Nama: _____ Tanggal: _____ Nilai: _____

Cara Menyembunyikan Alamat IP Lembar Kerja

Menyembunyikan alamat IP, penyamaran lokasi, proksi, Tor, dan pencegahan kebocoran DNS/WebRTC

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

- Jelaskan cara kerja alamat IP dan bagaimana alamat itu membocorkan lokasi.
- Bandingkan proksi, Tor, dan VPN untuk menyamarkan alamat jaringan.
- Kenali cara mendeteksi dan mencegah kebocoran DNS dan WebRTC.
- Pahami bagaimana situs web melacak pengguna lewat IP publiknya.
- Nilai perutean multi-hop dan terowongan terenkripsi untuk melindungi IP.

PETUNJUK LEMBAR KERJA PERLINDUNGAN IP

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 menyembunyikan alamat IP dan mencegah kebocoran. Akhiri dengan aktivitas bonus Berpikir Cepat.

MENYEMBUNYIKAN IP ANDA (PENGANTAR)

Alamat IP Anda adalah alamat surat digital yang mengungkap lokasi fisik dan kebiasaan jaringan Anda. Menyembunyikan IP adalah garis pertahanan pertama terhadap pelacakan online, pembuatan profil sasaran, dan pemblokiran berbasis geolokasi. Memahami cara menyamarkan alamat Anda dengan aman membantu melindungi privasi Anda secara online.

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

Pos 1: Tantangan Pilihan Ganda

1 **1. Apa yang diungkap alamat IP publik sebuah perangkat kepada situs web yang Anda kunjungi?**

- A. Nomor kartu kredit pengguna
- B. Perkiraan lokasi Anda dan nama ISP Anda
- C. Seluruh direktori berkas lokal
- D. Pengaturan bahasa keyboard

2 **2. Metode mana yang menyembunyikan IP dan mengenkripsi seluruh lalu lintas sistem?**

- A. Proksi web standar
- B. Menghapus cookie browser
- C. Virtual Private Network (VPN)
- D. Mematikan firewall bawaan

3 **3. Apa kelemahan privasi utama proksi web gratis?**

- A. Tidak mengenkripsi lalu lintas data di jaringan publik
- B. Harus memasang sistem operasi lain
- C. Sepenuhnya ilegal di Amerika Serikat
- D. Memerlukan sambungan saluran telepon khusus

4 **4. Bagaimana jaringan Tor memberikan anonimitas tinggi kepada penggunanya?**

- A. Dengan mempercepat koneksi
- B. Dengan merutekan lalu lintas melalui tiga relai yang dijalankan sukarelawan
- C. Dengan mendaftarkan nama Anda ke basis data global
- D. Dengan membatasi akses hanya untuk lembaga pemerintah

5 **5. Apa itu kebocoran DNS?**

- A. Kesalahan mengirim email ke alamat yang salah
- B. Saat kueri DNS melewati terowongan VPN dan menuju ISP
- C. Kerusakan catu daya router lokal
- D. Pembaruan driver adaptor jaringan lokal

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Server proksi mengenkripsi lalu lintas latar belakang sistem operasi seperti VPN.

○ Benar ○ Salah

7 Pertanyaan 7

7. Perutean Tor sangat aman tetapi memperlambat penjelajahan.

○ Benar ○ Salah

8 Pertanyaan 8

8. Kebocoran WebRTC dapat membuka IP asli Anda saat sesi VPN aktif.

○ Benar ○ Salah

9 Pertanyaan 9

9. Saat VPN aktif dan tidak ada kebocoran, ISP Anda tidak dapat melihat situs web yang Anda kunjungi.

○ Benar ○ Salah

10 Pertanyaan 10

10. Menyembunyikan alamat IP memblokir pelacakan lewat sidik jari browser.

○ 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. Kueri domain yang lolos dari terowongan aman disebut _____ .

2. API komunikasi _____ berbasis browser dapat tanpa sengaja membocorkan alamat IP asli Anda.

3. _____ web mengalihkan lalu lintas browser tetapi tidak mengenkripsi muatan paket.

