Nama: _____ Tanggal: _____ Nilai: _____

Panduan VPN dari VPN.com Lembar Kerja

Latihan praktis tentang protokol jaringan, tunneling, dan kontrol keamanan.

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 konsep tunneling dan enkapsulasi data.
- Kenali konfigurasi protokol standar dan kebutuhan bandwidth.
- Analisis peran firewall dan pemblokiran geografis dalam routing internet.
- Pahami bagaimana ISP melacak penjelajahan yang tidak terenkripsi dan bagaimana VPN mencegahnya.
- Bedakan batas operasional antara lokasi server dan yurisdiksi.

PETUNJUK PANDUAN VPN

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 pada skenario nyata di bagian studi kasus. Akhiri dengan aktivitas bonus Berpikir Cepat.

APA ITU VPN? (PENGANTAR)

Virtual Private Network lebih dari sekadar tombol privasi. VPN adalah terowongan terenkripsi yang meneruskan lalu lintas internet Anda melalui server jarak jauh. Ini menyembunyikan alamat IP Anda, mencegah ISP mencatat aktivitas online Anda, dan mengamankan data di jaringan publik. Memahami istilah-istilahnya penting untuk menjaga keamanan digital.

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

Pos 1: Tantangan Pilihan Ganda

1. **1. Apa itu protokol VPN?**
   - A. Perangkat keras untuk menyambungkan kabel.
   - B. Seperangkat aturan yang menentukan cara data dienkripsi dan dikirim.
   - C. Plugin browser yang memblokir iklan.
   - D. Perusahaan penyedia layanan internet.

2. **2. Jika koneksi VPN Anda terasa lambat, apa penyebab yang paling mungkin?**
   - A. Server VPN terlalu jauh atau kelebihan beban.
   - B. Resolusi monitor Anda terlalu tinggi.
   - C. Anda menonaktifkan cookie browser.
   - D. Tata letak keyboard Anda salah diatur.

3. **3. Mengapa VPN sangat disarankan saat memakai Wi-Fi publik?**
   - A. VPN membuat koneksi Wi-Fi menjadi gratis.
   - B. VPN memperluas jangkauan router.
   - C. VPN mengenkripsi lalu lintas agar peretas di jaringan yang sama tidak dapat membacanya.
   - D. VPN menghapus email sampah secara otomatis.

4. **4. Manakah yang menggambarkan pemblokiran geografis?**
   - A. Alat untuk mengukur jarak fisik ke server.
   - B. Pembatasan yang memblokir akses situs berdasarkan lokasi.
   - C. Protokol untuk mengompresi file lokal.
   - D. Mekanisme penyimpanan cadangan.

5. **5. Apa yang dapat dilihat penyedia layanan internet (ISP) Anda saat Anda memakai VPN?**
   - A. Kata kunci pencarian dan isi halaman web yang Anda lihat.
   - B. Bahwa Anda terhubung ke VPN, tetapi bukan rincian lalu lintasnya.
   - C. Tidak ada informasi apa pun, bahkan tidak tahu bahwa Anda sedang online.
   - D. File dan foto di hard drive lokal Anda.

Pos 2: Tantangan Benar atau Salah

6 Penyamaran Lokasi

6. VPN menyamarkan alamat IP publik perangkat Anda sehingga situs pihak ketiga tidak mudah mengetahui lokasi fisik Anda.

○ Benar ○ Salah

7 Pengaruh VPN terhadap Kecepatan

7. Mengaktifkan VPN membuat kecepatan dasar internet Anda dua kali lebih cepat daripada tanpa VPN.

○ Benar ○ Salah

8 Penyadapan Wi-Fi Publik

8. Jika Anda memakai Wi-Fi publik yang tidak aman tanpa VPN, pengguna lain di jaringan yang sama berpotensi menangkap lalu lintas Anda yang tidak terenkripsi.

○ Benar ○ Salah

9 Firewall & Koneksi yang Diblokir

9. Administrator jaringan dapat mengatur firewall untuk mendeteksi dan memblokir terowongan VPN keluar.

○ Benar ○ Salah

10 Kebijakan Tanpa Log yang Ketat

10. Kebijakan "tanpa log" yang ketat berarti penyedia VPN diwajibkan hukum menyimpan kueri pencarian dan tautan yang Anda kunjungi setidaknya selama 30 hari.

