



Analisis dan Implementasi VPN pada VPS untuk Peningkatan Aksesibilitas Jaringan di Lingkungan Perguruan Tinggi

Ubaidi¹✉, Nindian Puspa Dewi²

^{1,2}Informatika, Universitas Madura

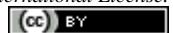
ubed@unira.ac.id

Abstrak

Perguruan Tinggi merupakan institusi pendidikan dengan lingkungan jaringan yang kompleks dan luas. Mahasiswa, dosen, dan tenaga kependidikan memerlukan akses yang aman dan terpercaya ke berbagai sumber daya dan layanan di jaringan kampus, termasuk akses ke data mahasiswa, penelitian, perpustakaan digital, dan sistem administratif. Karena itulah diperlukan infrastruktur yang aman dengan biaya yang efisien. Implementasi VPN (Virtual Private Network) merupakan salah satu teknologi yang dapat memberikan akses jaringan yang aman, mudah dan memiliki kecepatan transfer yang baik bagi para pengguna. VPN memungkinkan pengguna untuk mengenkripsi lalu lintas data mereka saat terhubung ke jaringan kampus, sehingga menjaga keamanan dan kerahasiaan informasi. Selain itu untuk efisiensi infrastruktur dapat dilakukan dengan implementasi VPS yang memungkinkan perguruan tinggi untuk menyediakan lingkungan server terisolasi yang dapat digunakan untuk berbagai tujuan dengan tetap menghemat biaya dan sumber daya, serta meningkatkan skalabilitas infrastruktur mereka.

Kata kunci: VPN, VPS, Aksesibilitas Jaringan, Perguruan Tinggi.

JIDT is licensed under a Creative Commons 4.0 International License.



1. Pendahuluan

Dalam era digital yang terus berkembang, terdapat tantangan dalam menyediakan akses jaringan yang aman dan handal bagi seluruh anggota perguruan tinggi, terutama ketika mereka berada di luar kampus atau mengakses jaringan dari lokasi yang berbeda. Ancaman keamanan seperti serangan siber, peretasan, dan pemantauan tak berwenang dapat mengancam integritas dan kerahasiaan data [1][2].

Sebagai solusi, implementasi VPN (Virtual Private Network) dapat memberikan akses jaringan yang aman bagi para pengguna, baik yang berada di dalam kampus maupun di luar kampus. VPN memungkinkan pengguna untuk mengenkripsi lalu lintas data mereka saat terhubung ke jaringan kampus, sehingga menjaga keamanan dan kerahasiaan informasi [3][4][5].

Di sisi lain, kebutuhan untuk menyediakan infrastruktur komputasi yang efisien dan fleksibel semakin mendesak di perguruan tinggi. Implementasi VPS (Virtual Private Server) dapat menjadi solusi untuk menghadapi tantangan ini[6]. VPS memungkinkan perguruan tinggi untuk menyediakan lingkungan server terisolasi yang dapat digunakan untuk berbagai tujuan, seperti pengembangan aplikasi, pengujian, penyimpanan data penelitian, dan layanan lainnya [7]. Dengan VPS, perguruan tinggi dapat menghemat biaya dan sumber daya, serta meningkatkan skalabilitas infrastruktur mereka[6].

Namun, meskipun potensi manfaat dari implementasi VPN dan VPS sangat menjanjikan, masih terdapat beberapa pertanyaan yang perlu dijawab dan tantangan yang harus diatasi dalam menerapkan teknologi ini di lingkungan perguruan tinggi[8]. Selain itu, bagaimana menghadapi kemungkinan penggunaan yang berlebihan pada infrastruktur VPS dan bagaimana memastikan infrastruktur tersebut selalu berjalan optimal. Dalam konteks ini, penelitian akan dilakukan di salah satu perguruan tinggi di Sumenep Madura. Hasil penelitian ini diharapkan dapat memberikan panduan praktis dan wawasan mendalam bagi perguruan tinggi dalam mengoptimalkan layanan jaringan dan infrastruktur komputasi mereka, sehingga dapat meningkatkan keamanan, mobilitas pengguna, dan efisiensi operasional.

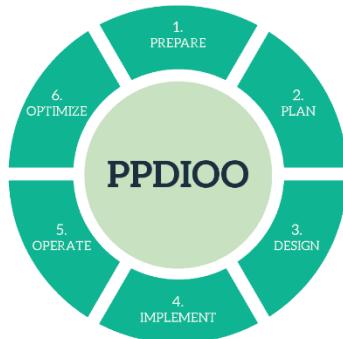
Penggunaan VPN (Virtual Private Network) dan VPS (Virtual Private Server) dalam konteks perguruan tinggi telah menjadi topik penelitian yang menarik dalam beberapa tahun terakhir. Berikut adalah beberapa state-of-the-art penelitian yang relevan dengan implementasi VPN dan VPS server di perguruan tinggi:

1. "Implementasi Virtual Private Network (VPN) Di Perpustakaan Universitas Islam Malang" oleh Lia Umaroh, Machsun Rifauddin (2020): Penelitian ini mengusulkan solusi VPN yang aman dan skalabel untuk perguruan tinggi. Penelitian ini menekankan pentingnya keamanan data mahasiswa dan penelitian, serta memberikan penekanan pada keandalan dan skalabilitas solusi VPN yang diimplementasikan [9].

