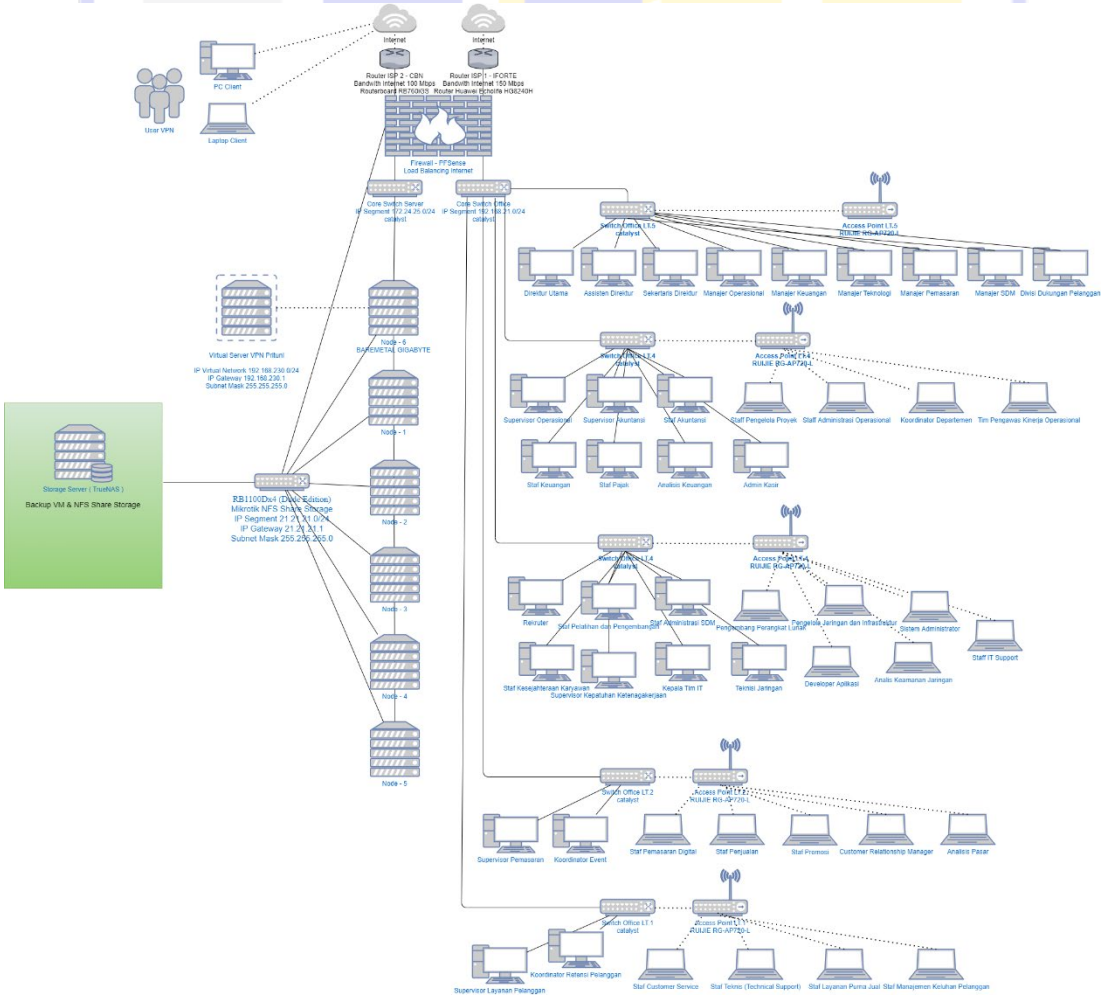
BAB IV

RANCANGAN JARINGAN USULAN

4.1. Jaringan Usulan

Pada bab ini akan dibahas mengenai rancangan jaringan usulan yang akan diterapkan di PT. Micro Piranti Computer. Rancangan jaringan ini dibuat berdasarkan hasil analisis jaringan yang telah dilakukan pada bab sebelumnya. Implementasi jaringan usulan bertujuan untuk meningkatkan keamanan dan efisiensi akses terhadap sumber daya perusahaan melalui VPN berbasis *Pritunl* pada sistem operasi *RedHat*.

