Nama: _____ Tanggal: _____ Nilai: _____

Proksi vs VPN Lembar Kerja

Membandingkan server proksi dan jaringan pribadi virtual, perbedaan enkripsi, serta routing per aplikasi vs seluruh sistem

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

- Bandingkan proksi aplikasi dengan enkripsi VPN untuk seluruh sistem.
- Kenali kemampuan SOCKS5 dibanding proksi HTTP dasar.
- Analisis bagaimana proksi berbasis browser membiarkan aplikasi latar belakang terbuka.
- Pahami cara ISP mencatat lalu lintas tanpa enkripsi di proksi.
- Pilih alat perutean yang tepat sesuai kebutuhan kecepatan dan keamanan.

PETUNJUK LEMBAR KERJA PERBANDINGAN PROKSI

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 membandingkan proksi dan VPN. Akhiri dengan aktivitas bonus Berpikir Cepat.

PROKSI VS VPN (PENGANTAR)

Proksi dan VPN punya fungsi privasi digital yang berbeda. Server proksi mengalihkan lalu lintas di lapisan aplikasi dan menyamarkan alamat IP untuk program tertentu tanpa mengenkripsi data. VPN bekerja di tingkat jaringan dan mengamankan seluruh lalu lintas sistem dengan enkripsi. Alat yang tepat bergantung pada kebutuhan keamanan Anda.

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

Pos 1: Tantangan Pilihan Ganda

1. Di lapisan OSI mana proksi HTTP standar bekerja?
   - A. Lapisan fisik
   - B. Lapisan jaringan
   - C. Lapisan aplikasi
   - D. Lapisan data link

2. Apa keunggulan utama SOCKS5 dibanding proksi HTTP standar?
   - A. Memaksa enkripsi muatan penuh
   - B. Mendukung perutean lalu lintas TCP/UDP apa pun
   - C. Kebal terhadap kebocoran DNS
   - D. Berjalan langsung di ruang kernel

3. Mengapa VPN umumnya lebih aman daripada server proksi?
   - A. Berjalan di perangkat keras jarak jauh yang lebih cepat
   - B. Mengenkripsi semua lalu lintas di seluruh sistem
   - C. Tidak memerlukan tabel rute lokal
   - D. Menghilangkan latensi jaringan sepenuhnya

4. Jenis proksi mana yang secara bawaan mengalihkan lalu lintas tanpa enkripsi?
   - A. Proksi HTTP dasar
   - B. Proksi HTTPS terenkripsi
   - C. Klien WireGuard yang aman
   - D. Server VPN tersamar

5. Apa yang terjadi pada lalu lintas aplikasi latar belakang saat memakai proksi browser?
   - A. Otomatis dienkripsi
   - B. Diblokir server proksi
   - C. Dirutekan lewat proksi
   - D. Melewati proksi dan membuka IP Anda

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Proksi SOCKS5 mengenkripsi semua muatan paket yang melewati server.

Benar Salah

7 Pertanyaan 7

7. VPN bekerja di lapisan jaringan untuk mengamankan semua lalu lintas sistem.

Benar Salah

8 Pertanyaan 8

8. Proksi umumnya lebih cepat daripada VPN karena melakukan enkripsi paket mendalam.

Benar Salah

9 Pertanyaan 9

9. Mengatur proksi memerlukan pengalihan lalu lintas di dalam aplikasi tertentu.

Benar Salah

10 Pertanyaan 10

10. Memakai proksi tidak melindungi lalu lintas data dari pelacakan ISP lokal.

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. _____ lapisan aplikasi mengalihkan lalu lintas browser tertentu tanpa mengamankan aplikasi lain.

2. _____ VPN yang andal mengenkapsulasi dan mengenkripsi semua paket data perangkat.