2. "Analisa dan Implementasi VPN Dinamis Menggunakan Hamachi Pada PT. Jajindo Metal Industries" oleh Ahmad Surya Rifandy, Salman Topiq. (2017): Penelitian ini fokus pada pembangunan jaringan komputer berbasis VPN dinamis untuk mempermudah melakukan kegiatan operasional antar kantor cabang dan kantor pusat, seperti melakukan transaksi data atau presentasi melalui jalur publik, salah satunya penggunaan bersama aplikasi bisnis Microsoft Dynamic Axapta 4.0 pada semua cabang yang dioperasikan melalui domain pada kantor pusat[3].
3. "Implementasi VPN Pada VPS Server Menggunakan OpenVPN dan Raspberry Pi " oleh Taufik Rahman, Giovanni Maria Vianney Tobia Mariatmojo, Hafis Nurdin, Herman Kuswanto (2022): Penelitian ini mengeksplorasi penggunaan teknologi VPN dalam meningkatkan pembelajaran bergerak (mobile learning) di perguruan tinggi. Penelitian ini mengidentifikasi manfaat penggunaan VPN dalam memberikan akses yang aman dan terenkripsi ke sumber daya pendidikan dari perangkat seluler di luar kampus[10].
4. "Implementasi Virtual Private Network (VPN) Menggunakan Openvpn Dan Easy-Rsa Pada Sistem Operasi Linux Debian" oleh Rizky Adityan Hidayat, Juli Yanto (2021): Hasil penelitian ini adalah implementasi VPN dengan OpenVPN dan Easy-Rsa pada Sistem Operasi Linux Debian. Simpulan dari penelitian ini setelah mengimplementasikan VPN dengan Sistem Operasi Linux Debian menggunakan OpenVPN dan Easy-RSA diharapkan dapat memudahkan tugas dan pekerjaan staf kantor dari segi waktu, tempat dan biaya[11].

2. Metode Penelitian

Penelitian ini menerapkan metode perancangan PPDIOO yang terdiri dari 6 tahapan yaitu prepare, plan, design, implement, operate dan optimize [12]. Metode ini biasa digunakan dalam melakukan perancangan jaringan. Adapun proses tahapan yang dilakukan dalam penelitian yaitu ditunjukkan pada Gambar 1 berikut:

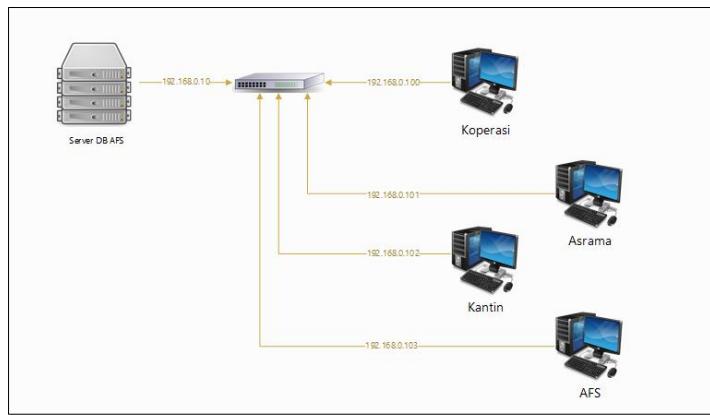


Gambar 1. Tahapan PPDIOO

1. Prepare (Persiapan)

Tahap ini merupakan tahap awal/persiapan. Pada tahapan ini dilakukan identifikasi kebutuhan dan arsitektur jaringan sesuai dengan kondisi jaringan dan kemampuan perguruan tinggi. Identifikasi dilakukan dengan melakukan observasi dan wawancara secara langsung ke pimpinan perguruan tinggi.

Observasi dilakukan untuk mengetahui konfigurasi jaringan saat ini seperti jumlah pengguna, ada tidaknya pembagian data dan arsitektur jaringan. Dari hasil observasi diperoleh jika jaringan menggunakan jaringan dari developer indihome yang dibagi menjadi jaringan kabel untuk kantor dan jaringan wifi. Adapun jumlah server yang dimiliki sejumlah 2 dan lebih dari 50 komputer serta laptop/hp civitas akademika yang memanfaatkan jaringan ini yaitu kira-kira berjumlah 103. Secara umum Gambar 2 berikut menunjukkan topologi jaringan sebelum dipasang VPN dan menggunakan VPS:



Gambar 2. Topologi Jaringan sebelum ada VPS

Identifikasi masalah dan kebutuhan juga dilakukan dengan melakukan wawancara dengan pengelola jaringan dan beberapa dosen dan mahasiswa sebagai pengguna langsung jaringan. Menurut pihak pengelola, server kampus harus selalu menyala selama 24 jam agar civitas akademika bisa mengakses sistem informasi kampus setiap saat dimana saja. Sehingga tidak menutup kemungkinan akan terjadi error atau kesalahan sistem yang membutuhkan akses perbaikan ke server. Permasalahan yang terjadi saat ini, monitoring server masih tidak bisa dilakukan di luar kampus, dengan alasan keamanan dan teknologi yang masih belum mumpuni. Hal ini mengakibatkan terbatasnya monitoring dan perbaikan server saat terjadi error di luar jam kerja.

