

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 4: Pengujian koneksi titik-ke-titik

Pada minggu 4 dilakukan proses implementasi konfigurasi VPN yang telah disusun pada minggu sebelumnya. Tujuan dari tahap ini adalah memastikan bahwa koneksi terowongan (tunnel) WireGuard dapat berjalan dengan baik, ditandai dengan keberhasilan handshake antara server dan client, serta kemampuan kedua mesin untuk saling berkomunikasi melalui jaringan VPN.

Tahapan dan Proses:

1. Menjalankan interface WireGuard pada server dan client

```
servervmvm@servervm:~$ sudo wg-quick up wg0
[sudo] password for servervmvm:
Sorry, try again.
[sudo] password for servervmvm:
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.8.0.1/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
```

Perintah: `sudo wg-quick up wg0`

Analisis pengujian server:

- a. Sistem berhasil membuat interface baru bernama wg0 dengan tipe WireGuard.
- b. Konfigurasi dimuat dari file konfigurasi sistem.
- c. IP Address 10.8.0.1/24 berhasil dipasang (assigned) pada interface wg0. Ini bertindak sebagai alamat gateway untuk jaringan VPN.
- d. MTU (Maximum Transmission Unit) diatur ke 1420 byte untuk mengakomodasi header enkripsi WireGuard tanpa menyebabkan fragmentasi paket yang berlebihan.

```
melah@melah-VMware-Virtual-Platform: ~$ sudo wg-quick up wg0
[sudo] password for melah:
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.8.0.2/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] wg set wg0 fwmark 51820
[#] ip -4 rule add not fwmark 51820 table 51820
[#] ip -4 rule add table main suppress_prefixlength 0
[#] ip -4 route add 0.0.0.0/0 dev wg0 table 51820
[#] sysctl -q net.ipv4.conf.all.src_valid_mark=1
[#] nft -f /dev/fd/63
```

Perintah: `sudo wg-quick up wg0`

Analisis pengujian client:

- a. Sama seperti server, client berhasil membuat interface wg0.

- b. IP Address 10.8.0.2/24 berhasil dipasang. Ini menunjukkan bahwa client telah memiliki identitas dalam jaringan privat VPN.
- c. Terlihat adanya penambahan aturan routing dan firewall (via nft dan ip rule), yang menandakan bahwa rute trafik jaringan telah dimodifikasi agar melewati tunnel VPN (termasuk fwmark 51820).

2. Verifikasi status WireGuard antar server dan client

```
servervmvm@servervm:~$ sudo wg
interface: wg0
  public key: Ddq9CxW/MtEQ/skoN3M7b793+st8LAIQY41jvwCfAg8=
  private key: (hidden)
  listening port: 51820

peer: ktwbFhRtJz2+eg+PjjSh/5Lbj3W0cAfHHgCs9+cvqG4=
  endpoint: 192.168.63.129:46637
  allowed ips: 10.8.0.2/32
  latest handshake: 23 seconds ago
  transfer: 180 B received, 92 B sent
servervmvm@servervm:~$ _
```

Perintah: sudo wg

Analisis pengujian server:

- a. Interface wg0: Server mendengarkan (listening) pada port UDP 51820.
- b. Peer Terdeteksi: Server berhasil mengenali peer (Client) dengan public key yang berawalan “ktwbFh...”.
- c. Endpoint: Terlihat alamat IP asli Client yaitu 192.168.63.129 yang terhubung ke port server.
- d. Latest Handshake: Status menunjukkan “23 seconds ago”. Ini adalah indikator utama keberhasilan. Jika handshake berhasil, berarti kunci kriptografi cocok dan koneksi aman telah aktif.
- e. Transfer: Terjadi pertukaran data (180 B diterima, 92 B dikirim), yang membuktikan jalur data terbuka.

```

melah@melah-VMware-Virtual-Platform:~$ sudo wg
interface: wg0
  public key: ktwbFhRtJz2+eg+PjjSh/5Lbj3W0cAfHHgCs9+cvqG4=
  private key: (hidden)
  listening port: 46637
  fwmark: 0xca6c

peer: Ddq9Cw/MtEQ/skoN3M7b793+st8LAIQY41jvwCfAg8=
  endpoint: 192.168.63.128:51820
  allowed ips: 0.0.0.0/0
  latest handshake: 7 seconds ago
  transfer: 92 B received, 180 B sent
  persistent keepalive: every 25 seconds
melah@melah-VMware-Virtual-Platform:~$