○ 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. Untuk mengamankan lalu lintas, VPN membungkus paket data Anda di dalam protokol lain, sebuah proses yang disebut _____ .

2. Jika unduhan terasa lambat saat streaming, penyebabnya mungkin keterbatasan _____ .

3. Layanan streaming yang hanya tersedia di negara tertentu memakai _____ untuk membatasi pengguna dari negara lain.

4. Aturan koneksi yang menentukan parameter enkripsi dan koneksi disebut _____ .

5. Komputer Anda memakai _____ lokal untuk memantau lalu lintas jaringan dan memblokir koneksi yang tidak aman.

6. Saat Anda terhubung ke VPN, data Anda dirutekan melalui _____ jarak jauh untuk menyembunyikan IP publik Anda.

BANK KATA KOSAKATA

BANDWIDTH FIREWALL GEO-BLOCKING ISP PRIVASI PROTOKOL SERVER TUNNELING

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Jaringan

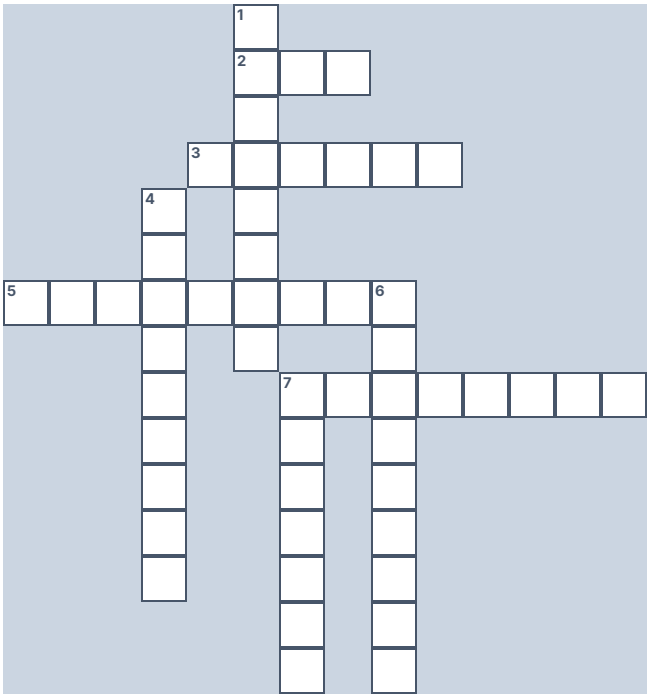
MENCOCOKKAN DEFINISI

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

☐	1. Tunneling	A	Seperangkat aturan yang menentukan cara data dikirim melalui jaringan.
☐	2. Protokol	B	Laju maksimum transfer data pada sebuah koneksi.
☐	3. Bandwidth	C	Pembatasan yang mencegah akses web berdasarkan lokasi fisik.
☐	4. Server	D	Sistem keamanan yang memantau dan memblokir lalu lintas tanpa izin.
☐	5. GEO-BLOCKING	E	Komputer jarak jauh yang merutekan lalu lintas Anda dan menyamarkan IP Anda.
☐	6. Firewall	F	Keadaan bebas dari pelacakan atau pengawasan publik.
☐	7. Privasi	G	Penyedia Layanan Internet yang membawa lalu lintas Anda dan dapat melihat aktivitas yang tidak terenkripsi.
☐	8. ISP	H	Membungkus paket data di dalam paket lain agar aman selama transit.

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. Penyedia layanan internet yang membawa lalu lintas Anda dan dapat melihat aktivitas tanpa enkripsi (3)

3. Komputer jarak jauh yang merutekan lalu lintas Anda dan menyamarkan IP Anda (6)

5. Membungkus paket data di dalam paket lain agar aman saat dikirim (9)

7. Seperangkat aturan yang menentukan cara data dikirim melalui jaringan (8)

PETUNJUK MENURUN

1. Sistem keamanan yang memantau dan memblokir lalu lintas tanpa izin (8)

4. Laju transfer data maksimum pada sebuah koneksi (9)

6. Pembatasan akses web berdasarkan lokasi fisik (9)

7. Keadaan bebas dari pelacakan atau pengawasan publik (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: Penyedia layanan internet yang membawa lalu lintas Anda dan dapat melihat aktivitas tanpa enkripsi (3 huruf):

3 mendatar: Komputer jarak jauh yang merutekan lalu lintas Anda dan menyamarkan IP Anda (6 huruf):

