Nama: _____ Tanggal: _____ Nilai: _____

WireGuard vs OpenVPN Lembar Kerja

Membandingkan protokol WireGuard dan OpenVPN, ukuran basis kode, kecepatan, dan standar kriptografi

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 kerumitan basis kode dan kecepatan audit kedua protokol.
- Analisis peningkatan performa saat berjalan di ruang kernel.
- Bandingkan sandi OpenSSL dengan kriptografi modern WireGuard.
- Siapkan pasangan kunci publik dan privat untuk jabat tangan antar-peer.
- Rutekan lalu lintas VPN melalui port firewall TCP dan UDP.

PETUNJUK LEMBAR KERJA PERBANDINGAN PROTOKOL

Jawab soal pilihan ganda dan benar/salah, lengkapi kalimat rumpang dengan kata dari bank kata, cocokkan definisi, lalu selesaikan teka-teki silang dan pencarian kata. Terapkan pengetahuan Anda untuk mengaudit protokol modern. Akhiri dengan aktivitas bonus Berpikir Cepat.

WIREGUARD VS OPENVPN (PENGANTAR)

Memilih protokol VPN berarti menyeimbangkan kecepatan dan pilihan konfigurasi. OpenVPN telah lama menjadi standar dan menawarkan fleksibilitas konfigurasi TCP/UDP. WireGuard adalah pengganti modern yang berjalan langsung di ruang kernel dengan sekitar 4.000 baris kode. Memahami perbedaan protokol adalah kunci untuk mengoptimalkan jaringan yang aman.

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

Pos 1: Tantangan Pilihan Ganda

1. **1. Berapa perkiraan ukuran basis kode protokol WireGuard?**
   - A. Sekitar 70.000 baris
   - B. Lebih dari 100.000 baris
   - C. Kurang dari 1.000 baris
   - D. Sekitar 4.000 baris

2. **2. Di ruang mana dalam sistem operasi WireGuard berjalan?**
   - A. Ruang pengguna
   - B. Ruang kernel
   - C. Ruang aplikasi
   - D. Ruang virtual

3. **3. Pustaka kriptografi apa yang terutama diandalkan OpenVPN?**
   - A. ChaCha20-Poly1305
   - B. Pustaka kriptografi OpenSSL
   - C. Framework protokol Noise
   - D. Pengodean DES teks biasa

4. **4. Apa keunggulan performa utama WireGuard dibanding OpenVPN?**
   - A. Jabat tangan koneksi lebih cepat dan latensi lebih rendah
   - B. Tidak memerlukan alamat IP publik
   - C. Dukungan bawaan untuk koneksi dial-up lama
   - D. Sama sekali tidak memakai baterai di perangkat seluler

5. **5. Bagaimana WireGuard mengautentikasi koneksi antar-peer?**
   - A. Dengan bertukar kata sandi pengguna biasa
   - B. Dengan memverifikasi sertifikat pendaftaran domain
   - C. Dengan pasangan kunci publik dan privat yang statis
   - D. Dengan memeriksa nomor seri perangkat keras

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Basis kode WireGuard yang ringkas membuatnya jauh lebih mudah diaudit.

Benar Salah

7 Pertanyaan 7

7. OpenVPN umumnya lebih cepat daripada WireGuard karena berjalan di ruang kernel.

Benar Salah

8 Pertanyaan 8

8. OpenVPN sangat mudah dikonfigurasi dan mendukung protokol UDP maupun TCP.

Benar Salah

9 Pertanyaan 9

9. WireGuard memakai kriptografi modern seperti ChaCha20 untuk enkripsi paket yang cepat.

Benar Salah

10 Pertanyaan 10

10. WireGuard memerlukan pengaturan otoritas sertifikat yang rumit untuk autentikasi.

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. Protokol modern _____ beroperasi langsung di dalam kernel sistem operasi.
2. Protokol lama _____ mengandalkan pustaka kriptografi OpenSSL.
3. Menjalankan kode di _____ mengurangi beban peralihan konteks.
4. OpenVPN berjalan di _____ dan merutekan paket melalui antarmuka virtual.
5. WireGuard memakai _____ publik dan privat untuk mengenali peer koneksi.
6. Basis kode yang kecil meningkatkan _____ perangkat lunak dari sisi keamanan.