4.1.1. Topologi Jaringan



Sumber : Hasil Penelitian

Gambar IV. 1. Topologi Usulan

Gambar IV. 1. menampilkan topologi jaringan usulan yang digunakan dalam implementasi VPN berbasis Pritunl. Topologi ini menghubungkan server VPN dengan perangkat pengguna melalui jaringan internet. Server VPN berfungsi sebagai gateway yang mengatur lalu lintas data dan memastikan bahwa hanya pengguna yang memiliki autentikasi yang valid yang dapat mengakses jaringan internal perusahaan. Dengan struktur ini, keamanan data dapat ditingkatkan, serta akses jaringan menjadi lebih terkontrol.

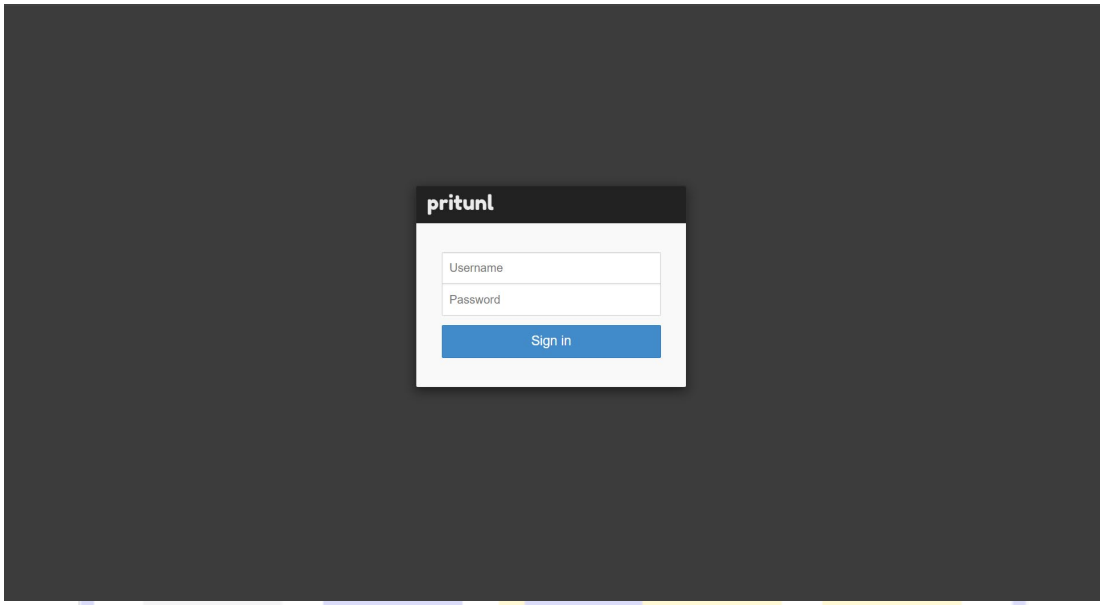
4.1.2. Skema Jaringan

Skema jaringan usulan menggambarkan bagaimana setiap perangkat dalam jaringan saling terhubung dan berkomunikasi. Server VPN Pritunl ditempatkan dalam jaringan internal perusahaan dan dikonfigurasi untuk menerima koneksi dari pengguna eksternal yang memerlukan akses aman. *Router* dan *firewall* berfungsi sebagai pengatur lalu lintas data yang keluar dan masuk, memastikan bahwa hanya lalu lintas yang aman yang diperbolehkan. Selain itu, penggunaan enkripsi data akan diterapkan untuk melindungi informasi yang dikirim melalui VPN.