4. Enkripsi berlapis jaringan _____ memberi tingkat anonimitas yang tinggi.

5. _____ publik Anda diberikan penyedia telekomunikasi dan menunjukkan wilayah Anda.

6. Menembus blokir media regional dilakukan lewat _____ lokasi.

BANK KATA KOSAKATA

ALAMAT IP KEBOCORAN DNS LOKASI PENYAMARAN PROKSI TEROWONGAN VPN TOR WEBRTC

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Jaringan

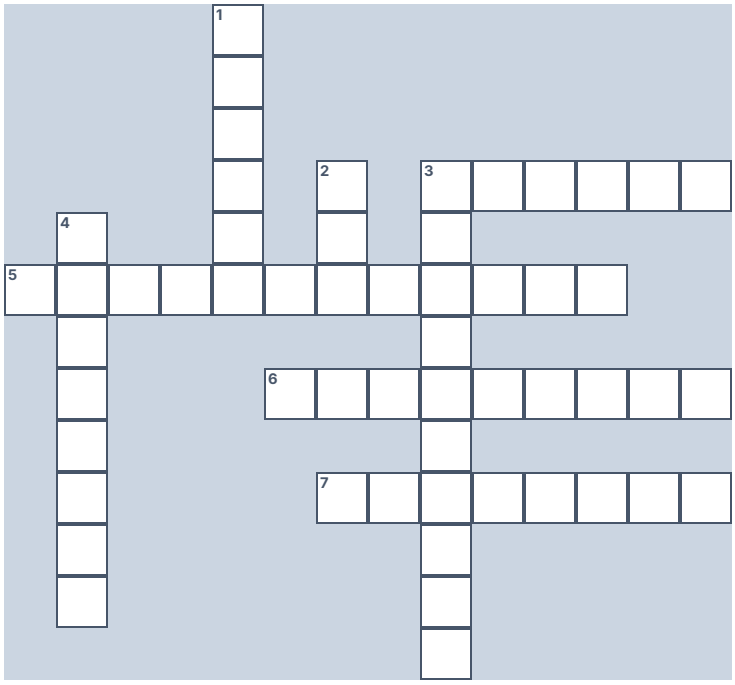
MENCOCOKKAN DEFINISI

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

☐	1. Alamat IP	A	Mengenkripsi semua lalu lintas perangkat dan merutekannya melalui server VPN.
☐	2. Terowongan VPN	B	Merutekan data lewat tiga server sukarela dengan enkripsi berlapis di setiap tahap.
☐	3. Jaringan Tor	C	Merutekan koneksi lewat server negara lain untuk menembus blokir wilayah.
☐	4. Proksi Web	D	Label angka unik yang mengenali antarmuka perangkat di internet.
☐	5. Kebocoran DNS	E	Mengalihkan lalu lintas browser di lapisan aplikasi tanpa enkripsi sistem.
☐	6. API WebRTC	F	Pencatatan tujuan lalu lintas internet tanpa enkripsi oleh penyedia telekomunikasi Anda.
☐	7. Penyamaran Lokasi	G	Kueri yang diproses di luar terowongan VPN sehingga domain yang dikunjungi terlihat oleh ISP.
☐	8. Pelacakan ISP	H	Fitur browser untuk suara/video yang dapat melewati terowongan dan membuka alamat IP asli.

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

3. Pengalihan lalu lintas browser di lapisan aplikasi tanpa enkripsi tingkat sistem (6)

5. Kueri yang di-resolve di luar terowongan VPN sehingga domain yang dikunjungi terlihat oleh ISP (12)

6. Pencatatan tujuan lalu lintas internet tanpa enkripsi oleh penyedia telekomunikasi Anda (9)

7. Label numerik unik yang mengidentifikasi antarmuka perangkat di internet (8)

PETUNJUK MENURUN

1. Fitur browser untuk suara/video yang dapat melewati terowongan dan mengungkap alamat IP asli (6)

2. Merutekan data melalui tiga server sukarelawan dengan lapisan enkripsi di setiap langkah (3)

3. Perutean koneksi melalui server di negara lain untuk menembus blokir geografis (10)

4. Pengarahan seluruh lalu lintas perangkat yang terenkripsi melalui server VPN (8)

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

3 mendatar: Pengalihan lalu lintas browser di lapisan aplikasi tanpa enkripsi tingkat sistem (6 huruf):