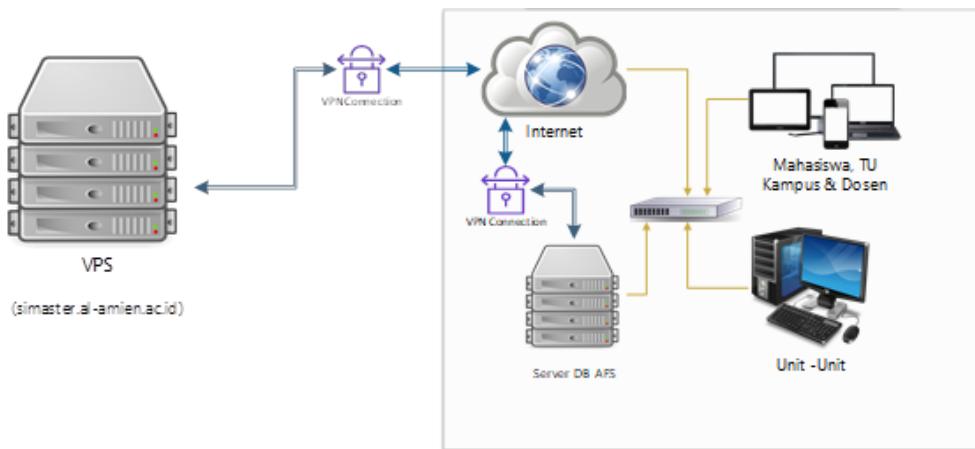
Pada jaringan di area asrama sudah terintegrasi dengan aplikasi pembayaran internal yang hanya bisa diakses local seperti di kantin, koperasi dan kafe di area kampus. Mahasiswa untuk melakukan transaksi hanya bisa non tunai berdasarkan kebijakan yang sudah berjalan selama 3 tahun, karena data transaksi hanya ada di local, jadi aplikasi simaster yang merupakan aplikasi akademik terpadu untuk mahasiswa tidak bisa menyajikan data transaksi keuangan yang dilakukan di area asrama.

2. Plan (Perencanaan)

Setelah melakukan identifikasi pada tahap persiapan, langkah selanjutnya adalah membuat konsep jaringan sesuai dengan kebutuhan perguruan tinggi. Pada tahapan ini ditentukan pula kebutuhan hardware dan software yang akan digunakan. Untuk mengatasi permasalahan tersebut maka akan digunakan VPN yang diimplementasikan pada VPS. Dalam penelitian ini, jenis VPN yang digunakan adalah WireGuard dan VPS Debian.

3. Design (Desain)

Pada tahap ini desain rencana jaringan diperjelas dengan membuat topologi jaringan, spesifikasi dan konfigurasinya. Gambar 3 berikut adalah output dari tahapan ini berupa gambaran dari topologi jaringan dan konfigurasinya yang akan dibuat sehingga mempermudah proses implementasi [9][13][14].



Gambar 3. Topologi Jaringan sesudah ada VPS

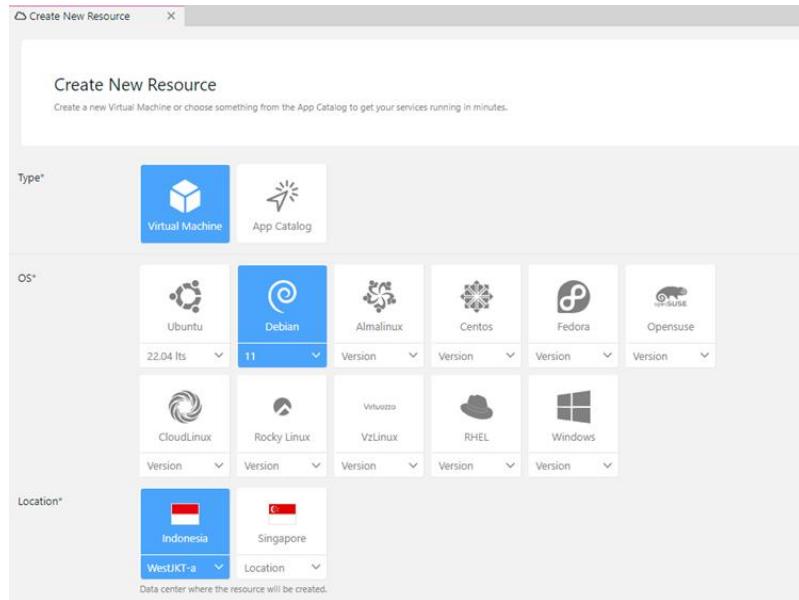
4. Implement (Implementasi)

Setelah rancangan dibuat maka langkah selanjutnya adalah instalasi dan konfigurasi jaringan sesuai dengan apa yang telah didesain dengan memperhatikan kebutuhan dan kondisi perguruan tinggi. Pada tahapan ini juga akan dilakukan ujicoba sistem.

Berikut beberapa tahapan yang akan dilakukan pada bagian implementasi [15][16] yaitu:

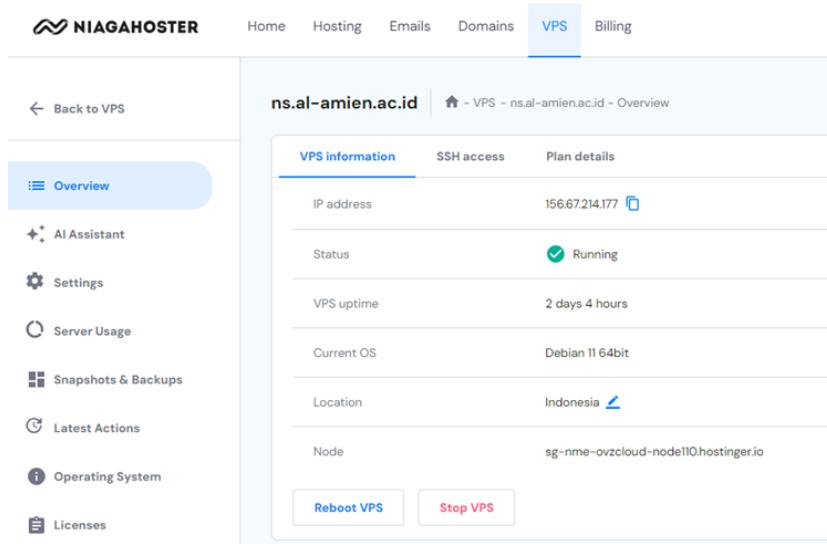
1. Instalasi sistem operasi yang mendukung VPN di VPS.