4.1.3. Keamanan Jaringan

Keamanan jaringan dalam sistem ini difokuskan pada beberapa aspek utama, seperti *firewall*, enkripsi data, dan autentikasi pengguna. *Firewall* dikonfigurasi untuk membatasi akses ke jaringan internal hanya bagi pengguna yang terdaftar dalam sistem *Pritunl*. Selain itu, setiap data yang dikirimkan melalui VPN akan dienkripsi menggunakan protokol keamanan yang kuat untuk menghindari ancaman penyadapan. Sistem autentikasi dua faktor juga diterapkan untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses jaringan perusahaan.

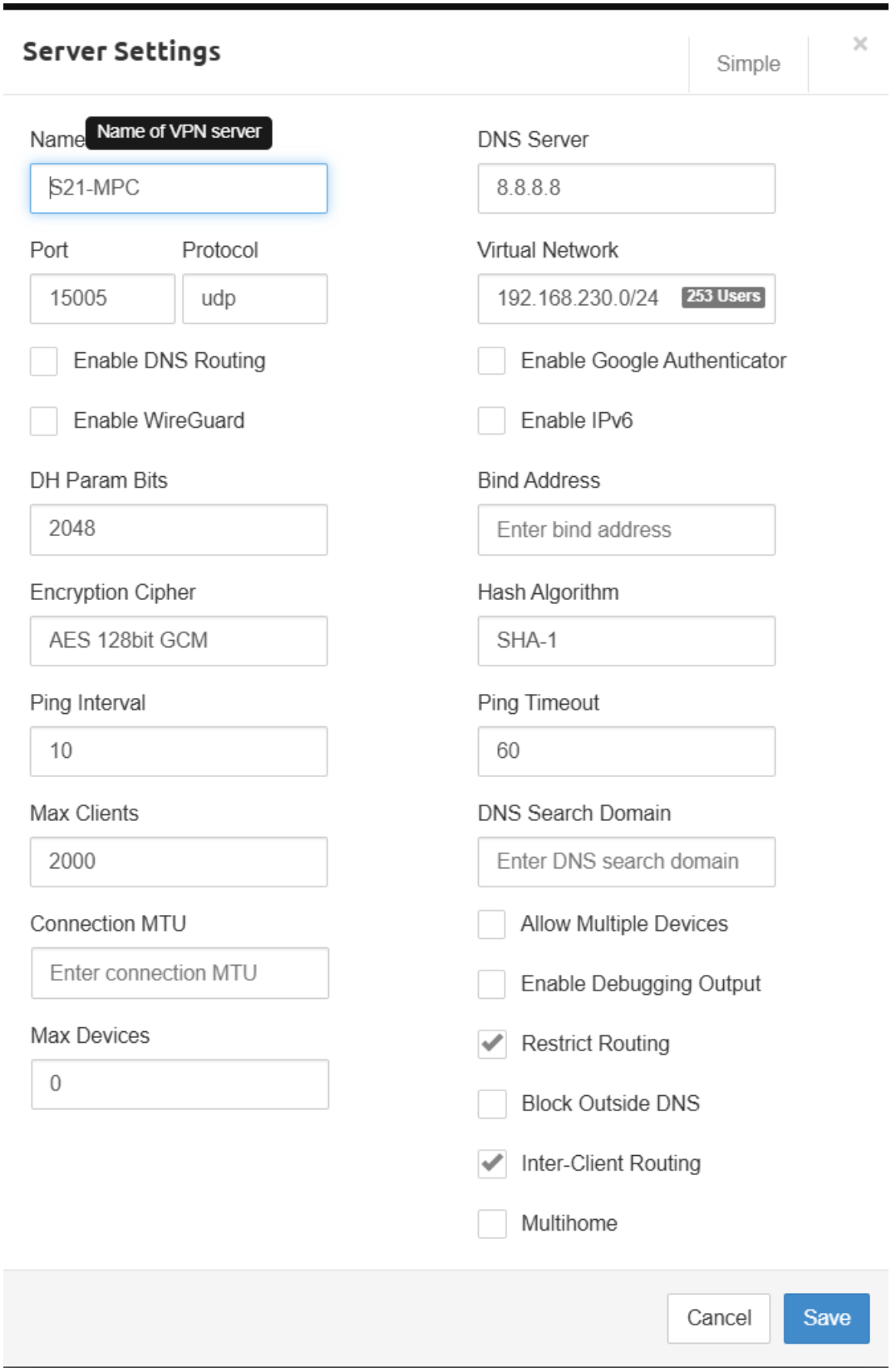