5 mendatar: Kueri yang di-resolve di luar terowongan VPN sehingga domain yang dikunjungi terlihat oleh ISP (12 huruf):

6 mendatar: Pencatatan tujuan lalu lintas internet tanpa enkripsi oleh penyedia telekomunikasi Anda (9 huruf):

7 mendatar: Label numerik unik yang mengidentifikasi antarmuka perangkat di internet (8 huruf):

PETUNJUK MENURUN

1 menurun: Fitur browser untuk suara/video yang dapat melewati terowongan dan mengungkap alamat IP asli (6 huruf):

2 menurun: Merutekan data melalui tiga server sukarelawan dengan lapisan enkripsi di setiap langkah (3 huruf):

3 menurun: Perutean koneksi melalui server di negara lain untuk menembus blokir geografis (10 huruf):

4 menurun: Pengarahan seluruh lalu lintas perangkat yang terenkripsi melalui server VPN (8 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 I G N R P M P X Q O C U
S T S E L J B E A B W C P X L
N K K Y K X T R K D E Q M J D
A I O N N K Q U P G B M M Q R
R S R T T G C T S Q R O H P S
A B P W D S Z E V C T Z W E F
M K H Z D N D A A Q C X P L C
A U B A Z N D N L K A D O A D
Y F H I D R Q M A E I R Z C S
N F Q V F A T A M Q O N P A T
E K E B O C O R A N D N S K X
P Q K R U S R D T N Y B F A S
X W J A R Z Y Y I L G I M N R
J M L T O H Q Q P H Z A O V G
U B Y R Y B H L Z G J O P N W

DAFTAR KOSAKATA

ALAMATIP KEBOCORANDNS WEBRTC PROKSI TOR PERUTEAN PELACAKAN PENYAMARAN

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. ALAMATIP
B. KEBOCORANDNS
C. WEBRTC
D. PROKSI
E. TOR
F. PERUTEAN
G. PELACAKAN
H. PENYAMARAN

DEFINISI & KOLOM PENCOCOKAN

1. Pengalihan lalu lintas browser di lapisan aplikasi tanpa enkripsi tingkat sistem.
2. Pencatatan tujuan lalu lintas internet tanpa enkripsi oleh penyedia telekomunikasi Anda.
3. Pengarahan seluruh lalu lintas perangkat yang terenkripsi melalui server VPN.
4. Label numerik unik yang mengidentifikasi antarmuka perangkat di internet.
5. Fitur browser untuk suara/video yang dapat melewati terowongan dan mengungkap alamat IP asli.
6. Perutean koneksi melalui server di negara lain untuk menembus blokir geografis.
7. Merutekan data melalui tiga server sukarelawan dengan lapisan enkripsi di setiap langkah.
8. Kueri yang di-resolve di luar terowongan VPN sehingga domain yang dikunjungi terlihat oleh ISP.

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. IMAATLPA
2. CWBTRE
3. ROT
4. CNAAKAPEL
5. EDARSBCNOKNO
6. SKPOIR
7. PNTEAEUR
8. AYMNPAEARN

Aktivitas Bonus: Berpikir Cepat

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

1	Alasan memakai VPN saat bepergian			
2	Browser yang Anda ketahui			
3	Hal yang bisa disembunyikan VPN			
4	Kata yang berkaitan dengan privasi			
5	Kata dari lembar kerja ini yang ingin Anda ingat			
6	Hal yang bisa ditebak situs dari IP Anda			
7	Angka atau tanda di alamat IP			
8	Mitos tentang VPN			
9	Layanan VPN yang Anda ketahui			
10	Hal yang bisa dilihat penyedia internet Anda			
11	Janji penyedia VPN yang baik			
12	Hal yang bisa membocorkan IP asli Anda			
13	Alasan menyembunyikan lokasi Anda			
14	Cara menyembunyikan alamat IP			
15	Perangkat yang bisa memakai 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 penyamaran IP ini, pecahkan pesan rahasia tentang menyembunyikan jejak digital. 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

19 1 13 1 18 11 1 14 1 12 1 13 1 20 1 14 4 1

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

20 5 18 19 5 13 2 21 14 25 9

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 proksi web menyembunyikan alamat IP saya?