Proses instalasi ini dilakukan pada akun niagahoster dan membuat resource baru untuk sistem operasi VPS, pada tahap ini sistem operasi yang dipilih adalah Debian 11 dan lokasi server ada di Indonesia, agar akses VPS lebih cepat dari pada memilih lokasi selain Indonesia, Gambar 4 berikut ini merupakan proses pemilihan sistem operasi dan hasil instalasinya.



Gambar 4. Pembuatan resource system operasi debian

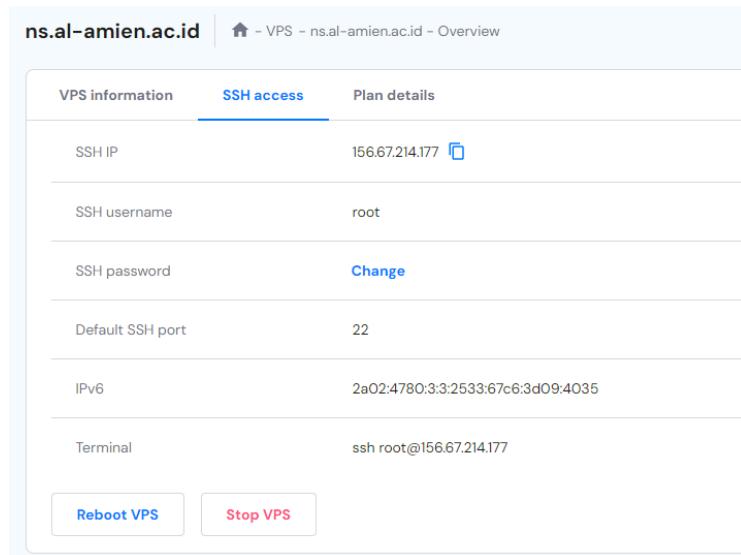
Sesudah sistem operasi terinstall, maka akan ada menu detail sistem operasi yang sudah terinstall di VPS, pada menu ini juga ada akses remote terminal[17], akan proses konfigurasi server bisa diremote dengan aplikasi terminal yang ditunjukkan pada Gambar 5 berikut.



Gambar 5. Sistem Operasi Debian 11 pada VPS

2. Instalasi dan Konfigurasi VPN di VPS

Proses instalasi wireguard dilakukan dengan aplikasi terminal yang menggunakan protocol SSH[18]. Gambar 6 berikut menunjukkan SSH pada VPS



Gambar 6. SSH access pada VPS

Proses instalasi wireguard bisa dilakukan dengan perintah sebagai berikut :

Update OS

sudo apt update

Install Wireguard

sudo apt install wireguard

Konfigurasi WireGuard

Buat kunci privat dan publik untuk server Anda dengan perintah berikut:

wg genkey | sudo tee /etc/wireguard/privatekey | wg pubkey | sudo tee /etc/wireguard/publickey

Buat file konfigurasi server WireGuard, misalnya /etc/wireguard/wg0.conf, dan tambahkan konfigurasi berikut sebagai contoh:

[Interface]

Address = 10.10.0.1/24

PrivateKey = <Server Private Key>

ListenPort = 51820

[Peer]

PublicKey = <Kunci Publik Klien>

AllowedIPs = 10.10.0.2/32

Jika konfigurasi sudah dilakukan, tahap berikutnya adalah menjadikan konfigurasi yang buat sebagai service pada sistem operasi dengan perintah sebagai berikut