4.1.4. Rancangan Aplikasi



Sumber : Hasil Penelitian

Gambar IV. 2. *Web Page Login VPN Pritunl*

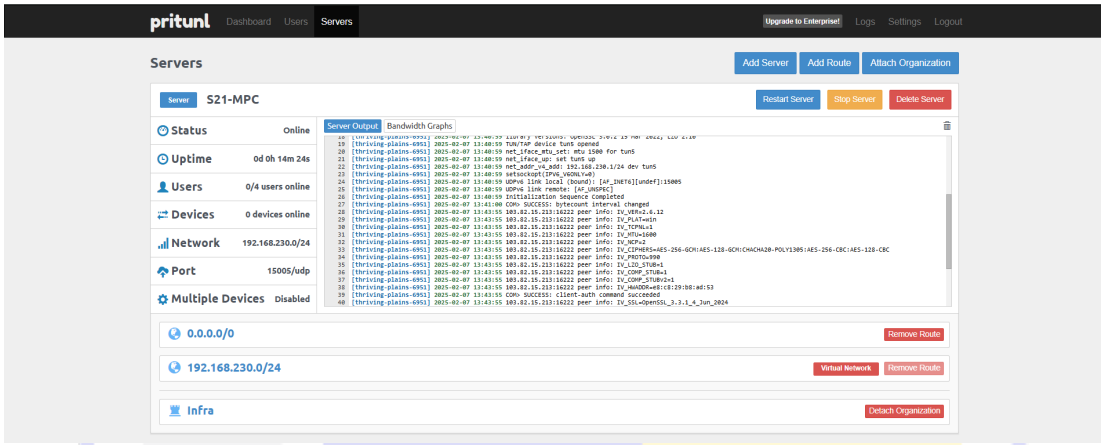
Gambar IV.2 menampilkan halaman *login* VPN Pritunl. Halaman ini merupakan titik awal bagi pengguna untuk mengakses jaringan perusahaan. Pengguna harus memasukkan kredensial yang valid untuk dapat masuk ke dalam sistem.



Sumber : Hasil Penelitian

Gambar IV. 3. *Web Page Server Settings*

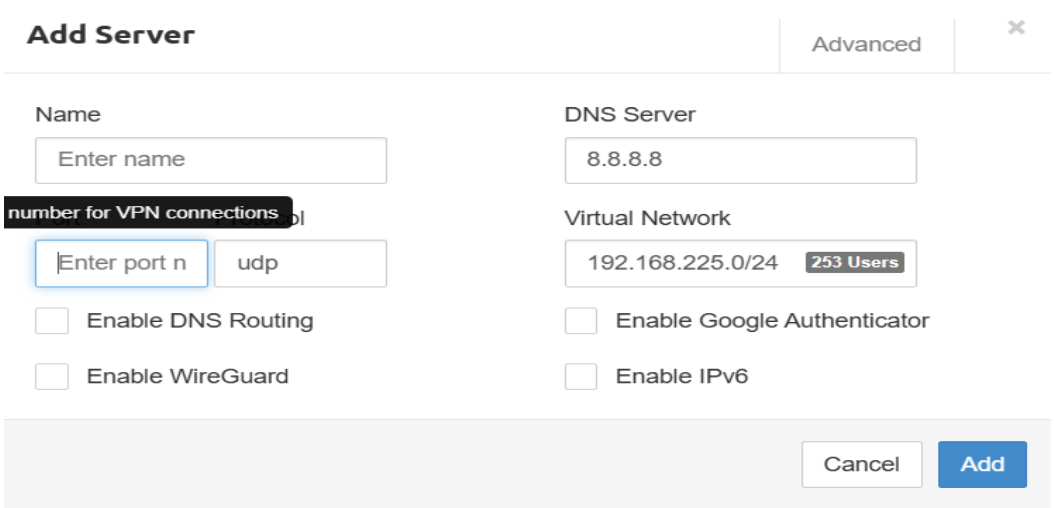
Gambar IV.3 menunjukkan halaman *server settings*, di mana administrator dapat mengonfigurasi server VPN, termasuk mengatur kebijakan akses dan enkripsi.



