Implementasi VPN WireGuard untuk Secure Remote Access

Kelompok 7

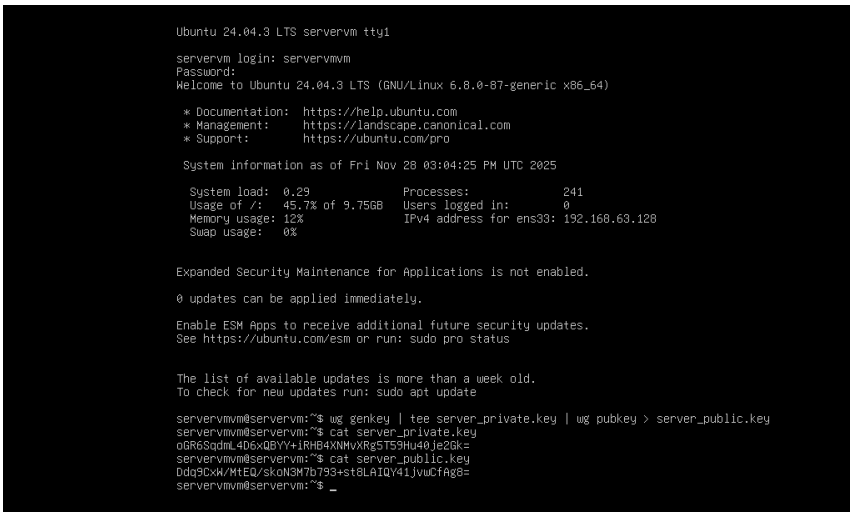
1. Janumelah (2201020048)
2. Mohd Allifyan Baitul Nesam (2201020023)
3. Anjas Revaldo (2201020108)
4. Safitri Wulandari (2201020085)
5. Danish Arya Yudhistira (2201020110)
6. M. Aditya Egi Dwi Nata (2201020141)

Minggu 3: Membuat sertifikat kunci & konfigurasi

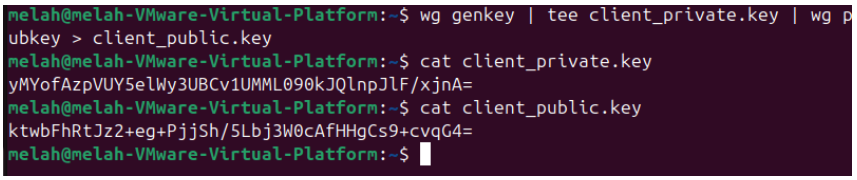
Pada minggu 3 dilakukan proses pembuatan pasangan kunci (key pair) serta penyusunan berkas konfigurasi awal WireGuard pada kedua mesin Linux. Tujuan dari tahap ini adalah menyiapkan identitas kriptografi server dan client sehingga keduanya dapat saling mengenali serta membentuk kanal komunikasi terenkripsi pada tahap pengujian minggu berikutnya.

Tahapan dan Proses:

1. Pembuatan key pair pada server dan client



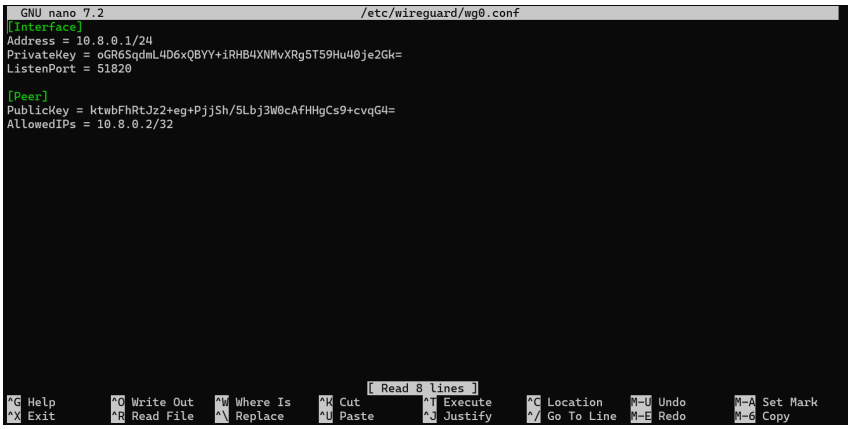
Pada tahap ini dihasilkan private key dan public key untuk mesin server. Private key digunakan untuk autentikasi server, sedangkan public key nantinya dibagikan kepada client agar perangkat dapat melakukan handshake secara aman.



