAI PASAR

Pasar VPN global telah tumbuh pesat, didorong oleh meningkatnya kebutuhan kerja jarak jauh dan tuntutan keamanan perusahaan.

3. REVOLUSI WIREGUARD

WireGuard memiliki basis kode yang sangat ramping dan dirancang untuk efisiensi, sehingga lebih mudah diaudit untuk mencari kerentanan keamanan dibandingkan protokol tradisional. [3]

4. STANDAR AUDIT YANG KETAT

Penyedia VPN terkemuka menyewa firma seperti Deloitte, KPMG, atau PwC untuk memeriksa klaim tanpa log, dan perusahaan keamanan seperti Cure53 untuk menguji aplikasi dan server mereka. [4]

5. ASAL-USUL ALIANSI 5-EYES

Kemitraan intelijen Five Eyes yang terdiri dari AS, Inggris, Kanada, Australia, dan Selandia Baru berawal dari kerja sama intelijen sinyal antara Sekutu di era Perang Dunia II.

6. DEEP PACKET INSPECTION

Firewall canggih menerapkan Deep Packet Inspection (DPI) untuk menganalisis metadata paket jaringan dan memblokir karakteristik koneksi VPN standar.

7. PENGGUNAAN DI PERUSAHAAN

Banyak organisasi memberi karyawan jarak jauh VPN untuk mengakses sistem internal seperti basis data, sehingga VPN menjadi alat keamanan yang umum di tempat kerja.

8. VPN TERDESENTRALISASI

VPN terdesentralisasi (dVPN) menyebarkan lalu lintas ke jaringan node yang dijalankan oleh sesama pengguna, sehingga mengurangi ketergantungan pada satu penyedia terpusat.

9. ANONIMITAS TOR VS. VPN

VPN menyalurkan lalu lintas melalui satu penyedia, sedangkan Tor (The Onion Router) mengirimkan lalu lintas melalui tiga relai sukarelawan (guard, middle, exit) untuk memaksimalkan privasi. [5]

10. BIAYA PELANGGARAN DATA

Menggabungkan VPN dengan model akses zero-trust, yang memeriksa setiap pengguna dan perangkat, membantu organisasi melindungi data dan membatasi kerusakan akibat pelanggaran data.

Referensi & Sumber Teknis

Publikasi, spesifikasi kriptografis, dan standar dokumen resmi yang dikutip dalam lembar kerja ini.

REFERENSI AKADEMIK & INDUSTRI

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

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

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

Kunci Jawaban: Menilai penyedia VPN, standar keamanan, audit, dan kebijakan log

1 **Kebijakan Log Teraudit** PROTOKOL — **Jawaban Benar: B**

CATATAN PENGAJAR

Kebijakan tanpa log yang diaudit secara independen adalah cara paling praktis untuk memeriksa klaim privasi zero-knowledge sebuah penyedia. Pemasaran yang mencolok atau klaim sepihak tidaklah cukup.

2 **Keunggulan WireGuard** LATENSI — **Jawaban Benar: D**

CATATAN PENGAJAR

WireGuard menawarkan perutean koneksi modern dan cepat di kernel dengan kode ringkas (~4.000 baris), sehingga audit sangat efisien.

3 **Soal 3** — **Jawaban Benar: B**

CATATAN PENGAJAR

VPN gratis tetap membayar server, dan FTC memperingatkan bahwa beberapa aplikasi VPN membagikan data pengguna kepada pihak ketiga, misalnya untuk menampilkan iklan.

4 **Yurisdiksi Hukum** KONTROL ROUTING — **Jawaban Benar: C**

CATATAN PENGAJAR

Yurisdiksi menentukan apakah VPN tunduk pada hukum pengawasan, kewajiban retensi data, dan panggilan paksa rahasia dari pemerintah.

5 **Perlindungan Kill Switch** PRIVASI — **Jawaban Benar: A**

CATATAN PENGAJAR

Kill switch langsung memutus perutean adaptor jaringan jika terowongan terputus, sehingga IP asli dan DNS tidak bocor.

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Batasan terhadap Malware** PENYAMARAN IP — **Jawaban Benar: Salah**

CATATAN PENGAJAR

VPN menyediakan jalur terenkripsi yang aman, tetapi tidak memindai muatan atau berkas. Antivirus tetap diperlukan untuk memblokir malware.

7 **Audit Independen** KECEPATAN — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Laporan audit memverifikasi konfigurasi perangkat lunak server, kepatuhan penyiapan hanya-RAM, dan tidak adanya basis data log.

8 **Soal 8** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Penyedia harus mematuhi hukum negara asalnya, yang dapat mencakup aturan retensi data dan perintah untuk menyerahkan data yang mereka simpan.