3. Protokol _____ berada di antara lapisan aplikasi dan transport.

4. Proksi HTTP bekerja di lapisan _____ model OSI.

5. Server proksi standar tidak memiliki _____ muatan, sehingga data rentan.

6. VPN memberikan perlindungan tingkat _____ untuk semua adaptor jaringan.

BANK KATA KOSAKATA

APLIKASI DUKUNGAN UDP ENKRIPSI PROKSI SISTEM SOCKS5 TEROWONGAN VISIBILITAS ISP

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Jaringan

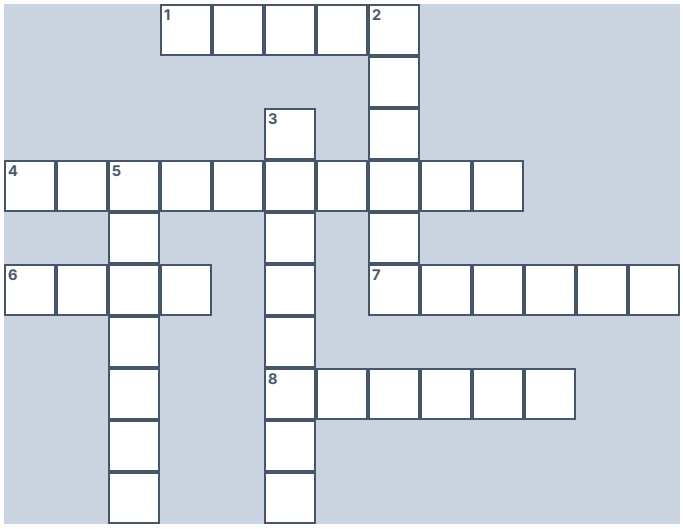
MENCOCOKKAN DEFINISI

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

☐	1. Proksi HTTP	A	Perutean tingkat sistem operasi yang mengenkripsi semua lalu lintas aplikasi.
☐	2. Proksi SOCKS5	B	Lapisan aplikasi tempat protokol proksi web standar bekerja.
☐	3. Terowongan VPN	C	Kemampuan SOCKS5 meneruskan UDP selain TCP, berbeda dengan proksi HTTP biasa.
☐	4. Seluruh Sistem	D	Ekstensi klien yang hanya menyembunyikan lalu lintas di dalam browser.
☐	5. Lapisan OSI 7	E	Enkripsi dan enkapsulasi yang membungkus semua lalu lintas latar belakang perangkat.
☐	6. Dukungan UDP	F	Keadaan saat data proksi tanpa enkripsi tetap terlihat oleh ISP.
☐	7. Proksi Browser	G	Proksi lapisan aplikasi yang mengalihkan lalu lintas browser tertentu.
☐	8. Visibilitas ISP	H	Protokol proksi di antara lapisan aplikasi dan lapisan transport, tanpa enkripsi.

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

1. Versi HTTP terenkripsi yang melindungi lalu lintas antara browser dan situs web (5)

4. Data jaringan yang tetap terlihat oleh ISP jika dikirim lewat proksi tanpa enkripsi (10)

6. Proksi lapisan aplikasi yang mengalihkan lalu lintas browser tertentu (4)

7. Isi paket data yang tidak dienkripsi oleh server proksi standar (6)

8. Protokol proksi di antara lapisan aplikasi dan transport, tanpa enkripsi, yang dapat meneruskan UDP maupun TCP (6)

PETUNJUK MENURUN

2. Tingkat sistem operasi tempat VPN mengenkripsi lalu lintas semua aplikasi (6)

3. Cara menembus blokir dengan mengalihkan lalu lintas lewat server perantara (8)

5. Jeda tambahan saat lalu lintas melewati server perantara (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

1 mendatar: Versi HTTP terenkripsi yang melindungi lalu lintas antara browser dan situs web (5 huruf):

4 mendatar: Data jaringan yang tetap terlihat oleh ISP jika dikirim lewat proksi tanpa enkripsi (10 huruf):

6 mendatar: Proksi lapisan aplikasi yang mengalihkan lalu lintas browser tertentu (4 huruf):