BANK KATA KOSAKATA

KEMUDAHAN AUDIT | OPENSSL | OPENVPN | PASANGAN KUNCI | RUANG KERNEL | RUANG PENGGUNA | TCP/UDP | WIREGUARD

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Jaringan

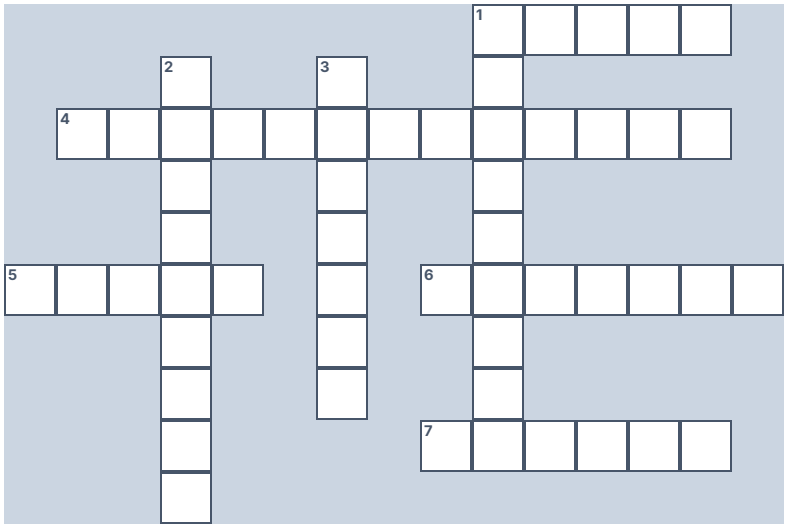
MENCOCOKKAN DEFINISI

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	Area eksekusi tempat OpenVPN berjalan sehingga muncul beban perpindahan konteks.
☐	2. OpenVPN	B	Ukuran basis kode WireGuard yang ringkas, sehingga jauh lebih mudah diaudit.
☐	3. Ruang Kernel	C	Pustaka kriptografi yang diandalkan OpenVPN untuk algoritme sandi.
☐	4. Ruang Pengguna	D	Protokol transport yang didukung OpenVPN; WireGuard sendiri hanya berjalan melalui UDP.
☐	5. 4.000 Baris	E	Area eksekusi sistem operasi tempat WireGuard berjalan demi kecepatan.
☐	6. OpenSSL	F	Token asimetris yang dipakai WireGuard untuk memverifikasi koneksi antar-peer.
☐	7. Pasangan Kunci	G	Protokol VPN modern yang dirancang untuk kecepatan tinggi dan audit kode yang mudah.
☐	8. TCP/UDP	H	Protokol lama yang tangguh dengan basis kode konfigurasi yang besar dan rumit.

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. Pemeriksaan kode yang jauh lebih mudah pada basis kode WireGuard yang ringkas (5)

4. Area eksekusi tempat OpenVPN berjalan, sehingga menimbulkan overhead perpindahan konteks (13)

5. Kerangka protokol kriptografi yang menjadi dasar handshake WireGuard (5)

6. Ukuran basis kode WireGuard yang kecil sehingga jauh lebih mudah diaudit (7)

7. Area eksekusi sistem operasi tempat WireGuard berjalan demi kecepatan (6)

PETUNJUK MENURUN

1. Prosedur matematis yang dipakai untuk mengenkripsi data (9)

2. Pertukaran awal yang memakai pasangan kunci asimetris untuk memverifikasi koneksi peer (9)

3. Pustaka kriptografi yang diandalkan OpenVPN untuk algoritme sandi (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: Pemeriksaan kode yang jauh lebih mudah pada basis kode WireGuard yang ringkas (5 huruf):

4 mendatar: Area eksekusi tempat OpenVPN berjalan, sehingga menimbulkan overhead perpindahan konteks (13 huruf):

5 mendatar: Kerangka protokol kriptografi yang menjadi dasar handshake WireGuard (5 huruf):

6 mendatar: Ukuran basis kode WireGuard yang kecil sehingga jauh lebih mudah diaudit (7 huruf):

7 mendatar: Area eksekusi sistem operasi tempat WireGuard berjalan demi kecepatan (6 huruf):

PETUNJUK MENURUN

1 menurun: Prosedur matematis yang dipakai untuk mengenkripsi data (9 huruf):

2 menurun: Pertukaran awal yang memakai pasangan kunci asimetris untuk memverifikasi koneksi peer (9 huruf):

3 menurun: Pustaka kriptografi yang diandalkan OpenVPN untuk algoritme sandi (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.