9 **Ukuran Kode Protokol** FIREWALL — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Kode yang lebih kecil mengurangi celah serangan dan memudahkan tim keamanan memverifikasi keutuhan protokol.

10 **Monetisasi Iklan** TANPA LOG — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Tanpa biaya langganan, VPN gratis mengandalkan penambangan data, pemrofilan lalu lintas, dan sisipan iklan browser untuk mendapat pemasukan.

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

F 1. WireGuard	H 2. Log Teraudit	E 3. Yurisdiksi	B 4. Kill Switch
C 5. Five Eyes	A 6. VPN Gratis	D 7. Server Hanya-RAM	G 8. OpenVPN

POS 3: KUNCI ISTILAH KUNCI

1 TANPA LOG	2 WIREGUARD	3 KILL SWITCH	4 YURISDIKSI
5 HANYA-RAM	6 AUDIT		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 E – LOG	2 A – AUDIT	3 H – BIAYA	4 F – KECEPATAN
5 D – OPENVPN	6 G – KILLSWITCH	7 C – WIREGUARD	8 B – YURISDIKSI

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan WireGuard, Log Teraudit, dan Yurisdiksi dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

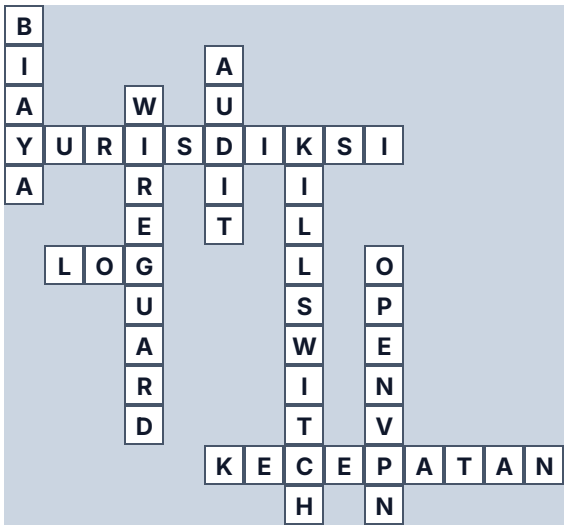
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

4 mendatar: YURISDIKSI Wilayah geografis yang mengatur kewajiban hukum penyedia VPN (10 huruf)

6 mendatar: LOG Catatan aktivitas pengguna yang sebaiknya tidak disimpan penyedia VPN (3 huruf)

8 mendatar: KECEPATAN Laju koneksi yang perlu diuji sebelum memilih VPN (9 huruf)

PETUNJUK MENURUN

1 menurun: BIAYA Harga langganan; VPN gratis sering menutupnya dengan mencatat dan menjual data penjelajahan (5 huruf)

2 menurun: AUDIT Pemeriksaan oleh firma keamanan siber independen yang memverifikasi klaim privasi (5 huruf)

3 menurun: WIREGUARD Protokol modern dan cepat dengan sekitar 4.000 baris kode yang mudah diaudit (9 huruf)

5 menurun: KILLSWITCH Mekanisme pengaman yang memblokir internet jika terowongan aman terputus (10 huruf)

7 menurun: OPENVPN Protokol open source matang yang banyak diaudit, dengan basis kode jauh lebih besar daripada WireGuard (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1. IDATU	AUDIT	5. KDIUIISYSR	YURISDIKSI
2. DWREIUAGR	WIREGUARD	6. PEVONNP	OPENVPN
3. GOL	LOG	7. AKANTEEPC	KECEPATAN
4. WCSHLTIKIL	KILLSWITCH	8. ABAYI	BIAYA

KUNCI TANTANGAN SANDI RAHASIA

"BANDINGKAN LAPORAN DENGAN SISTEM YANG AMAN"

Kunci Jawaban Studi Kasus

A Skenario A: Keamanan Jaringan Publik

SNIFFING & ENKRIPSI | Dilema Sarah

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Risiko: Penyadapan paket, pencegatan data, dan serangan man-in-the-middle. Seseorang di jaringan kedai kopi yang sama dapat menangkap data login atau file tugasnya.
- Perlindungan VPN: Mengenkripsi isi paket jaringan sehingga lalu lintas terowongan yang dicegat tidak dapat dibaca oleh penyadap pasif di jaringan lokal jika VPN dikonfigurasi dengan benar.

B Skenario B: Mengakses Sumber yang Diblokir

GEOBLOKIR & IP | Dilema Alex

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Mengapa Diblokir: Layanan streaming memakai pemblokiran geografis yang mencocokkan alamat IP lokal Alex dengan negara tempat ia berada dan memblokirnya berdasarkan lisensi wilayah.
- Bagaimana VPN Membantu: Menyamarkan lokasi aslinya dengan meneruskan lalu lintas melalui server di negara asalnya. Situs melihat IP dari negara asal sehingga akses diizinkan.