Sumber : Hasil Penelitian

Gambar IV. 4. *Web Page Server VPN Pritunl New*

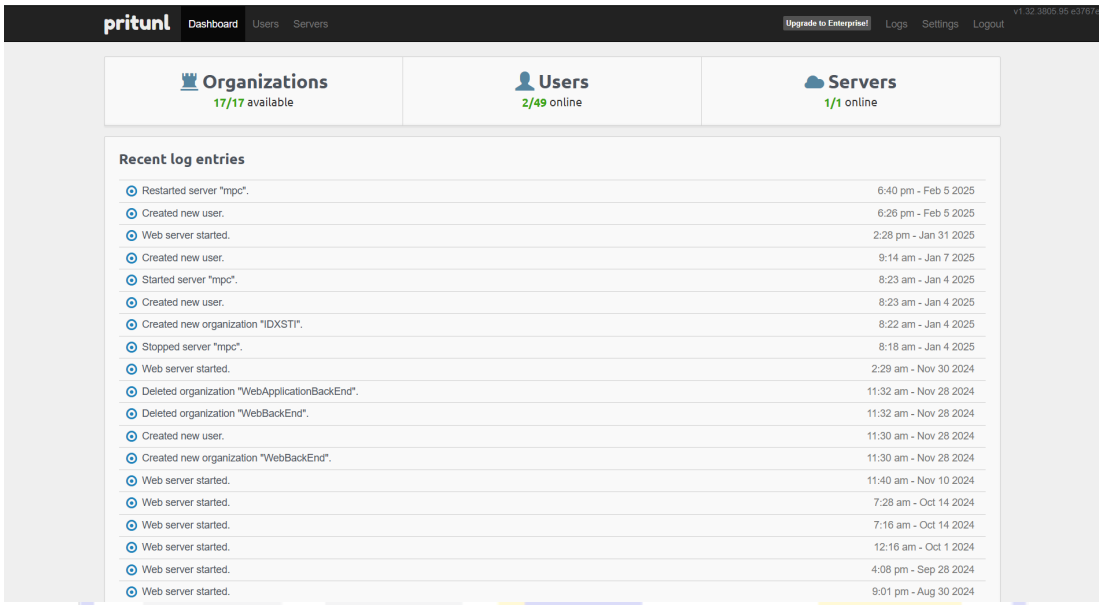
Gambar IV.4 menampilkan halaman konfigurasi server VPN *Pritunl* yang baru dibuat. Pada halaman ini, administrator dapat melakukan pengaturan dasar server, seperti memilih metode autentikasi, menentukan subnet jaringan, serta mengatur kebijakan enkripsi. Pengaturan yang dilakukan di halaman ini akan mempengaruhi bagaimana pengguna dapat terhubung ke jaringan VPN secara aman.



Sumber : Hasil Penelitian

Gambar IV. 5. *Web Page* Pembuatan Server VPN *Pritunl*

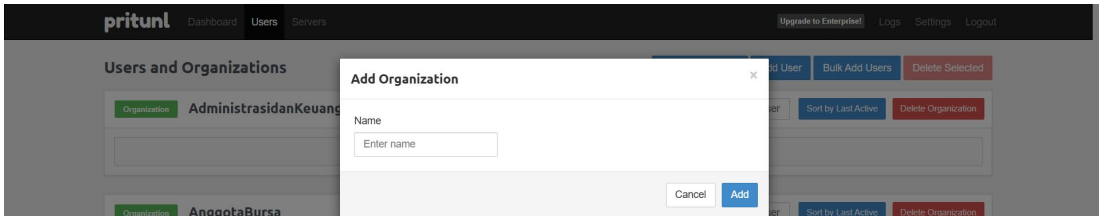
Gambar IV.5 menunjukkan proses pembuatan server VPN di *Pritunl*. Administrator dapat menyesuaikan konfigurasi server seperti menentukan alamat IP *virtual*, *port* yang digunakan, serta metode autentikasi yang dipilih. Halaman ini juga memungkinkan administrator untuk menentukan kebijakan keamanan sebelum server diaktifkan.