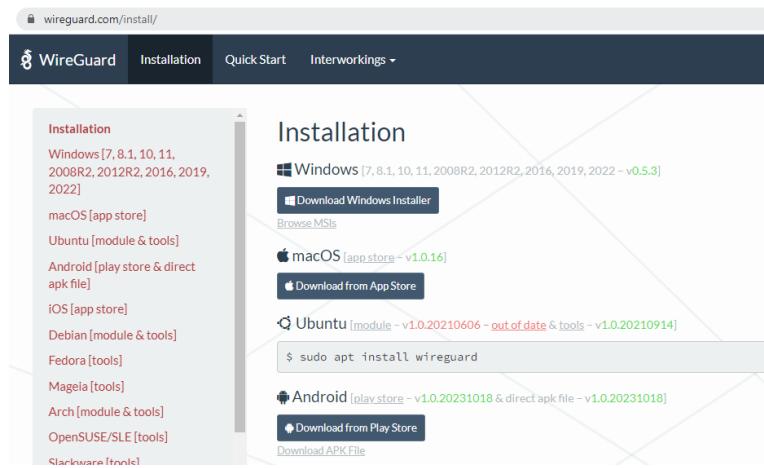
sudo wg-quick up wg0

sudo systemctl enable wg-quick@wg0

sudo systemctl start wg-quick@wg0

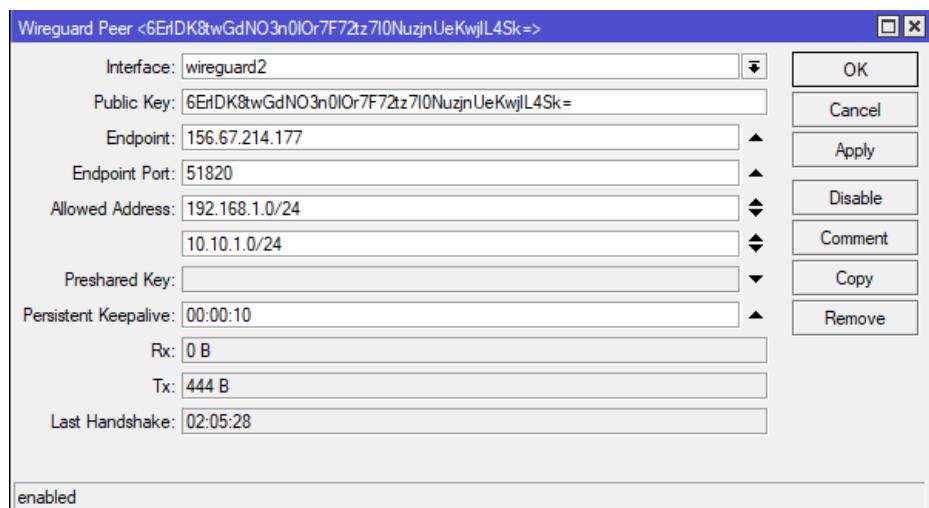
3. Konfigurasi VPN Wireguard pada sisi client.

Wireguard client compatible dengan berbagai platform sistem operasi, sehingga bisa diterapkan pada banyak sistem operasi dan bisa didownload pada situs resmi wireguard seperti ditunjukkan pada Gambar 7.



Gambar 7. Wireguard tools

Agar koneksi jaringan local dan VPS bisa terkoneksi, wireguard tools yang digunakan langsung pada aplikasi mikrotik yang dijadikan router pada jaringan internet dikampus, dengan konfigurasi yang ditunjukkan pada Gambar 8.



Gambar 8. Wireguard tools pada mikrotik

A screenshot of a PuTTY terminal window. The session title is '156.67.214.177 - PuTTY'. The terminal shows a root login with the password 'root'. It then displays the Debian Linux welcome message. The user runs the 'wg' command, which outputs the configuration for a 'wg0' interface and a 'peer' entry. The 'wg0' interface has a public key and a listening port of 51820. The 'peer' entry shows a connection to an IP of 180.247.138.68 with a port of 50002, and various statistics for data transfer and handshake times.

Gambar 9. Wireguard tools pada Debian

5. Operate (Operasi)

Pada tahapan ini, jaringan sudah siap digunakan dengan tetap melakukan pengelolaan, perbaikan, pemantauan dan pemeliharaan kinerja jaringan. Pengelolaan dan pemeliharaan sistem jaringan yang ditelah diimplementasikan.

6. Optimize (Optimasi)

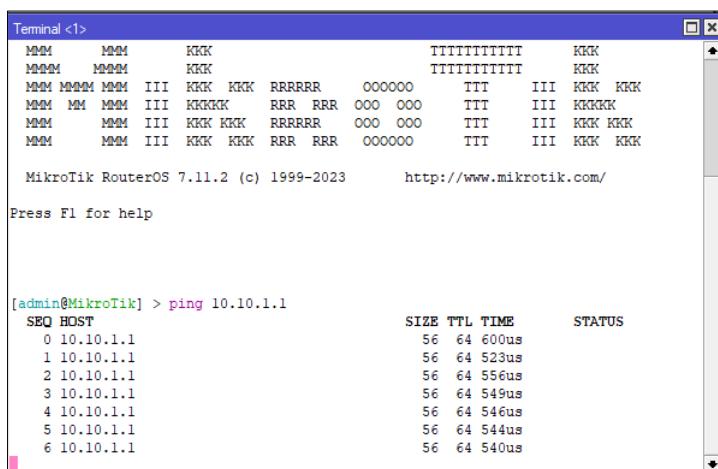
Tahapan ini dilakukan jika ternyata ada banyak masalah dalam jaringan yang menuntut adanya perubahan konfigurasi jaringan. Jika terlalu banyak permasalahan yang timbul maka tidak memungkinkan akan kembali ke tahapan awal.

3. Hasil dan Pembahasan

Setelah implementasi selesai, maka selanjutnya akan dilakukan pengujian untuk mengetahuan kinerja dari jaringan VPN yang telah dibangun sebelum dan setelah menggunakan VPN. Ada beberapa bentuk pengujian yang dilakukan yaitu :

1. Ujicoba koneksi dari client Mikrotik ke VPS

Setelah dilakukan konfigurasi koneksi client mikrotik ke VPS Wireguard server, maka dilakukan uji ping koneksi ke ip server VPN sesuai dengan ip yang didaftarkan di wireguard server 10.10.0.1/32 dan ip peer/client yang dimikrotik didaftarkan dengan ip 10.10.0.2/32 yang hasil ping disajikan pada Gambar 10.



