

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

```
Ubuntu 24.04.3 LTS servervm tty1
servervm login: servervmvm
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri Nov 28 03:04:25 PM UTC 2025

System load: 0.29          Processes:      241
Usage of /:  45.7% of 9.75GB Users logged in:    0
Memory usage: 12%         IPv4 address for ens33: 192.168.63.128
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

servervmvm@servervm:~$ wg genkey | tee server_private.key | wg pubkey > server_public.key
servervmvm@servervm:~$ cat server_private.key
oGR6Sqdml4D6xQBYY+IRH84WNWvXRg5T59Hu40je2Gk=
servervmvm@servervm:~$ cat server_public.key
Dd9BckW/1tE0/sk0N3M7b79S+stLA1Q41jvucfng6=
servervmvm@servervm:~$ _
```

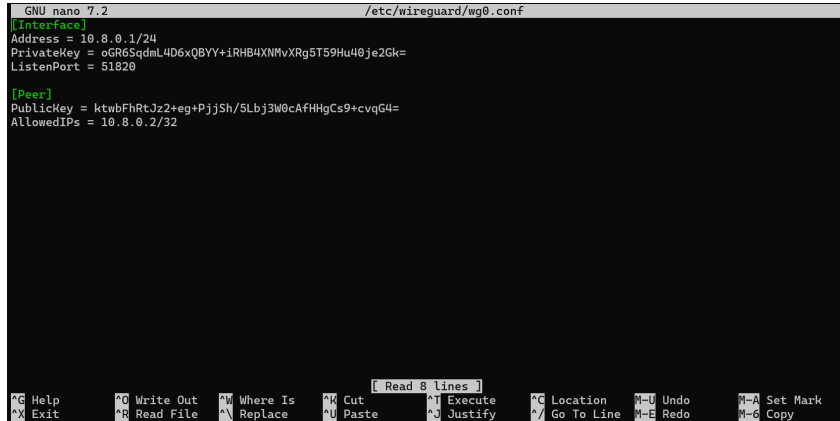
Pada tahap ini dihasilkan private key dan public key untuk mesin server. Private key digunakan untuk autentikasi server, sedangkan public key nantinya dibagikan kepada client agar perangkat dapat melakukan handshake secara aman.

```
melah@melah-VMware-Virtual-Platform:~$ wg genkey | tee client_private.key | wg p
ubkey > client_public.key
melah@melah-VMware-Virtual-Platform:~$ cat client_private.key
yMYofAzpVUY5elWy3UBCv1UMML090kJQlnpJLF/xjnA=
melah@melah-VMware-Virtual-Platform:~$ cat client_public.key
ktwbFhRtJz2+eg+PjjSh/SLbj3W0cAfHHgCs9+cvqG4=
melah@melah-VMware-Virtual-Platform:~$
```

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.

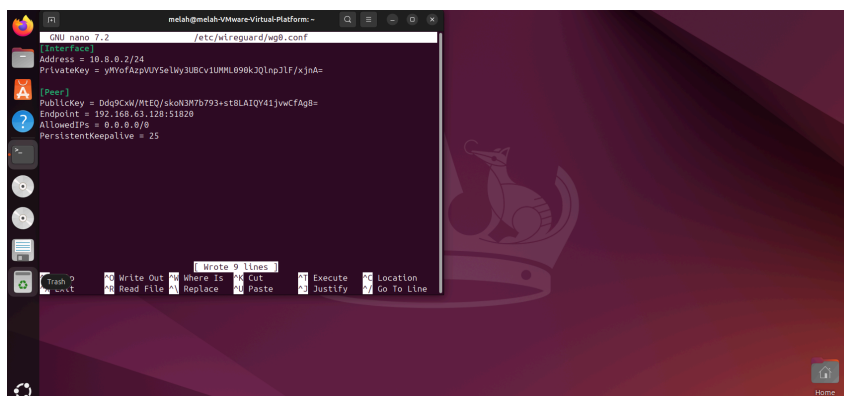


```
GNU nano 7.2 /etc/wireguard/wg0.conf
[Interface]
Address = 10.8.0.1/24
PrivateKey = oGR6SqdML4D6xQBYy+iRHB4XNMvXRg5T59Hu40je2Gk=
ListenPort = 51820

[Peer]
PublicKey = ktwbFhRtJz2+eg+PjjSh/5Lbj3W0cAfHHgCs9+cvqG4=
AllowedIPs = 10.8.0.2/32
```

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

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



```
GNU nano 7.2 /etc/wireguard/wg0.conf
[Interface]
Address = 10.8.0.2/24
PrivateKey = yMyoA2pVUVSeLky3UBCVIUMML090k30lnpJf/xjA=

[Peer]
PublicKey = Ddg9Cw/MtEQ/skN3M7b793+st8LA1QY41jvCfag=
Endpoint = 192.168.63.128:51820
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 25
```

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

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

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

3. Pengaktifan IP forwarding pada server

```
servervmvm@servervm:~$ echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf
sudo sysctl -p
net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
servervmvm@servervm:~$
```

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.