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

DAFTAR KOSAKATA

KERNEL RUANGPENGGUNA OPENSSL NOISE AUDIT RINGKAS
ALGORITME HANDSHAKE

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. KERNEL**
- **B. RUANGPENGGUNA**
- **C. OPENSSL**
- **D. NOISE**
- **E. AUDIT**
- **F. RINGKAS**
- **G. ALGORITME**
- **H. HANDSHAKE**

DEFINISI & KOLOM PENCOCOKAN

1. Ukuran basis kode WireGuard yang kecil sehingga jauh lebih mudah diaudit.
2. Pustaka kriptografi yang diandalkan OpenVPN untuk algoritme sandi.
3. Area eksekusi tempat OpenVPN berjalan, sehingga menimbulkan overhead perpindahan konteks.
4. Prosedur matematis yang dipakai untuk mengenkripsi data.
5. Pertukaran awal yang memakai pasangan kunci asimetris untuk memverifikasi koneksi peer.
6. Pemeriksaan kode yang jauh lebih mudah pada basis kode WireGuard yang ringkas.
7. Area eksekusi sistem operasi tempat WireGuard berjalan demi kecepatan.
8. Kerangka protokol kriptografi yang menjadi dasar handshake WireGuard.

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. **RKNELE** _____
2. **OELSSNP** _____
3. **DATIU** _____
4. **REMOTIALG** _____
5. **GUUANGAPGERNN** _____
6. **SNIEO** _____
7. **RAKSIGN** _____
8. **ESKHDAHAN** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Alasan memilih WireGuard			
2	Janji penyedia VPN yang baik			
3	Alasan memilih OpenVPN			
4	Alasan memakai VPN saat bepergian			
5	Hal yang bisa dilihat penyedia internet Anda			
6	Cara mengenali Wi-Fi palsu			
7	Mitos tentang VPN			
8	Tempat Anda akan memakai VPN			
9	Hal yang cepat dalam kehidupan sehari-hari			
10	Hal yang tidak bisa dicegah VPN			
11	Hal yang membuat kode lebih mudah diperiksa			
12	Hal yang bisa disembunyikan VPN			
13	Perbedaan WireGuard dan OpenVPN			
14	Kata yang berkaitan dengan privasi			
15	Nama enkripsi yang Anda ketahui			

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 pakai Wi-Fi kafe, dan aplikasi VPN-ku membolehkan aku memilih WireGuard atau OpenVPN. Panggilan videoku terus terputus saat aku berpindah antara jaringan kafe dan hotspot ponselku. Protokol mana yang sebaiknya kupilih, dan kenapa protokol itu lebih baik menangani perpindahan jaringan?"

ALEX (MAHASISWA YANG SEDANG BEPERGIAN)

👩‍💻 "Aku sedang di luar negeri dan memakai jaringan hotel yang sepertinya memblokir sebagian besar lalu lintas VPN. WireGuard sama sekali tidak bisa tersambung, padahal aku perlu mengakses sumber daya sekolahku di negara asal. Apa yang kemungkinan diblokir, dan bagaimana OpenVPN bisa membantuku menembusnya?"

Pos 9: Memecahkan Sandi

Untuk menuntaskan latihan audit protokol, pecahkan pesan tersembunyi tentang eksekusi di ruang kernel ini.

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

11 15 4 5   4 9   11 5 18 14 5 12

13 5 13 2 21 1 20   20 5 18 15 23 15 14 7 1 14

3 5 16 1 20

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 protokol itu penting?

Protokol menentukan cara VPN membangun terowongannya, kriptografi apa yang melindungi data Anda, dan seberapa cepat VPN tersambung dan tersambung kembali. WireGuard dan OpenVPN adalah dua protokol open-source yang paling banyak ditawarkan aplikasi VPN, dan keduanya menawarkan kompromi yang berbeda antara kesederhanaan, kecepatan, dan kemudahan konfigurasi.

Q3: Apakah salah satunya lebih privat daripada yang lain?

Tidak ada protokol yang membuat Anda anonim. Keduanya mengenkripsi lalu lintas terowongan dengan cipher yang kuat; privasi Anda terutama bergantung pada apa yang dicatat penyedia VPN dan cara penyedia mengelola kunci, akun, dan server.

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 keduanya open source?

Ya. WireGuard dan OpenVPN edisi komunitas sama-sama memublikasikan kode sumbernya, sehingga peneliti independen dapat meninjaunya. Basis kode WireGuard yang kecil membuat peninjauan menyeluruh jauh lebih cepat.

Pos 10: FAQ Dasar VPN (Bagian B)

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

Q6: Mana yang lebih cepat?