Terminal <1>

```
MM M M KKK TTTTTTTTTT KKK
MM M M KKK TTTTTTTTTT KKK
MM M M M III KKK KKK RRRRRR 000000 TTT III KKK KKK
MM M M III KKKK KKK RRR RRR 000 000 TTT III KKKKKK
MM M M III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MM M M III KKK KKK RRR RRR 000000 TTT III KKK KKK

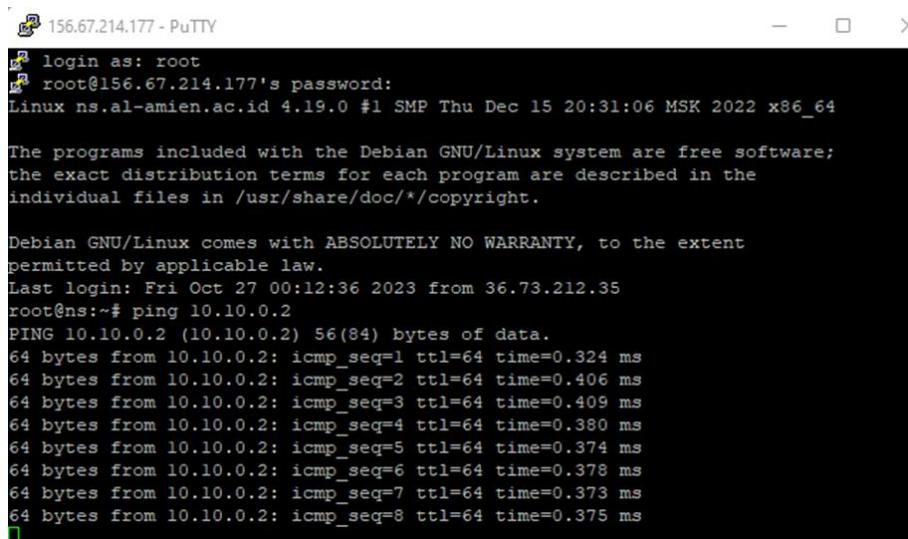
MikroTik RouterOS 7.11.2 (c) 1999-2023 http://www.mikrotik.com/
Press F1 for help

[admin@MikroTik] > ping 10.10.1.1
SEQ HOST SIZE TTL TIME STATUS
0 10.10.1.1 56 64 600us
1 10.10.1.1 56 64 523us
2 10.10.1.1 56 64 556us
3 10.10.1.1 56 64 549us
4 10.10.1.1 56 64 546us
5 10.10.1.1 56 64 544us
6 10.10.1.1 56 64 540us
```

Gambar 10. Ujicoba koneksi dari Mikrotik ke VPS

2. Ujicoba VPS ke client Mikrotik

Berdasarkan konfigurasi VPN pada VPS, peer client mikrotik didaftarkan dengan ip 10.10.0.2/32 dan ip server 10.10.0.1/32 dimana hasil konfigurasi dan ujicoba disajikan pada Gambar 11.



```
156.67.214.177 - PuTTY
login as: root
root@156.67.214.177's password:
Linux ns.al-amien.ac.id 4.19.0 #1 SMP Thu Dec 15 20:31:06 MSK 2022 x86_64

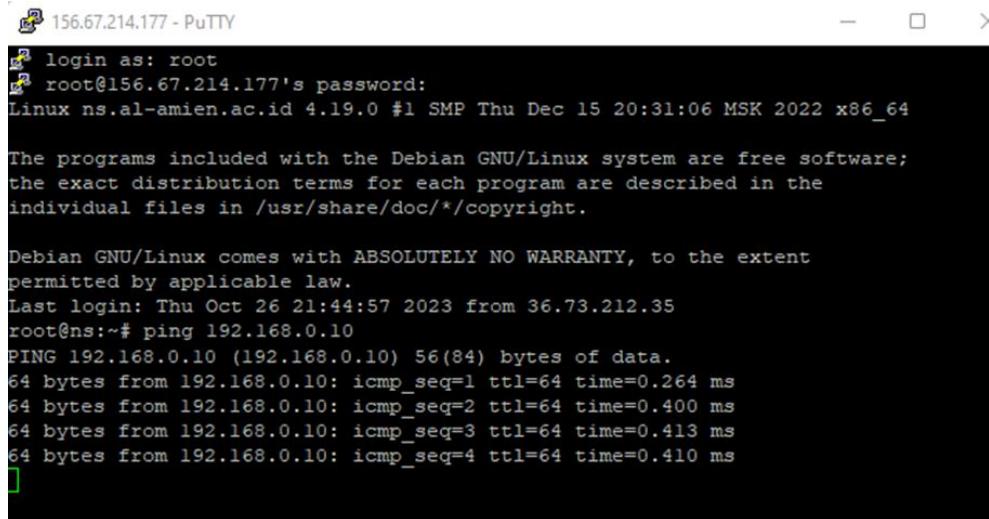
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Oct 27 00:12:36 2023 from 36.73.212.35
root@ns:~# ping 10.10.0.2
PING 10.10.0.2 (10.10.0.2) 56(84) bytes of data.
64 bytes from 10.10.0.2: icmp_seq=1 ttl=64 time=0.324 ms
64 bytes from 10.10.0.2: icmp_seq=2 ttl=64 time=0.406 ms
64 bytes from 10.10.0.2: icmp_seq=3 ttl=64 time=0.409 ms
64 bytes from 10.10.0.2: icmp_seq=4 ttl=64 time=0.380 ms
64 bytes from 10.10.0.2: icmp_seq=5 ttl=64 time=0.374 ms
64 bytes from 10.10.0.2: icmp_seq=6 ttl=64 time=0.378 ms
64 bytes from 10.10.0.2: icmp_seq=7 ttl=64 time=0.373 ms
64 bytes from 10.10.0.2: icmp_seq=8 ttl=64 time=0.375 ms
```