Ya, tetapi hanya untuk lalu lintas yang dikirim melaluinya, biasanya browser Anda. Sebagian besar proksi web tidak mengenkripsi data Anda, sehingga ISP atau operator jaringan tetap dapat melihat apa yang Anda kirim dan terima.

Q5: Apakah menyembunyikan IP saya legal?

Di banyak negara, ya, tetapi sebagian negara membatasi atau melarang VPN dan alat lain yang dipakai untuk menyembunyikan alamat IP. Menyembunyikan IP tidak pernah membuat tindakan ilegal menjadi legal, jadi periksa hukum setempat sebelum Anda memakainya.

Pos 10: FAQ Dasar VPN (Bagian B)

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

Q6: Apakah Tor menyembunyikan IP saya?

Ya. Tor mengirim lalu lintas Anda melalui tiga relai sukarela (guard, middle, dan exit), sehingga situs web melihat alamat relai exit, dan tidak ada satu relai pun yang mengetahui sekaligus siapa Anda dan ke mana Anda pergi. [1]

Q7: Apa yang diungkap oleh IP saya?

IP publik Anda biasanya mengungkap ISP dan perkiraan lokasi Anda, seperti negara atau kota. Situs juga dapat memakainya untuk menghubungkan kunjungan-kunjungan Anda dan menerapkan pemblokiran geografis.

Q8: Bagaimana cara memastikan IP saya tersembunyi?

Sambungkan VPN Anda, lalu kunjungi situs pemeriksa IP dan jalankan uji kebocoran DNS dan WebRTC. IP dan server DNS yang ditampilkan seharusnya milik VPN, bukan ISP Anda. Jika IP asli Anda muncul, aktifkan perlindungan kebocoran.

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: Mengapa situs web masih bisa melacak saya setelah saya menyembunyikan alamat IP?

Menyembunyikan IP tidak menghentikan fingerprinting browser. Pelacak dapat menggabungkan detail seperti resolusi layar, font yang terpasang, dan pengaturan browser menjadi sebuah pengenal, dan cookie atau akun yang sedang login juga dapat mengidentifikasi Anda, jadi gunakan juga browser yang berfokus pada privasi. [3]

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: Bisakah lalu lintas IPv6 membocorkan alamat IP asli saya?

Ya, jika VPN Anda hanya melewatkan IPv4 ke dalam terowongan. Perangkat Anda lalu bisa mengirim lalu lintas IPv6 di luar terowongan dan mengekspos alamat yang diberikan ISP Anda. Gunakan VPN yang menerowongkan atau memblokir IPv6, lalu pastikan dengan uji kebocoran IPv6.

Q5: Bagaimana Obfuscation menembus pemblokiran VPN?

Obfuskasi (atau "Stealth VPN") menyamarkan paket lalu lintas VPN agar tampak seperti lalu lintas web HTTPS biasa (port 443). Ini membantu melewati Deep Packet Inspection (DPI) yang dipakai 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: Apakah split tunneling mengekspos alamat IP asli saya?

Ya, untuk aplikasi yang Anda kecualikan. Lalu lintas yang dikirim di luar terowongan memakai IP asli Anda, dan RFC 8828 mencatat bahwa WebRTC dapat mengungkap alamat ISP di balik VPN split-tunnel kecuali browser membatasinya. [2]

Q7: Apa itu alamat IP bersama dan bagaimana alamat ini membantu privasi?

Dengan IP bersama, banyak pengguna VPN tampil online dengan alamat yang sama pada saat yang sama. Hal ini membuat situs web jauh lebih sulit mengaitkan satu kunjungan tertentu dengan Anda dibandingkan dengan IP khusus yang hanya Anda pakai.

Q8: Bisakah ISP saya melihat bahwa saya memakai VPN untuk menyembunyikan IP?