5 mendatar: Membungkus paket data di dalam paket lain agar aman saat dikirim (9 huruf):

7 mendatar: Seperangkat aturan yang menentukan cara data dikirim melalui jaringan (8 huruf):

PETUNJUK MENURUN

1 menurun: Sistem keamanan yang memantau dan memblokir lalu lintas tanpa izin (8 huruf):

4 menurun: Laju transfer data maksimum pada sebuah koneksi (9 huruf):

6 menurun: Pembatasan akses web berdasarkan lokasi fisik (9 huruf):

7 menurun: Keadaan bebas dari pelacakan atau pengawasan publik (7 huruf):

Pos 6: Mencari Kata Tersembunyi

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

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

DAFTAR KOSAKATA

TUNNELING BANDWIDTH GEOBLOKIR PROTOKOL FIREWALL SERVER ISP PRIVASI

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. TUNNELING**
- **B. BANDWIDTH**
- **C. GEOBLOKIR**
- **D. PROTOKOL**
- **E. FIREWALL**
- **F. SERVER**
- **G. ISP**
- **H. PRIVASI**

DEFINISI & KOLOM PENCOCOKAN

_____ 1. Penyedia layanan internet yang membawa lalu lintas Anda dan dapat melihat aktivitas tanpa enkripsi.

_____ 2. Sistem keamanan yang memantau dan memblokir lalu lintas tanpa izin.

_____ 3. Laju transfer data maksimum pada sebuah koneksi.

_____ 4. Komputer jarak jauh yang merutekan lalu lintas Anda dan menyamarkan IP Anda.

_____ 5. Pembatasan akses web berdasarkan lokasi fisik.

_____ 6. Seperangkat aturan yang menentukan cara data dikirim melalui jaringan.

_____ 7. Keadaan bebas dari pelacakan atau pengawasan publik.

_____ 8. Membungkus paket data di dalam paket lain agar aman saat dikirim.

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. **LENUTINGN** _____
2. **RGIBEOKLO** _____
3. **EIFWALLR** _____
4. **SPI** _____
5. **DWAHIDBTN** _____
6. **OLTKPORO** _____
7. **ESVRRE** _____
8. **RVIPSAI** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Hal yang Anda kaitkan dengan kata 'terowongan'			
2	Hal tentang VPN yang ingin Anda ajarkan ke keluarga			
3	Hal di situs web yang bisa melacak Anda			
4	Mitos tentang VPN			
5	Kata dari lembar kerja ini yang ingin Anda ingat			
6	Perangkat yang bisa memakai VPN			
7	Hal yang tidak bisa dicegah VPN			
8	Negara yang ingin Anda 'kunjungi' secara online			
9	Janji penyedia VPN yang baik			
10	Cara mengenali Wi-Fi palsu			
11	Pertanyaan Anda tentang VPN			
12	Layanan VPN yang Anda ketahui			
13	Kata yang berkaitan dengan privasi			
14	Hal yang bisa disembunyikan VPN			
15	Alasan memakai VPN di kafe			

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

VPN mengenkripsi lalu lintas Anda untuk mengamankannya. Gunakan kunci Huruf-ke-Angka di bawah untuk memecahkan pesan rahasia 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	16	14		13	5	14	7	5	14	11	18	9	16	19	9		12	1	12	21
				12	9	14	20	1	19		1	14	4	1						

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: Apakah menggunakan VPN legal?

Penggunaan VPN legal di banyak negara, tetapi beberapa yurisdiksi membatasi, mengatur, atau memblokir layanan VPN. Pengguna sebaiknya memeriksa hukum setempat yang berlaku sebelum menggunakannya. Untuk detail lebih lanjut, lihat panduan legalitas di VPN.com.

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. [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: 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?

Obfuskasi (atau "Stealth VPN") menyamarkan lalu lintas VPN agar tampak seperti lalu lintas HTTPS biasa (port 443). Ini dapat 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: Apa itu Split Tunneling dan kapan sebaiknya digunakan?

Split Tunneling memungkinkan Anda memilih aplikasi mana yang dirutekan melalui terowongan VPN terenkripsi dan mana yang tersambung langsung ke internet. Gunakan fitur ini untuk merutekan aplikasi perbankan yang sensitif melalui VPN, sementara game lokal tersambung langsung tanpa tambahan latensi dari 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: Bisakah VPN menghindari pelambatan internet oleh ISP?