7 mendatar: Isi paket data yang tidak dienkripsi oleh server proksi standar (6 huruf):

8 mendatar: Protokol proksi di antara lapisan aplikasi dan transport, tanpa enkripsi, yang dapat meneruskan UDP maupun TCP (6 huruf):

PETUNJUK MENURUN

2 menurun: Tingkat sistem operasi tempat VPN mengenkripsi lalu lintas semua aplikasi (6 huruf):

3 menurun: Cara menembus blokir dengan mengalihkan lalu lintas lewat server perantara (8 huruf):

5 menurun: Jeda tambahan saat lalu lintas melewati server perantara (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 N I G N R M P X Q O C U S
T E A L J B A B S C P X L K Y
K X T T K D Q M J O D I N N K
Q P A M E T S I S G C M M Q R
S T U T G L C S Q O H K S B W
I D M S Z A V P C S Z W S F K
S H Z D N L D Q I X P P C 5 U
N B A Z N U D K A N D T O D F
E H I D R L Q M E I T R T Z S
T F Q V F I H A A Q O A N H P
A T X Q K N T R U S D N S Y B
L F S X W T T J A R Z Y Y A L
G I M R J A P M L T O H Q Q N
H Z A O V S G U B Y R Y B H L
Z G J O P N W C M Z Y G Y O W

DAFTAR KOSAKATA

SOCKS5 HTTP HTTPS LATENSI PINTASAN SISTEM LALULINTAS MUATAN

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. SOCKS5
B. HTTP
C. HTTPS
D. LATENSI
E. PINTASAN
F. SISTEM
G. LALULINTAS
H. MUATAN

DEFINISI & KOLOM PENCOCOKAN

_____ 1. Cara menembus blokir dengan mengalihkan lalu lintas lewat server perantara.

_____ 2. Tingkat sistem operasi tempat VPN mengenkripsi lalu lintas semua aplikasi.

_____ 3. Protokol proksi di antara lapisan aplikasi dan transport, tanpa enkripsi, yang dapat meneruskan UDP maupun TCP.

_____ 4. Data jaringan yang tetap terlihat oleh ISP jika dikirim lewat proksi tanpa enkripsi.

_____ 5. Versi HTTP terenkripsi yang melindungi lalu lintas antara browser dan situs web.

_____ 6. Jeda tambahan saat lalu lintas melewati server perantara.

_____ 7. Isi paket data yang tidak dienkripsi oleh server proksi standar.

_____ 8. Proksi lapisan aplikasi yang mengalihkan lalu lintas browser tertentu.

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. **CSKS5O** _____
2. **HSPTT** _____
3. **TIPASNAN** _____
4. **IALSUTNLAL** _____
5. **PHTT** _____
6. **STNLEIA** _____
7. **ESTMSI** _____
8. **ANMATU** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Perbedaan proxy dan VPN			
2	Hal yang tidak terenkripsi tanpa VPN			
3	Cara mengenali Wi-Fi palsu			
4	Hal yang dilakukan perantara sehari-hari			
5	Situasi saat proxy sudah cukup			
6	Perangkat yang bisa memakai VPN			
7	Jenis proxy yang Anda ketahui			
8	Hal yang bisa disembunyikan VPN			
9	Mitos tentang VPN			
10	Janji penyedia VPN yang baik			
11	Hal yang tidak bisa dicegah VPN			
12	Kata dari lembar kerja ini yang ingin Anda ingat			
13	Alasan memakai VPN saat bepergian			
14	Situasi saat Anda ingin VPN			
15	Tempat Anda akan 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 lagi di Coffee & Bytes, pakai jaringan terbuka bernama 'Free_Wi-Fi_No_Password'. Aku perlu login ke email sekolah, dan kata temanku proksi browser gratis sudah cukup aman. Apakah proksi bisa melindungi login dan berkasku, atau aku perlu VPN?"