Biasanya, ya. ISP Anda dapat melihat bahwa Anda tersambung ke alamat IP server VPN, kapan Anda tersambung, dan berapa banyak data yang Anda kirim, tetapi tidak dapat melihat situs web yang Anda kunjungi atau isi di dalam terowongan terenkripsi.

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: Mana yang lebih baik untuk menyembunyikan IP saya, proksi atau VPN?

VPN biasanya lebih baik. VPN menyembunyikan IP Anda untuk setiap aplikasi di perangkat dan mengenkripsi lalu lintasnya, sedangkan proksi web biasanya hanya mencakup browser dan sering kali tidak menambahkan enkripsi.

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 memakai WireGuard atau OpenVPN.

2. FINGERPRINTING

Menyembunyikan IP tidak menghentikan fingerprinting browser, yang dapat mengidentifikasi Anda dari detail seperti resolusi layar dan font yang terpasang. [3]

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.

4. PAPARAN ALAMAT WEBRTC

RFC 8828 memperingatkan bahwa WebRTC dapat menemukan alamat publik VPN sekaligus alamat ISP yang menjadi jalur VPN tersebut, kecuali browser membatasinya. [2]

5. ASAL-USUL ALIANSI 5-EYES

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

6. DEEP PACKET INSPECTION

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

7. PEMAKAIAN ULANG SIRKUIT TOR

Tor memakai ulang sirkuit yang sama selama sekitar sepuluh menit lalu membangun sirkuit baru, sehingga aktivitas penjelajahan Anda lebih sulit dikaitkan satu sama lain. [1]

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 menerowongkan lalu lintas melalui satu penyedia, sedangkan Tor (The Onion Router) mengirim lalu lintas melalui tiga relai sukarela (guard, middle, exit) untuk memaksimalkan privasi. [1]

10. PROKSI VS. TEROWONGAN VPN

Proksi web mengubah alamat IP yang dilihat situs untuk lalu lintas browser Anda, tetapi tidak seperti VPN, proksi biasanya tidak mengenkripsi lalu lintas itu atau mencakup aplikasi lain di perangkat Anda. [5]

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

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

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

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

[5] 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

Kunci Jawaban: Menyembunyikan alamat IP, penyamaran lokasi, proksi, Tor, dan mencegah kebocoran DNS/WebRTC

1 Soal 1

Jawaban Benar: B

CATATAN PENGAJAR

Apa yang diungkap alamat IP publik sebuah perangkat kepada situs web yang Anda kunjungi? → Perkiraan lokasi Anda dan nama ISP Anda

2 Enkripsi Sistem VPN LATENSI

Jawaban Benar: C

CATATAN PENGAJAR

Berbeda dari proksi yang hanya mengalihkan lalu lintas browser, VPN membuat terowongan terenkripsi untuk seluruh sistem yang mengamankan aplikasi latar belakang, game, dan kueri sistem operasi.

3 Proksi Tanpa Enkripsi KEAMANAN WI-FI

Jawaban Benar: A

CATATAN PENGAJAR

Proksi web hanya meneruskan lalu lintas browser tanpa mengenkripsi muatan paket, sehingga operator jaringan atau ISP masih bisa melacak isi lalu lintas Anda.

4 Soal 4

Jawaban Benar: B

CATATAN PENGAJAR

Bagaimana jaringan Tor memberikan anonimitas tinggi kepada penggunanya? → Dengan merutekan lalu lintas melalui tiga relai yang dijalankan sukarelawan

5 Kebocoran DNS dari Terowongan PRIVASI

Jawaban Benar: B

CATATAN PENGAJAR

Kebocoran DNS terjadi saat permintaan resolusi nama domain melewati terowongan VPN dan langsung menuju resolver ISP, sehingga domain yang dikunjungi terungkap.

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Rincian Batasan Proksi** PENYAMARAN IP — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Proksi bekerja di lapisan aplikasi dan tidak terintegrasi dengan driver jaringan sistem seperti terowongan VPN.

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

CATATAN PENGAJAR

Meneruskan lalu lintas melalui tiga relai sukarela dengan enkripsi berlapis menambah latensi, sehingga Tor biasanya lebih lambat daripada koneksi langsung.