Terkadang. VPN dapat membantu saat ISP secara selektif memperlambat aktivitas yang dapat dikenali, tetapi VPN tidak dapat mengatasi kemacetan jaringan, batas data, batas kecepatan akun, atau kualitas jaringan yang buruk.

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) dikembangkan oleh sekelompok vendor termasuk Microsoft dan diterbitkan sebagai RFC 2637 pada Juli 1999 untuk mendukung VPN akses jarak jauh. [6]

2. NILAI PASAR

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

3. REVOLUSI WIREGUARD

WireGuard memiliki basis kode yang sangat ringkas dan efisien, sehingga lebih mudah diaudit untuk mencari celah keamanan daripada protokol tradisional. [3]

4. STANDAR AUDIT YANG KETAT

Penyedia VPN papan atas menyewa auditor eksternal (seperti Cure53 atau PwC) untuk meninjau kode secara independen dan memverifikasi bahwa mereka tidak mencatat aktivitas pengguna.

5. ASAL-USUL ALIANSI 5-EYES

Aliansi Five Eyes berawal dari perjanjian intelijen sinyal UKUSA tahun 1946 antara AS dan Inggris, yang kemudian diikuti Kanada, Australia, dan Selandia Baru.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) memeriksa isi paket dan pola lalu lintas, bukan hanya header, dan sebagian firewall menggunakannya untuk mendeteksi dan memblokir protokol VPN yang umum.

7. PENGGUNAAN DI PERUSAHAAN

Sebagian besar karyawan perusahaan di seluruh dunia menggunakan VPN yang aman untuk masuk ke basis data internal, sehingga VPN menjadi standar keamanan utama.

8. VPN TERDESENTRALISASI

VPN terdesentralisasi (dVPN) menyebarkan lalu lintas ke jaringan node yang dijalankan para pengguna, sehingga tidak bergantung 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, dan exit) sehingga tidak ada satu relai pun yang mengetahui kedua ujungnya.

10. BIAYA PELANGGARAN DATA

Menerapkan model akses aman zero trust bersama VPN membantu organisasi melindungi kekayaan intelektual dan mengurangi dampak finansial kebocoran data.

Referensi & Sumber Teknis

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

LITERATUR AKADEMIK & STANDAR KEAMANAN

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

[2] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

RINGKASAN STANDAR TEKNIS

- Standar enkapsulasi: RFC 4301 menetapkan arsitektur keamanan IPsec untuk paket internet.
- Pelacakan oleh ISP: Merutekan kueri DNS melalui terowongan VPN terenkripsi dapat mengurangi visibilitas DNS bagi ISP setempat.
- Protokol kontrol firewall: Paket yang disamarkan dapat menembus filter inspeksi paket mendalam.

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1

Jawaban Benar: B

CATATAN PENGAJAR

Protokol VPN menetapkan aturan untuk membangun terowongan dan mengenkripsi data; pilihan lainnya menggambarkan kabel, pemblokir iklan, dan ISP.

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

Jarak menambah latensi dan server yang kelebihan beban memiliki kapasitas lebih sedikit untuk dibagi; resolusi layar, cookie, dan tata letak keyboard tidak memengaruhi kecepatan koneksi.

3 Soal 3

Jawaban Benar: C

CATATAN PENGAJAR

Di jaringan terbuka, orang lain dapat mencegat paket yang tidak terenkripsi; VPN mengenkripsi lalu lintas sehingga data yang dicegat tidak dapat dibaca.

4 Soal 4

Jawaban Benar: B

CATATAN PENGAJAR

Pemblokiran geografis mencocokkan alamat IP publik pengunjung dengan basis data lokasi dan menolak akses dari luar wilayah yang diizinkan.

5 Soal 5

Jawaban Benar: B

CATATAN PENGAJAR

ISP dapat melihat bahwa Anda mengirim data terenkripsi ke server VPN, tetapi tidak dapat melihat situs yang Anda kunjungi atau apa yang Anda cari.

Kunci Jawaban: Pos 2 - Benar atau Salah

6 Soal 6

Jawaban Benar: Benar

CATATAN PENGAJAR

Situs web melihat alamat IP server VPN, bukan IP Anda, sehingga perkiraan lokasi Anda tersembunyi dari mereka.