ALEX (MAHASISWA YANG SEDANG BEPERGIAN)

👩‍💻 "Aku sedang di luar negeri, dan film dokumenter biologi yang di-host di negaraku menampilkan 'This video is not available in your current location.' Teman sekelasku memakai proksi, sedangkan aku punya VPN. Kenapa aku diblokir, dan alat mana yang lebih ampuh?"

Pos 9: Memecahkan Sandi

Untuk menuntaskan latihan perbandingan proksi ini, pecahkan pesan rahasia tentang tunneling 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

16 18 15 11 19 9

13 5 14 25 5 13 2 21 14 25 9 11 1 14

20 5 20 1 16 9 20 9 4 1 11

13 5 14 7 5 14 11 18 9 16 19 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: Apa itu server proksi?

Server proksi adalah perantara yang meneruskan permintaan antara aplikasi Anda dan server tujuan. Situs web melihat alamat IP proksi, bukan IP Anda, tetapi hanya lalu lintas dari aplikasi yang dikonfigurasi untuk memakai proksi yang dialihkan, dan proksi dasar tidak mengenkripsi lalu lintas tersebut.

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 proksi sama dengan VPN?

Tidak. Proksi meneruskan lalu lintas untuk aplikasi tertentu, biasanya tanpa enkripsi. VPN membangun terowongan terenkripsi di lapisan jaringan yang membawa semua lalu lintas perangkat, termasuk aplikasi latar belakang.

Pos 10: FAQ Dasar VPN (Bagian B)

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

Q6: Bolehkah saya memakai proksi gratis?

Boleh, tetapi proksi gratis sering dijalankan oleh operator yang tidak dikenal. Karena proksi dasar tidak mengenkripsi lalu lintas, operatornya dapat melihat bahkan mengubah halaman yang tidak terenkripsi. Periksa siapa yang menjalankan layanan itu sebelum memakainya.

Q7: Apakah proksi menyimpan log?

Bisa. Proksi menangani setiap permintaan yang diteruskannya, sehingga operatornya mungkin mencatat alamat IP Anda, situs yang Anda kunjungi, dan waktunya. Periksa siapa yang menjalankannya dan apa isi kebijakan privasinya.

Q8: Kapan proksi sudah cukup?

Proksi bisa cukup untuk tugas berisiko rendah, seperti mengubah lokasi yang tampak pada satu browser. Untuk perbankan, Wi-Fi publik, atau melindungi setiap aplikasi di perangkat, VPN adalah pilihan yang lebih aman karena mengenkripsi semua lalu lintas.

Q9: Bisakah proksi melindungi semua aplikasi di ponsel saya?

Tidak. Hanya aplikasi yang mematuhi pengaturan proksi yang memakainya; aplikasi lainnya tersambung langsung. Sebaliknya, aplikasi VPN merutekan semua aplikasi di ponsel melalui terowongan terenkripsinya.

Q10: Apa itu proksi SOCKS5?

SOCKS5, yang didefinisikan dalam RFC 1928, adalah protokol proksi yang berada di antara lapisan aplikasi dan lapisan transport. SOCKS5 dapat meneruskan koneksi TCP dan datagram UDP serta mendukung autentikasi, tetapi tidak memiliki enkripsi bawaan. [1]

Pos 10: FAQ Lanjutan VPN (Bagian C)

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

Q1: Di lapisan jaringan mana proksi dan VPN bekerja?

Proksi HTTP bekerja di lapisan aplikasi (Layer 7) dan memahami permintaan web. SOCKS5 berada di antara lapisan aplikasi dan lapisan transport. Protokol VPN seperti IPsec atau WireGuard bekerja di lapisan jaringan, sehingga dapat membawa semua lalu lintas IP dari perangkat.

Q2: Apakah situs HTTPS tetap terenkripsi saat melalui proksi?

Ya. Saat Anda membuka situs HTTPS melalui proksi, enkripsi TLS berjalan end-to-end antara browser Anda dan situs tersebut, sehingga proksi melihat domainnya tetapi tidak melihat isi halamannya. Halaman HTTP biasa tetap dapat dibaca.