Sumber : Hasil Penelitian

Gambar IV. 6. *Web Page Dashboard*

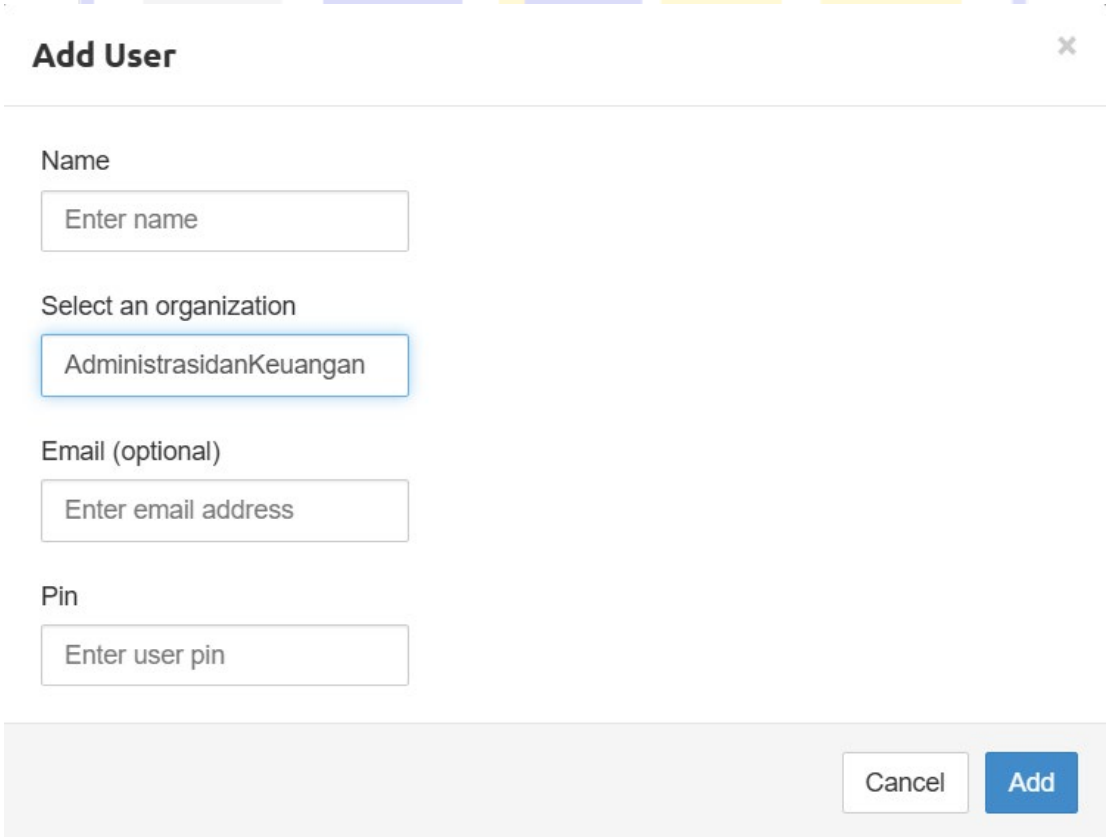
Gambar IV.6 menampilkan halaman *dashboard* utama Pritunl. Di halaman ini, administrator dapat melihat status server VPN, jumlah pengguna yang sedang terhubung, serta melakukan monitoring terhadap lalu lintas jaringan yang melewati VPN. Informasi pada dashboard ini sangat penting untuk memastikan server berjalan dengan optimal dan aman.