```

Perintah: sudo wg

Analisis pengujian client:

- a. Interface wg0: Client menggunakan port acak (46637) untuk koneksi keluar.
- b. Peer Terdeteksi: Client berhasil mengenali Server dengan public key berawalan “Ddq9Cx...”.
- c. Endpoint: Client terhubung ke IP asli Server 192.168.63.128 pada port 51820.
- d. Allowed IPs: Terkonfigurasi 0.0.0.0/0, yang artinya Client diset untuk melewatkan semua lalu lintas internetnya melalui VPN ini.
- e. Latest Handshake: Status “7 seconds ago” mengkonfirmasi koneksi aktif.
- f. Keepalive: Fitur persistent keepalive aktif setiap 25 detik untuk menjaga koneksi tetap hidup meski tidak ada lalu lintas data (penting untuk menembus NAT).

3. Pengujian ping antar IP VPN

```

servervmvm@servervm:~$ ping 10.8.0.2
PING 10.8.0.2 (10.8.0.2) 56(84) bytes of data:
64 bytes from 10.8.0.2: icmp_seq=1 ttl=64 time=3.81 ms
64 bytes from 10.8.0.2: icmp_seq=2 ttl=64 time=1.46 ms
64 bytes from 10.8.0.2: icmp_seq=3 ttl=64 time=1.19 ms
^C
--- 10.8.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.187/2.152/3.807/1.175 ms
servervmvm@servervm:~$ _

```

Perintah: ping 10.8.0.2 (IP VPN client)

Analisis pengujian server:

- a. Server berhasil mengirim 3 paket (packets transmitted: 3) ke IP VPN Client.
- b. Server berhasil menerima 3 balasan (3 received).
- c. Packet Loss: 0%.

- d. Waktu Respon (RTT): Rata-rata waktu respon sangat cepat, sekitar 1.187 ms hingga 3.807 ms, menunjukkan latensi yang rendah.

```
melah@melah-VMware-Virtual-Platform:~$ ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data:
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=1.56 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=1.46 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=1.43 ms
^C
--- 10.8.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.431/1.484/1.561/0.055 ms
melah@melah-VMware-Virtual-Platform:~$
```

Perintah: ping 10.8.0.1 (IP VPN server)

Analisis pengujian client:

- Client berhasil mengirim 3 paket ke IP VPN Server.
- Client berhasil menerima 3 balasan.
- Packet Loss: 0%.
- Waktu Respon (RTT): Waktu respon juga sangat rendah, rata-rata sekitar 1.431 ms hingga 1.561 ms.

4. Verifikasi IP routing pada client

```
melah@melah-VMware-Virtual-Platform:~$ ip route
default via 192.168.63.2 dev ens33 proto dhcp src 192.168.63.129 metric 100
10.8.0.0/24 dev wg0 proto kernel scope link src 10.8.0.2
192.168.63.0/24 dev ens33 proto kernel scope link src 192.168.63.129 metric 100
```

Perintah: ip route

Analisis pengujian:

- Rute default jaringan fisik:
 - Sistem masih mempertahankan rute default yang ada sebelum VPN diaktifkan, yaitu default via 192.168.63.2 dev ens33.
 - Ini mengarahkan semua lalu lintas yang tidak secara eksplisit dirutekan ke gateway fisik (192.168.63.2) melalui interface fisik (ens33). Rute ini digunakan untuk akses ke jaringan lokal (LAN) dan internet non-VPN (jika tidak ada full tunneling).
- Rute jaringan lokal fisik:

1. Terdapat rute untuk jaringan lokal fisik (192.168.63.0/24 dev ens33). Rute ini memastikan komunikasi dalam jaringan lokal tetap menggunakan ens33.

c. Rute kunci VPN (WireGuard):

1. Ini adalah bukti konfigurasi VPN yang berhasil: 10.8.0.0/24 dev wg0.
2. Baris ini secara eksplisit menginstruksikan sistem bahwa setiap paket yang ditujukan ke subnet VPN (10.8.0.0/24) harus dikirim melalui interface virtual wg0.
3. IP sumber (src) untuk paket-paket ini adalah alamat VPN Client itu sendiri (10.8.0.2).

5. Verifikasi alamat IP interface WireGuard

```
servervm@servervm:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e7:aa:58 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.63.128/24 metric 100 brd 192.168.63.255 scope global dynamic ens33
        valid_lft 1736sec preferred_lft 1736sec
    inet6 fe80::20c:29ff:fe7:aa58/64 scope link
        valid_lft forever preferred_lft forever
3: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 10.8.0.1/24 scope global wg0
        valid_lft forever preferred_lft forever
servervm@servervm:~$
```

Perintah: ip a

Analisis pengujian server:

- a. Ditemukan interface 3: wg0 dengan status <POINTOPOINT, NOARP, UP, LOWER_UP>. Status UP menunjukkan interface aktif.
- b. MTU (Maximum Transmission Unit) diatur ke 1420, yang merupakan nilai standar untuk WireGuard.
- c. Alamat IP VPN: Ditemukan baris inet 10.8.0.1/24 scope global wg0. Ini membuktikan bahwa Server berhasil memasang alamat 10.8.0.1 pada interface wg0.

```

melah@melah-VMware-Virtual-Platform:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:8b:cf:34 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.63.129/24 brd 192.168.63.255 scope global dynamic noprefixroute ens33
        valid_lft 1161sec preferred_lft 1161sec
    inet6 fe80::20c:29ff:fe8b:cf34/64 scope link
        valid_lft forever preferred_lft forever
3: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 10.8.0.2/24 scope global wg0
        valid_lft forever preferred_lft forever

```

Perintah: ip a

Analisis pengujian client:

- Ditemukan interface 3: wg0 dengan status <POINTOPOINT, NOARP, UP, LOWER_UP>, mengkonfirmasi interface aktif.
- Alamat IP VPN: Ditemukan baris inet 10.8.0.2/24 scope global wg0. Ini membuktikan bahwa Client berhasil memasang alamat 10.8.0.2 pada interface wg0.
- Alamat IP fisik (interface ens33) Client juga terlihat (inet 192.168.63.129/24).

6. Pengujian handshake berulang

```

Every 1.0s: sudo wg show                                server@: wed Dec 3 11:21:28 2025
interface: wg0
  public key: 0a9c0a1MEQ/sk4dH7b73+st8A1QV41jvCfAgB=
  private key: (hidden)
  listening port: 51820
peer: k1ub7R4z2+gpfJJShSLBj9M6cRfHg059+cvG4=
  endpoint: 10.8.0.129:4667
  allowed ips: 10.8.0.0/24
  latest handshake: 33 seconds ago
  transfer: 23.54 KiB received, 3.14 KiB sent

```

Perintah: watch -n 1 sudo wg show

Analisis pengujian server:

- Latest Handshake: Menunjukkan nilai “33 seconds ago”. Nilai yang terus diperbarui ini membuktikan bahwa tunnel antara Server dan Client masih aktif dan key exchange kriptografi berjalan lancar.
- Transfer Data: Terlihat statistik data 23.54 KiB received, 3.14 KiB sent. Angka ini mengkonfirmasi adanya pertukaran data yang berkelanjutan, biasanya dikarenakan persistent keepalive atau aktivitas latar belakang sistem.

```
melah@melah-VMware-Virtual-Platform: ~  
Every 1.0s: sudo wg show melah-VMware-Virtual-Platform: Wed Dec 3 18:22:39 2025  
  
interface: wg0  
  public key: ktwbFhRtJz2+eg+PjjSh/5Lbj3W0cAfHHgCs9+cvqG4=  
  private key: (hidden)  
  listening port: 46637  
  fwmark: 0xca6c  
  
peer: Ddq9CxW/MtEQ/skoN3M7b793+st8LAIQY41jvwCfAg8=  
  endpoint: 192.168.63.128:51820  
  allowed ips: 0.0.0.0/0  
  latest handshake: 1 minute, 44 seconds ago  
  transfer: 3.14 KiB received, 23.63 KiB sent  
  persistent keepalive: every 25 seconds
```

Perintah: `watch -n 1 sudo wg show`

Analisis pengujian client:

- a. Latest Handshake: Menunjukkan “1 minute, 44 seconds ago”. Meskipun berbeda dengan server karena pengecekan dilakukan pada waktu yang berbeda, nilai ini berada dalam rentang waktu keepalive 25 detik yang dikonfigurasi, memastikan bahwa koneksi tidak terputus (timed out).
- b. Transfer Data: Statistik transfer menunjukkan 3.14 KiB received, 23.63 KiB sent. Angka konsisten dengan data yang dikirim dan diterima oleh Server, menunjukkan bahwa transfer data melalui tunnel berjalan dua arah dengan baik.

7. Pengujian akses jarak jauh (*remote access*) melalui SSH

```
melah@melah-VMware-Virtual-Platform:~$ ssh servervm@10.8.0.1  
The authenticity of host '10.8.0.1 (10.8.0.1)' can't be established.  
ED25519 key fingerprint is SHA256:ipF3S0838AsQ6QBcp8t9uj6FuWimZBe6RfGUSbUpZag.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.8.0.1' (ED25519) to the list of known hosts.  
servervm@10.8.0.1's 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 Wed Dec 3 12:39:17 PM UTC 2025  
  
System load:  0.0          Processes:      229  
Usage of /:   50.4% of 9.75GB  Users logged in: 1  
Memory usage: 15%          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  
  
Last login: Wed Dec 3 12:34:13 2025 from 192.168.63.1  
servervm@servervm:~$
```

Perintah: `ssh servervmvm@10.8.0.1`

Analisis pengujian:

- a. Koneksi Dibuat: Perintah ini berhasil menemukan dan terhubung ke alamat IP VPN Server (10.8.0.1).
- b. Verifikasi Kunci: Sistem memberikan peringatan authenticity of host (standard pada koneksi SSH pertama), yang kemudian diterima oleh pengguna (yes).
- c. Akses Berhasil: Setelah memasukkan password, Client berhasil mendapatkan akses shell ke Server. Hal ini dibuktikan dengan perubahan prompt terminal menjadi `servervmvm@servervm:~$` (sama seperti terminal Server).
- d. Verifikasi IP Sumber: Informasi last login menunjukkan bahwa koneksi masuk berasal dari 192.168.63.1, namun yang paling penting, koneksi SSH itu sendiri berjalan di atas alamat VPN (10.8.0.1).

Hasil:

1. Interface WireGuard (wg0) pada server dan client berhasil dijalankan tanpa error.
2. Proses handshake antara server dan client berhasil dilakukan, ditunjukkan oleh status "latest handshake" pada perintah `sudo wg`.
3. Pengujian ping menunjukkan bahwa kedua mesin dapat berkomunikasi melalui alamat IP VPN (10.8.0.1 dan 10.8.0.2).
4. Koneksi titik-ke-titik telah berhasil divalidasi dan siap digunakan untuk tahap selanjutnya, yaitu Wireshark capture pada minggu ke-5.