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 proksi transparan dan siapa yang memakainya?

Proksi transparan mencegat lalu lintas tanpa pengaturan apa pun di perangkat pengguna. Sekolah, perusahaan, dan ISP memakainya untuk caching atau pemfilteran konten. Pengguna sering tidak tahu keberadaannya, dan proksi ini tidak memberi mereka privasi sama sekali.

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: Mengapa proksi bisa terasa lebih cepat daripada koneksi VPN?

Proksi dasar melewatkan enkripsi dan hanya menangani lalu lintas dari satu aplikasi, sehingga pemrosesannya lebih sedikit. VPN mengenkripsi setiap paket dari perangkat. Dengan protokol modern, perbedaannya sering kecil, dan perlindungan yang diberikan proksi jauh lebih sedikit.

Q8: Bisakah situs web mengetahui bahwa saya memakai proksi atau VPN?

Sering kali, ya. Banyak situs mencocokkan alamat IP dengan daftar server proksi dan VPN yang dikenal, dan proksi HTTP mungkin menambahkan header seperti Via atau X-Forwarded-For. Layanan streaming umumnya memblokir keduanya.

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 proksi menghentikan pelambatan oleh ISP?

Jarang. Proksi dasar tidak mengenkripsi lalu lintas, sehingga ISP tetap dapat melihat jenis aktivitasnya. VPN menyembunyikan jenis lalu lintas, tetapi tidak satu pun dari kedua alat ini mengatasi kemacetan jaringan atau batas kuota data.

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. STANDAR SOCKS

SOCKS Protocol Version 5 diterbitkan oleh IETF sebagai RFC 1928 pada Maret 1996 dan hingga kini masih menjadi spesifikasi acuan untuk proksi SOCKS5 yang dipakai browser dan aplikasi. [1]

2. LAPISAN SHIM

RFC 1928 menggambarkan SOCKS sebagai lapisan shim di antara lapisan aplikasi dan lapisan transport, sehingga SOCKS tidak dapat meneruskan lalu lintas lapisan jaringan seperti ICMP. [1]

3. RELAI UDP

SOCKS5 menambahkan perintah UDP ASSOCIATE, yang memungkinkan proksi meneruskan datagram UDP selain koneksi TCP, sesuatu yang tidak ditangani proksi HTTP biasa. [1]

4. PORT SOCKS BAWAAN

Klien SOCKS5 secara bawaan tersambung ke server proksi di port TCP 1080, sesuai definisi RFC 1928; banyak layanan proksi memungkinkan pengguna memilih port lain. [1]

5. PERANTARA HTTP

Standar HTTP (RFC 9110) mendefinisikan proksi sebagai agen penerus pesan yang dipilih oleh klien, yang meneruskan permintaan menuju server asal.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) memeriksa isi paket dan pola lalu lintas; lalu lintas proksi yang tidak terenkripsi sepenuhnya terlihat olehnya, sedangkan lalu lintas VPN jauh lebih sedikit terungkap.

7. VPN LAPISAN JARINGAN

IPsec, yang dijelaskan dalam NIST SP 800-77, melindungi lalu lintas di lapisan jaringan, sehingga paket IP setiap aplikasi dapat diamankan tanpa pengaturan per aplikasi. [2]

8. CAKUPAN HANYA BROWSER

Proksi yang diatur di satu browser hanya memengaruhi browser itu; klien email, game, dan pembaruan sistem tetap memakai koneksi normal perangkat.

9. TOR VS. PROKSI

Tor mengirim lalu lintas melalui tiga relai sukarela (guard, middle, dan exit) dan biasanya diakses melalui proksi SOCKS lokal, sehingga menambahkan lapisan yang tidak dapat diberikan oleh satu proksi saja.