WireGuard biasanya lebih cepat: protokol ini berjalan di kernel, memakai enkripsi ChaCha20-Poly1305 yang ramping, dan menyelesaikan handshake dengan cepat. OpenVPN memiliki overhead lebih besar, tetapi kecepatan sebenarnya juga bergantung pada beban server dan jarak.

Q7: Apakah keduanya dapat berjalan melalui TCP dan UDP?

Tidak. OpenVPN dapat berjalan melalui UDP atau TCP, dan mode TCP membantu di jaringan yang memblokir UDP. WireGuard hanya mengirim paketnya melalui UDP, sehingga bisa gagal di jaringan yang hanya mengizinkan TCP. [4]

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 WireGuard dan OpenVPN di ponsel?

Bisa. WireGuard bersifat lintas platform, dengan aplikasi untuk Windows, macOS, Linux, iOS, dan Android, dan klien OpenVPN tersedia untuk sistem yang sama. Sebagian besar aplikasi VPN memungkinkan Anda memilih salah satunya. [1]

Q10: Mengapa WireGuard begitu kecil?

WireGuard mendukung satu set cipher modern yang tetap, bukan banyak pilihan. Implementasinya di Linux memerlukan kurang dari 4.000 baris kode, sehingga lebih mudah diaudit daripada basis kode VPN yang lebih besar. [3]

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: Cipher apa yang dipakai WireGuard?

WireGuard memakai ChaCha20 dengan Poly1305 untuk enkripsi, Curve25519 untuk pertukaran kunci, BLAKE2s untuk hashing, dan framework Noise untuk handshake-nya. Tidak ada negosiasi cipher, sehingga pengguna tidak dapat memilih opsi yang lemah. [2]

Q3: Cipher dan pustaka apa yang dapat dipakai OpenVPN?

OpenVPN terintegrasi erat dengan pustaka OpenSSL dan memakai TLS untuk bertukar kunci. Administrator dapat memilih cipher kanal data seperti AES-256-GCM, yang menambah fleksibilitas tetapi juga membuka peluang pengaturan yang lemah. [4]

Q4: Bagaimana setiap protokol mengautentikasi peer?

Peer WireGuard saling mengenali melalui kunci publik statis, mirip dengan bertukar kunci SSH, dan setiap kunci dipetakan ke IP terowongan yang diizinkan. OpenVPN biasanya mengandalkan otoritas sertifikat dengan sertifikat X.509, yang sering dikombinasikan dengan nama pengguna dan kata sandi.

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 yang terjadi saat saya beralih dari Wi-Fi ke data seluler?

WireGuard bersifat connectionless: protokol ini mengirim paket dari alamat baru dan terowongan tetap berjalan setelah handshake singkat. OpenVPN menyimpan status sesi, sehingga perubahan jaringan dapat memerlukan penyambungan ulang yang sedikit lebih lama.

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: Apakah OpenVPN masih pilihan yang baik jika WireGuard lebih cepat?

Ya. OpenVPN sudah matang dan banyak diterapkan, dapat berjalan melalui TCP saat UDP diblokir, dan mendukung pengaturan perusahaan berbasis sertifikat. Banyak penyedia menawarkan kedua protokol sehingga pengguna dapat beralih jika salah satunya diblokir atau lambat.

Q9: Port apa yang mereka pakai?

Port standar OpenVPN adalah 1194, tetapi dapat dipindahkan ke port UDP atau TCP mana pun, termasuk 443. WireGuard mendengarkan di port UDP yang diatur dalam konfigurasinya; 51820 adalah port yang dipakai dalam contoh resminya.

Q10: Protokol mana yang lebih mudah diatur secara manual?

WireGuard biasanya lebih sederhana: buat pasangan kunci, tukarkan kunci publik, dan cantumkan allowed IPs. OpenVPN memerlukan sertifikat, CA, dan lebih banyak opsi, meskipun profil .ovpn menggabungkan semuanya ke dalam satu berkas.