Gambar 11. Ujicoba VPS ke Mikrotik

3. Ujicoba VPS ke Ip database

Sesudah koneksi VPS ke mikrotik berhasil, maka dilakukan proses routing di server VPS agar jalur dengan ip 192.168.0.10/24 bisa diarahkan ke jalur interface VPN, sehingga VPS bisa terkoneksi dengan server database yang berada di jaringan lokal. Gambar 12 menunjukkan hasil routing di server VPS.



```
156.67.214.177 - PuTTY
login as: root
root@156.67.214.177's password:
Linux ns.al-amien.ac.id 4.19.0 #1 SMP Thu Dec 15 20:31:06 MSK 2022 x86_64

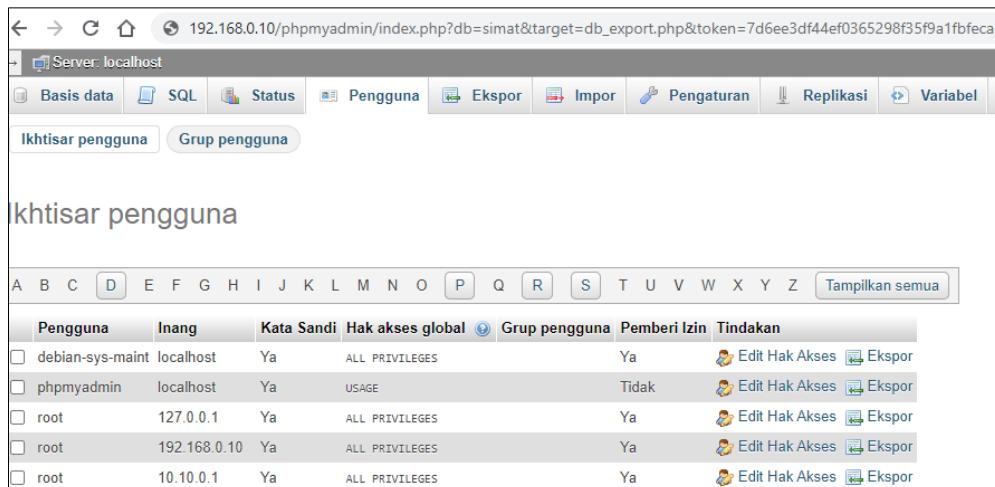
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct 26 21:44:57 2023 from 36.73.212.35
root@ns:~# ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=64 time=0.264 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=64 time=0.400 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=64 time=0.413 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=64 time=0.410 ms
```

Gambar 12. Ujicoba VPS ke ip database

4. Ujicoba login VPS ke ip mysql database server

Jika koneksi VPS ke database berhasil, untuk bisa melakukan remote ke database mysql, harus dibuatkan akses user di mysql agar bisa di remote oleh server VPS dimana ipnya adalah 10.10.0.1/32 seperti pada Gambar 13.



Pengguna	Inang	Kata Sandi	Hak akses global	Grup pengguna	Pemberi Izin	Tindakan
debian-sys-maint	localhost	Ya	ALL PRIVILEGES		Ya	Edit Hak Akses Ekspor
phpmyadmin	localhost	Ya	USAGE		Tidak	Edit Hak Akses Ekspor
root	127.0.0.1	Ya	ALL PRIVILEGES		Ya	Edit Hak Akses Ekspor
root	192.168.0.10	Ya	ALL PRIVILEGES		Ya	Edit Hak Akses Ekspor
root	10.10.0.1	Ya	ALL PRIVILEGES		Ya	Edit Hak Akses Ekspor

Gambar 13. Data user Mysql

Sesudah remote ip user mysql buatkan dengan sumber ip 10.10.0.1, maka VPS bisa langsung melakukan koneksi ke database dengan 192.168.0.10 sesuai dengan Gambar 14.



```
156.67.214.177 - PuTTY
root@ns:~# mysql -uroot -h 192.168.0.10 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1528397
Server version: 10.3.31-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
ERROR 1064 (42000): You have an error in your SQL syntax: check the manual that
corresponds to your MariaDB server version for the right syntax to use near 'sho
w databases' at line 1
MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| idiah         |
| idiah-pasca  |
| idiah20       |
| idiah21       |
| information_schema |
| mysql          |
| performance_schema |
| phpmyadmin    |
+-----+
8 rows in set (0.000 sec)

MariaDB [(none)]> use idiah
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [idiah]> 
```

Gambar 14. Remote mysql di terminal VPS

4. Kesimpulan

Implementasi VPN pada VPS adalah solusi yang efektif untuk meningkatkan keamanan dan aksesibilitas jaringan dalam berbagai konteks, termasuk di lingkungan Pendidikan. Selain lebih meningkatkan keamanan juga dapat meningkatkan aksesibilitas jaringan, dengan manfaat yang signifikan dalam perlindungan data, dukungan kerja jarak jauh, dan Fleksibilitas. Dengan begitu pengguna bisa mengakses dimana saja dan kapan saja dengan aman.