10. KOMPROMI KECEPATAN

Proksi bisa tampak lebih cepat karena melewatkan enkripsi, tetapi protokol VPN modern seperti WireGuard hanya menambah sedikit overhead sambil melindungi semua lalu lintas perangkat.

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Kunci Jawaban: Membandingkan server proksi dan jaringan privat virtual, perbedaan enkripsi, dan perutean tingkat aplikasi vs seluruh sistem

1 **Lapisan OSI Proksi** PROTOKOL — **Jawaban Benar: C**

CATATAN PENGAJAR

Proksi HTTP/HTTPS standar bekerja di lapisan aplikasi (Lapisan 7) dan mengalihkan lalu lintas browser tertentu, tanpa perutean jaringan untuk seluruh sistem.

2 **Soal 2** — **Jawaban Benar: B**

CATATAN PENGAJAR

SOCKS5 meneruskan lalu lintas TCP dan UDP di antara lapisan aplikasi dan lapisan transport tetapi secara bawaan tidak mengenkripsi, sedangkan proksi HTTP menangani permintaan web.

3 **Enkripsi Sistem VPN** KEAMANAN WI-FI — **Jawaban Benar: B**

CATATAN PENGAJAR

VPN membungkus dan mengenkripsi semua lalu lintas sistem operasi, sedangkan proksi hanya mengalihkan lalu lintas aplikasi yang diatur.

4 **Proksi Tanpa Enkripsi** KONTROL ROUTING — **Jawaban Benar: A**

CATATAN PENGAJAR

Proksi HTTP meneruskan lalu lintas browser di lapisan aplikasi tanpa mengenkripsi muatan paket, sehingga operator jaringan atau ISP masih bisa melacak isinya.

5 **Celah Pintasan** PRIVASI — **Jawaban Benar: D**

CATATAN PENGAJAR

Proksi browser hanya berlaku untuk browser itu sendiri. Aplikasi latar belakang, pembaruan sistem operasi, dan klien email melewati proksi dan membuka alamat IP asli Anda.

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Soal 6** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

SOCKS5 meneruskan lalu lintas di antara lapisan aplikasi dan lapisan transport tetapi secara bawaan tidak melakukan enkripsi, sehingga isi paket tetap dapat dibaca selama transit.

7 **Terowongan Lapisan Jaringan** KECEPATAN — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Karena berjalan di lapisan jaringan, VPN merutekan dan mengenkripsi lalu lintas keluar dari perangkat Anda, sehingga membantu melindungi lalu lintas di seluruh sistem.

8 **Batas Enkripsi Proksi** RISIKO SNIFFING — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Proksi kadang lebih cepat justru karena TIDAK mengenkripsi, sehingga data rentan diperiksa.

9 **Pengalihan Tingkat Aplikasi** FIREWALL — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Berbeda dari VPN untuk seluruh sistem, server proksi harus diatur manual di pengaturan browser atau kolom proksi tiap aplikasi.

10 **Risiko Pelacakan ISP** TANPA LOG — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Karena proksi HTTP/SOCKS5 standar tidak mengenkripsi muatan data, ISP lokal tetap dapat melihat semua aktivitas online Anda.

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

G 1. Proksi HTTP	H 2. Proksi SOCKS5	E 3. Terowongan VPN	A 4. Seluruh Sistem
B 5. Lapisan OSI 7	C 6. Dukungan UDP	D 7. Proksi Browser	F 8. Visibilitas ISP

POS 3: KUNCI ISTILAH KUNCI

1 PROKSI	2 TEROWONGAN	3 SOCKS5	4 APLIKASI
5 ENKRIPSI	6 SISTEM		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 E – PINTASAN	2 F – SISTEM	3 A – SOCKS5	4 G – LALULINTAS
5 C – HTTPS	6 D – LATENSI	7 H – MUATAN	8 B – HTTP

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan Proksi HTTP, Proksi SOCKS5, dan Terowongan VPN dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