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 kelompok vendor yang mencakup Microsoft dan diterbitkan sebagai RFC 2637 pada Juli 1999 untuk mendukung VPN akses jarak jauh. [6]

2. DUA TRANSPORT

OpenVPN dapat membawa terowongannya melalui UDP atau TCP, dan dalam mode TLS, kanal kontrol dan kanal datanya berbagi satu port. [4]

3. REVOLUSI WIREGUARD

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

4. KRIPTOGRAFI MODERN

WireGuard menggabungkan ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24, dan HKDF di dalam framework protokol Noise, tanpa pilihan cipher yang bisa salah diatur oleh pengguna. [2]

5. OPENSSL DI DALAM OPENVPN

OpenVPN terintegrasi erat dengan pustaka OpenSSL dan memperoleh banyak kemampuan kriptografisnya dari pustaka itu, termasuk TLS yang dipakai untuk bertukar kunci. [4]

6. DEEP PACKET INSPECTION

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

7. KUNCI BERGAYA SSH

Koneksi WireGuard diatur dengan bertukar kunci publik sederhana, mirip dengan bertukar kunci SSH, tanpa memerlukan otoritas sertifikat. [1]

8. LINTAS PLATFORM

WireGuard pertama kali dirilis untuk kernel Linux dan kini tersedia untuk Windows, macOS, BSD, iOS, dan Android, sehingga protokol yang sama dapat bekerja di sebagian besar perangkat. [1]

9. FORWARD SECRECY

WireGuard mengulang handshake Noise_IK setiap beberapa menit untuk merotasi kunci sesi simetris, sehingga memberikan perfect forward secrecy meskipun kunci jangka panjang kelak bocor. [2]

10. ANTARMUKA TUN/TAP

OpenVPN dirancang untuk bekerja dengan antarmuka jaringan virtual TUN/TAP, yang tersedia di sebagian besar platform dan membawa paket-paket terowongan. [4]

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

[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] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Kunci Jawaban: Membandingkan protokol WireGuard dan OpenVPN, ukuran basis kode, kecepatan, dan standar kriptografi

1 **Ukuran Kode WireGuard** PROTOKOL — **Jawaban Benar: D**

CATATAN PENGAJAR

WireGuard sangat ringkas, hanya sekitar 4.000 baris kode. Hal ini menjaga permukaan serangan tetap kecil dan mempermudah audit.

2 **Kecepatan di Ruang Kernel** LATENSI — **Jawaban Benar: B**

CATATAN PENGAJAR

Dengan berjalan langsung di ruang kernel, WireGuard menghindari overhead peralihan konteks, sehingga memungkinkan throughput tinggi.

3 **Soal 3** — **Jawaban Benar: B**

CATATAN PENGAJAR

OpenVPN terintegrasi erat dengan OpenSSL, yang menyediakan cipher seperti AES-GCM dan membuatnya sangat mudah dikonfigurasi tetapi lebih rumit.

4 **Performa Protokol** KONTROL ROUTING — **Jawaban Benar: A**

CATATAN PENGAJAR

WireGuard menyelesaikan jabat tangan dalam hitungan milidetik dan langsung menyesuaikan diri saat berpindah jaringan (misalnya dari Wi-Fi ke seluler).

5 **Kriptografi Asimetris** PRIVASI — **Jawaban Benar: C**

CATATAN PENGAJAR

WireGuard memakai Cryptokey Routing yang mengaitkan kunci publik dengan alamat IP terowongan yang diizinkan, mirip pengaturan SSH.

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Soal 6** **Jawaban Benar: Benar**

CATATAN PENGAJAR

Implementasi WireGuard di Linux kurang dari 4.000 baris, sehingga tim keamanan dapat meninjaunya jauh lebih cepat daripada basis kode VPN yang jauh lebih besar seperti OpenVPN.

7 **Latensi Ruang Pengguna** KECEPATAN **Jawaban Benar: Salah**

CATATAN PENGAJAR

OpenVPN berjalan di ruang pengguna dan meneruskan paket bolak-balik dari antarmuka virtual kernel, yang menambah overhead peralihan konteks (kecuali memakai offload kernel seperti OpenVPN DCO).

8 **Konfigurasi OpenVPN** RISIKO SNIFFING **Jawaban Benar: Benar**

CATATAN PENGAJAR

OpenVPN dapat berjalan melalui TCP (untuk keandalan dan menembus firewall) atau UDP (untuk kecepatan), sehingga cocok dengan firewall perusahaan yang rumit.

9 **Kriptografi Modern** FIREWALL **Jawaban Benar: Benar**

CATATAN PENGAJAR

WireGuard meninggalkan sandi lama dan memakai primitif modern yang aman seperti ChaCha20 dan Poly1305, yang berjalan cepat di CPU ponsel.

10 **Penyederhanaan dengan Pasangan Kunci** TANPA LOG **Jawaban Benar: Salah**

CATATAN PENGAJAR

WireGuard tidak memakai sertifikat atau hierarki CA yang rumit; WireGuard mengandalkan pasangan kunci publik/privat sederhana yang dipertukarkan antar-peer.