Daftar Rujukan

- [1] S. Dewi, "Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertarahastra Ciamis," *EVOLUSI : Jurnal Sains dan Manajemen*, vol. 8, no. 1, 2020, <https://doi.org/10.31294/evolusi.v8i1.7658>
- [2] S. M. Pedapudi, N. Vadlamani, "Comprehensive Network Security Management in Virtual Private Network Environment," *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, IEEE, <https://doi.org/10.1109/icaaic53929.2022.9793196>
- [3] A.S. Rifandy, S. Topiq, "Analisa dan Implementasi VPN Dinamis Menggunakan Hamachi Pada PT. Jajido Metal Industries," *Jurnal Nasional Komputasi dan Teknologi Informasi*. 2023;6(2):178-186
- [4] I. K. S. Satwika, "ANALISIS QUALITY OF SERVICE JARINGAN VIRTUAL PRIVATE NETWORK (VPN) DI STMIK STIKOM INDONESIA," *JURNAL ILMIAH INFORMATIKA*, vol. 7 no. 1, 2019, <https://doi.org/10.33884/jif.v7i01.1016>
- [5] S. Dewi, S. Sulistiayah, "Analisa Virtual Private Network (VPN) IP Multi Protocol Label Switching (MPLS) Untuk Jaringan Wide Area Network (WAN)", *Journal of Information System, Applied, Management, Accounting and Research*, Vol. 6, No. 1, 2022, <https://doi.org/10.52362/jisamar.v6i1.662>
- [6] D. Irwan, I. Supian, "Private Cloud Storage Pada Virtual Server Menggunakan IP Public Dinamis," *JREC (Journal of Electrical and Electronics)*, Vol. 8, No. 2, 2020, <https://doi.org/10.33558/jrec.v8i2.2341>
- [7] K. S. Mahedy, "IMPLEMENTASI SISTEM BACKUP DATA PADA SISTEM INFORMASI PERPUSTAKAAN UNIVERSITAS PENDIDIKAN GANESHA," *Jurnal Pendidikan Teknologi dan Kejuruan*, Vol. 18, No.2, 2021, <https://doi.org/10.23887/jptk-undiksha.v18i2.35597>
- [8] B. Shi, "Computer Network Information Security Protection Based on Virtual Private Network," *Journal of Physics: Conference Series*, Vol. 1646, No.1, 2020, <https://doi.org/10.1088/1742-6596/1646/1/012121>
- [9] L. Umaroh, M. Rifauddin, "Implementasi Virtual Private Network (VPN) Di Perpustakaan Universitas Islam Malang," *BACA: Jurnal Dokumentasi dan Informasi*, Vol.41, No.2, 2020, <https://doi.org/10.14203/j.baca.v41i2.531>

- [10] T. Rahman, G.M. Vianney, T. Mariatmojo, H. Nurdin, H. Kuswanto, “Implementasi VPN Pada VPS Server Menggunakan OpenVPN dan Raspberry Pi,” *TEKNIKA*, Vol. 11, No.2, 2022, DOI: 10.34148/teknika.v11i2.482
- [11] R. A. Hidayat, J. Yanto, “Implementasi Virtual Private Network (VPN) Menggunakan Openvpn Dan Easy-Rsa Pada Sistem Operasi Linux Debian,” *Jurnal Maklumatika*, Vol. 7, No.2, 2021
- [12] G. Ardhyogi, B. Soewito, “INFRASTRUCTURE SHARING PLANNING IN DEF INDUSTRIAL AREA USING PPDIOO FRAMEWORK”, *Journal of Theoretical and Applied Information Technology*, Vol.100, No.13, 2022
- [13] E. D. C. Bitbit, M. A. B. Gampoy, T. S. Ricafort, R. D. Tinio, R. L. Pula, R. F. Leona, & C. N. P. Olipas, “Crafting a Network Plan for a Microfinance Establishment and Its Branch Network through Virtual Private Network (VPN) Implementation,” *European Journal of Theoretical and Applied Sciences*, Vol. 1, No. 3, 2023, [https://doi.org/10.59324/ejtas.2023.1\(3\).43](https://doi.org/10.59324/ejtas.2023.1(3).43)
- [14] S. Sudiana, K. Kusrini & A. Sunyoto. “DESAIN SISTEM MANAJEMEN SERVER DATABASE SECARA REMOTE CONTROL BERBASIS VPN (VIRTUAL PRIVATE NETWORK),” *KURVATEK*, Vol. 3, No. 1, 2018, <https://doi.org/10.33579/krvtk.v3i1.752>
- [15] T. G. S. Putra, I. R. Widiasari, “Rancangan Virtual Private Server Pada Kantor Kelurahan Menggunakan ZeroTier,” *Building of Informatics, Technology and Science (BITS)*, Vol. 4, No. 2, 2022, <https://doi.org/10.47065/bits.v4i2.1810>
- [16] J. Westfall, “Set Up and Manage Your Virtual Private Server,” *Apress*, <https://doi.org/10.1007/978-1-4842-6966-4>
- [17] R. C. S. Hariyono and M. Mahmudin, “PENGGUNAAN IP PUBLIK VIRTUAL PRIVATE SERVER (VPS) UNTUK AKSES SERVER LOKAL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) TUNNEL: ”, *ijir*, Vol. 3, No. 1, 2022.
- [18] A. Maulidi, M. Abdullah, D. W. Handani, “Virtual private network (VPN) model for AIS real time monitoring,” *IOP Conference Series: Earth and Environmental Science*, Vol. 1081, No. 1, 2022, <https://doi.org/10.1088/1755-1315/1081/1/012028>