Proses serupa dilakukan pada mesin client, yaitu menghasilkan private key dan public key baru. Key pair ini diperlukan agar server dapat mengenali identitas client saat proses koneksi VPN dilakukan.

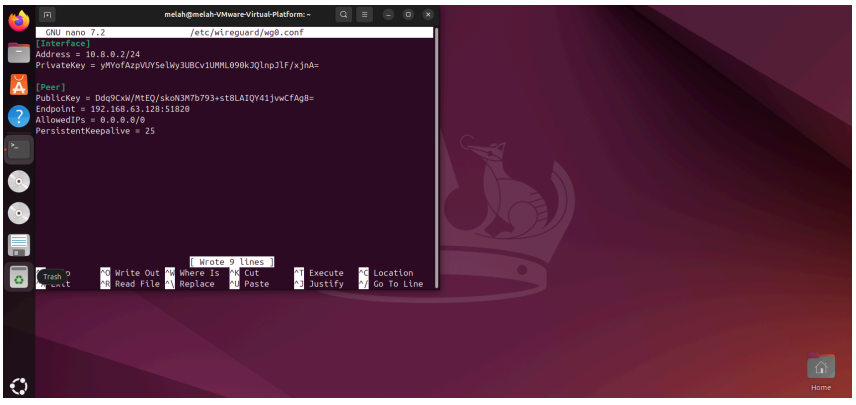
2. Penyusunan konfigurasi WireGuard pada server dan client

Struktur konfigurasi wg0.conf terdiri dari [Interface] untuk pengaturan identitas, alamat IP, dan port dari perangkat dan [Peer] untuk informasi tentang perangkat tujuan dan IP mana saja yang boleh diarahkan melalui tunnel.



Pada gambar di atas sebuah berkas konfigurasi /etc/wireguard/wg0.conf dibuat berisi:

a. Alamat IP virtual server (10.8.0.1/24).
b. Private key server.
c. Port yang digunakan (51820).
d. Serta peer client yang ditambahkan setelah client selesai dikonfigurasi.

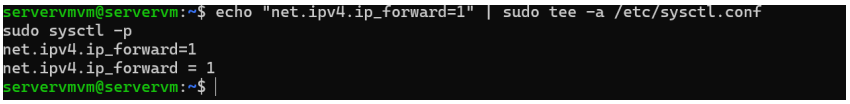


Pada gambar di atas, client juga dibuatkan berkas /etc/wireguard/wg0.conf yang memuat:

a. Alamat IP virtual client (10.8.0.2/24).
b. Private key client.

c. Informasi public key server.
d. Serta endpoint IP server untuk tujuan koneksi.

3. Pengaktifan IP forwarding pada server



Server diatur untuk mengizinkan penerusan paket (IP forwarding). Pengaturan ini diperlukan agar server mampu meneruskan lalu lintas jaringan dari client ke jaringan lain melalui interface VPN.

Hasil:

1. Pasangan kunci (private key dan public key) pada kedua mesin, yaitu server dan client, berhasil dibuat menggunakan perintah wg genkey dan wg pubkey.
2. Berkas konfigurasi wg0.conf pada server dan client telah tersusun dengan struktur yang benar, mencakup alamat IP virtual, private key masing-masing, serta informasi peer.
3. Pengaturan IP forwarding pada server berhasil diaktifkan sehingga siap digunakan untuk proses routing lalu lintas VPN.
4. Tahap persiapan konfigurasi telah selesai, dan lingkungan siap untuk dilanjutkan pada tahap berikutnya, yaitu menjalankan interface WireGuard dan melakukan pengujian konektivitas pada minggu ke-4.