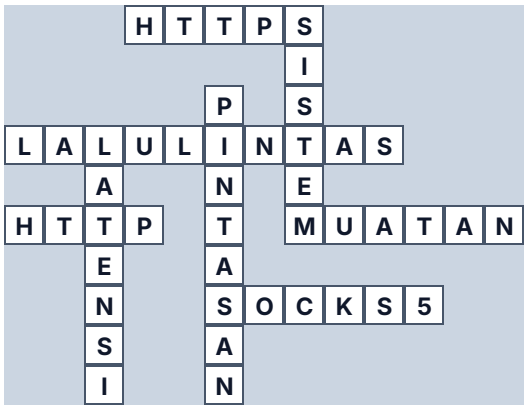
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

C	R	N	I	G	N	R	M	P	X	Q	O	C	U	S
T	E	A	L	J	B	A	B	S	C	P	X	L	K	Y
K	X	T	T	K	D	Q	M	J	O	D	I	N	N	K
Q	P	A	M	E	T	S	I	S	G	C	M	M	Q	R
S	T	U	T	G	L	C	S	Q	O	H	K	S	B	W
I	D	M	S	Z	A	V	P	C	S	Z	W	S	F	K
S	H	Z	D	N	L	D	Q	I	X	P	P	C	5	U
N	B	A	Z	N	U	D	K	A	N	D	T	O	D	F
E	H	I	D	R	L	Q	M	E	I	T	R	T	Z	S
T	F	Q	V	F	I	H	A	A	Q	O	A	N	H	P
A	T	X	Q	K	N	T	R	U	S	D	N	S	Y	B
L	F	S	X	W	T	T	J	A	R	Z	Y	Y	A	L
G	I	M	R	J	A	P	M	L	T	O	H	Q	Q	N
H	Z	A	O	V	S	G	U	B	Y	R	Y	B	H	L
Z	G	J	O	P	N	W	C	M	Z	Y	G	Y	O	W

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

1 mendatar: HTTPS Versi HTTP terenkripsi yang melindungi lalu lintas antara browser dan situs web (5 huruf)

4 mendatar: LALULINTAS Data jaringan yang tetap terlihat oleh ISP jika dikirim lewat proksi tanpa enkripsi (10 huruf)

6 mendatar: HTTP Proksi lapisan aplikasi yang mengalihkan lalu lintas browser tertentu (4 huruf)

7 mendatar: MUATAN Isi paket data yang tidak dienkripsi oleh server proksi standar (6 huruf)

8 mendatar: SOCKS5 Protokol proksi di antara lapisan aplikasi dan transport, tanpa enkripsi, yang dapat meneruskan UDP maupun TCP (6 huruf)

PETUNJUK MENURUN

2 menurun: SISTEM Tingkat sistem operasi tempat VPN mengenkripsi lalu lintas semua aplikasi (6 huruf)

3 menurun: PINTASAN Cara menembus blokir dengan mengalihkan lalu lintas lewat server perantara (8 huruf)

5 menurun: LATENSI Jeda tambahan saat lalu lintas melewati server perantara (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1. CSKS5O	SOCKS5	5. PHTT	HTTP
2. HSPTT	HTTPS	6. STNLEIA	LATENSI
3. TIPASNAN	PINTASAN	7. ESTMSI	SISTEM
4. IALSUTNLAL	LALULINTAS	8. ANMATU	MUATAN

KUNCI TANTANGAN SANDI RAHASIA

"PROKSI MENYEMBUNYIKAN TETAPI TIDAK MENGENKRIPSI"

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.
- Proksi vs VPN: Proksi browser dasar tidak mengenkripsi lalu lintasnya. VPN mengenkripsi semua yang ada di perangkat, sehingga paket yang dicegat tidak dapat dibaca oleh penyadap lokal.

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.
- Mana yang Lebih Baik: Keduanya memberinya IP dari negara asalnya, tetapi proksi hanya mencakup aplikasi yang dikonfigurasi, sedangkan VPN juga mengenkripsi semua lalu lintas perangkatnya.