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. WireGuard	H 2. OpenVPN	E 3. Ruang Kernel	A 4. Ruang Pengguna
B 5. 4.000 Baris	C 6. OpenSSL	F 7. Pasangan Kunci	D 8. TCP/UDP

POS 3: KUNCI ISTILAH KUNCI

1 WIREGUARD	2 OPENVPN	3 RUANG KERNEL	4 RUANG PENGGUNA
5 PASANGAN KUNCI	6 KEMUDAHAN AUDIT		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 F – RINGKAS	2 C – OPENSSL	3 B – RUANGPENGGUNA	4 G – ALGORITME
5 H – HANDSHAKE	6 E – AUDIT	7 A – KERNEL	8 D – NOISE

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan WireGuard, OpenVPN, dan Ruang Kernel dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

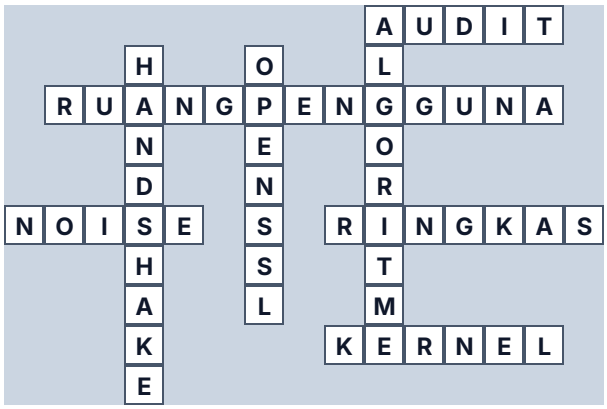
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

1 mendatar: AUDIT Pemeriksaan kode yang jauh lebih mudah pada basis kode WireGuard yang ringkas (5 huruf)

4 mendatar: RUANGPENGGUNA Area eksekusi tempat OpenVPN berjalan, sehingga menimbulkan overhead perpindahan konteks (13 huruf)

5 mendatar: NOISE Kerangka protokol kriptografi yang menjadi dasar handshake WireGuard (5 huruf)

6 mendatar: RINGKAS Ukuran basis kode WireGuard yang kecil sehingga jauh lebih mudah diaudit (7 huruf)

7 mendatar: KERNEL Area eksekusi sistem operasi tempat WireGuard berjalan demi kecepatan (6 huruf)

PETUNJUK MENURUN

1 menurun: ALGORITME Prosedur matematis yang dipakai untuk mengenkripsi data (9 huruf)

2 menurun: HANDSHAKE Pertukaran awal yang memakai pasangan kunci asimetris untuk memverifikasi koneksi peer (9 huruf)

3 menurun: OPENSSL Pustaka kriptografi yang diandalkan OpenVPN untuk algoritme sandi (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1.	RKNELE	KERNEL	5.	GUUANGAPGERNN	RUANGPENGGUNA
2.	OELSSNP	OPENSSL	6.	SNIEO	NOISE
3.	DATIU	AUDIT	7.	RAKSIGN	RINGKAS
4.	REMOTIALG	ALGORITME	8.	ESKHDAHAN	HANDSHAKE

KUNCI TANTANGAN SANDI RAHASIA

"KODE DI KERNEL MEMBUAT TEROWONGAN CEPAT"

Kunci Jawaban Studi Kasus

A Skenario A: Memilih Protokol

SNIFFING & ENKRIPSI | Dilema Sarah

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Rekomendasi: WireGuard. Desainnya yang ringan dan connectionless memungkinkan terowongan pulih dengan cepat saat jaringannya berubah, dan ChaCha20-Poly1305 menjaga enkripsi tetap cepat.
- Keamanan: Kedua protokol mengenkripsi lalu lintasnya di Wi-Fi kafe, sehingga keduanya melindungi login-nya jika dikonfigurasi dengan benar; pilihan ini terutama memengaruhi kecepatan dan stabilitas.

B Skenario B: Menembus Blokir VPN

GEOBLOKIR & IP | Dilema Alex

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Penyebab Diblokir: WireGuard hanya memakai UDP, dan firewall hotel kemungkinan memblokir UDP atau mengenali paket WireGuard melalui pemfilteran atau Deep Packet Inspection.
- Cara OpenVPN Membantu: OpenVPN dapat berjalan melalui TCP, termasuk port 443 yang dipakai HTTPS, yang jarang diblokir sepenuhnya oleh firewall hotel karena penjelajahan web bergantung padanya.