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

CATATAN PENGAJAR

WebRTC dapat mengungkap alamat lokal dan, pada sebagian konfigurasi VPN, IP publik dari ISP di balik terowongan (RFC 8828).

9 **Soal 9** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Tanpa kebocoran DNS atau WebRTC, ISP hanya melihat lalu lintas terenkripsi menuju server VPN, bukan situs yang Anda kunjungi.

10 **Batasan terhadap Sidik Jari** TANPA LOG — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Sidik jari browser menyasar ciri konfigurasi perangkat (resolusi layar, font, plugin) yang tetap terlihat meski IP disembunyikan.

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

D 1. Alamat IP	A 2. Terowongan VPN	B 3. Jaringan Tor	E 4. Proksi Web
G 5. Kebocoran DNS	H 6. API WebRTC	C 7. Penyamaran Lokasi	F 8. Pelacakan ISP

POS 3: KUNCI ISTILAH KUNCI

1 KEBOCORAN DNS	2 WEBRTC	3 PROKSI	4 TOR
5 ALAMAT IP	6 LOKASI		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 D – PROKSI	2 G – PELACAKAN	3 F – PERUTEAN	4 A – ALAMATIP
5 C – WEBRTC	6 H – PENYAMARAN	7 E – TOR	8 B – KEBOCORANDNS

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan Alamat IP, Terowongan VPN, dan Jaringan Tor dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

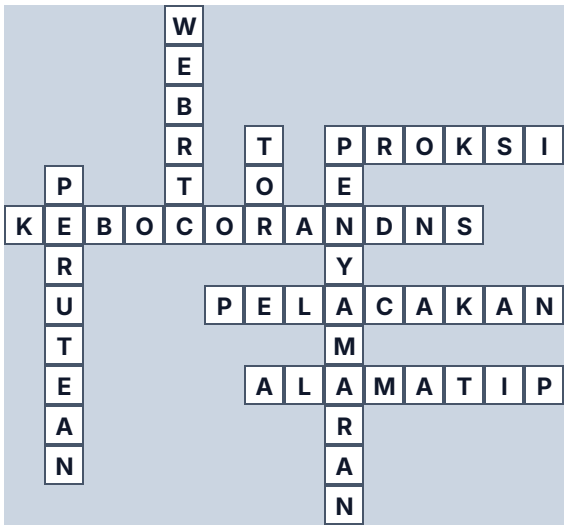
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

3 mendatar: PROKSI Pengalihan lalu lintas browser di lapisan aplikasi tanpa enkripsi tingkat sistem (6 huruf)

5 mendatar: KEBOCORANDNS Kueri yang di-resolve di luar terowongan VPN sehingga domain yang dikunjungi terlihat oleh ISP (12 huruf)

6 mendatar: PELACAKAN Pencatatan tujuan lalu lintas internet tanpa enkripsi oleh penyedia telekomunikasi Anda (9 huruf)

7 mendatar: ALAMATIP Label numerik unik yang mengidentifikasi antarmuka perangkat di internet (8 huruf)

PETUNJUK MENURUN

1 menurun: WEBRTC Fitur browser untuk suara/video yang dapat melewati terowongan dan mengungkap alamat IP asli (6 huruf)

2 menurun: TOR Merutekan data melalui tiga server sukarelawan dengan lapisan enkripsi di setiap langkah (3 huruf)

3 menurun: PENYAMARAN Perutean koneksi melalui server di negara lain untuk menembus blokir geografis (10 huruf)

4 menurun: PERUTEAN Pengarahan seluruh lalu lintas perangkat yang terenkripsi melalui server VPN (8 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1.	IMAATLPA	ALAMATIP	5.	EDARSBCNOKNO	KEBOCORANDNS
2.	CWBTRE	WEBRTC	6.	SKPOIR	PROKSI
3.	ROT	TOR	7.	PNTEAEUR	PERUTEAN
4.	CNAAKAPEL	PELACAKAN	8.	AYMNPAEARN	PENYAMARAN

KUNCI TANTANGAN SANDI RAHASIA

"SAMARKAN ALAMAT ANDA DENGAN SISTEM TERSEMBUNYI"

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.