7 Soal 7

Jawaban Benar: Salah

CATATAN PENGAJAR

Enkripsi dan hop tambahan ke server VPN biasanya sedikit menurunkan kecepatan; VPN tidak dapat menggandakan kecepatan dasar koneksi Anda.

8 Soal 8

Jawaban Benar: Benar

CATATAN PENGAJAR

Di Wi-Fi yang tidak aman, alat packet sniffing dapat menangkap lalu lintas yang tidak terenkripsi, seperti login yang dikirim tanpa HTTPS.

9 Soal 9

Jawaban Benar: Benar

CATATAN PENGAJAR

Administrator dapat memblokir port VPN yang dikenal, seperti port 1194 milik OpenVPN, atau memakai Deep Packet Inspection untuk mendeteksi lalu lintas VPN.

10 Soal 10

Jawaban Benar: Salah

CATATAN PENGAJAR

Kebijakan tanpa log adalah janji penyedia untuk tidak menyimpan catatan aktivitas Anda; tidak ada hukum yang mewajibkan VPN menyimpan pencarian selama 30 hari.

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. Tunneling	A 2. Protokol	B 3. Bandwidth	E 4. Server
C 5. GEO-BLOCKING	D 6. Firewall	F 7. Privasi	G 8. ISP

POS 3: KUNCI ISTILAH KUNCI

1 TUNNELING	2 BANDWIDTH	3 GEO-BLOCKING	4 PROTOKOL
5 FIREWALL	6 SERVER		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 G – ISP	2 E – FIREWALL	3 B – BANDWIDTH	4 F – SERVER
5 C – GEOBLOKIR	6 D – PROTOKOL	7 H – PRIVASI	8 A – TUNNELING

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan Tunneling, Protokol, dan Bandwidth dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

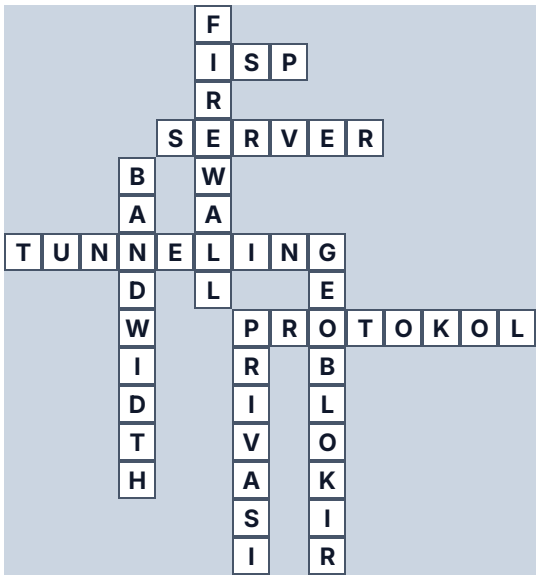
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PETUNJUK MENDATAR

2 mendatar: ISP Penyedia layanan internet yang membawa lalu lintas Anda dan dapat melihat aktivitas tanpa enkripsi (3 huruf)

3 mendatar: SERVER Komputer jarak jauh yang merutekan lalu lintas Anda dan menyamarkan IP Anda (6 huruf)

5 mendatar: TUNNELING Membungkus paket data di dalam paket lain agar aman saat dikirim (9 huruf)

7 mendatar: PROTOKOL Seperangkat aturan yang menentukan cara data dikirim melalui jaringan (8 huruf)

PETUNJUK MENURUN

1 menurun: FIREWALL Sistem keamanan yang memantau dan memblokir lalu lintas tanpa izin (8 huruf)

4 menurun: BANDWIDTH Laju transfer data maksimum pada sebuah koneksi (9 huruf)

6 menurun: GEOBLOKIR Pembatasan akses web berdasarkan lokasi fisik (9 huruf)

7 menurun: PRIVASI Keadaan bebas dari pelacakan atau pengawasan publik (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1.	L E N U T I N G N	TUNNELING	5.	D W A H I D B T N	BANDWIDTH
2.	R G I B E O K L O	GEOBLOKIR	6.	O L T K P O R O	PROTOKOL
3.	E I F W A L L R	FIREWALL	7.	E S V R R E	SERVER
4.	S P I	ISP	8.	R V I P S A I	PRIVASI

KUNCI TANTANGAN SANDI RAHASIA

"VPN MENGENKRIPSI LALU LINTAS ANDA"

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.