Sumber : Hasil Penelitian

Gambar IV. 7. *Web Page Add Organization*

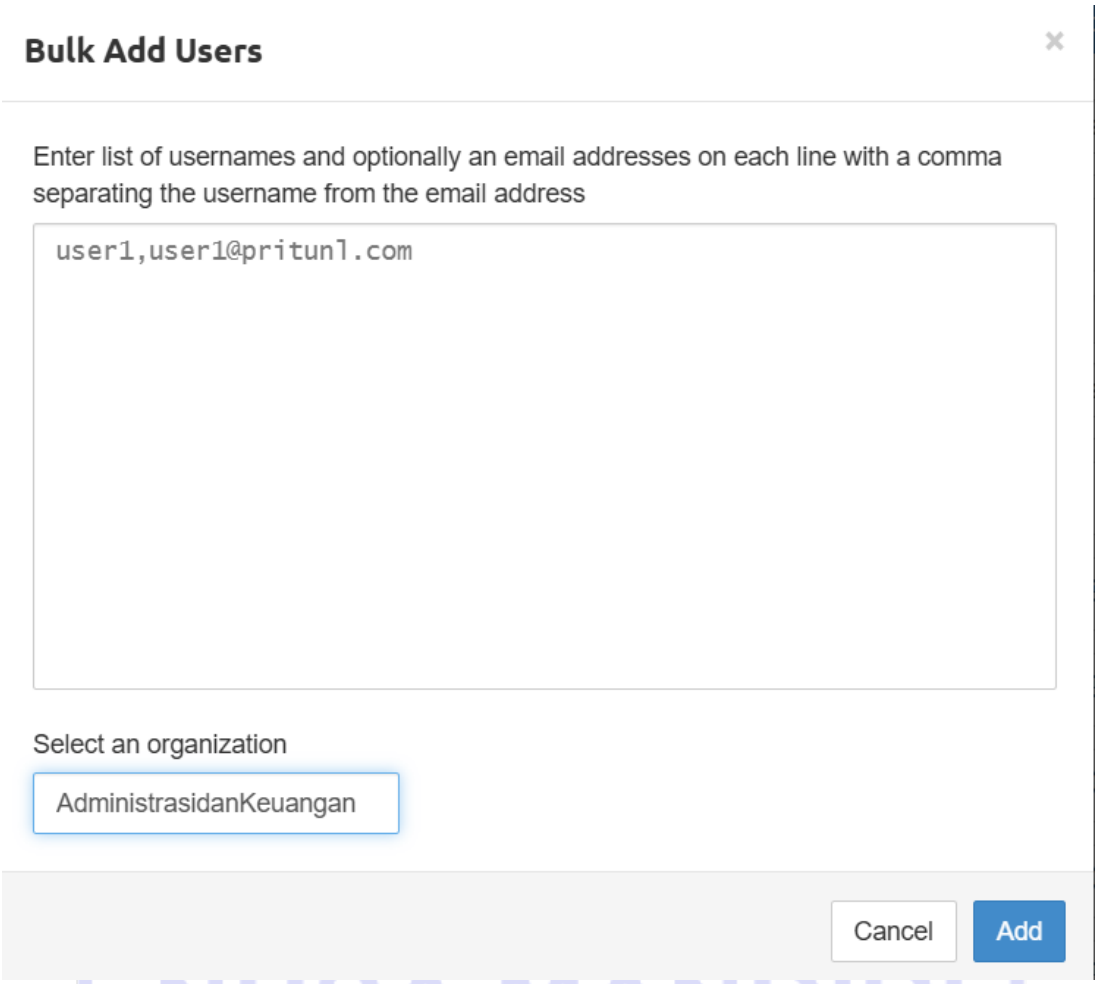
Gambar IV.7 menunjukkan halaman penambahan organisasi dalam sistem *Pritunl*. Dalam pengelolaan VPN, organisasi digunakan untuk mengelompokkan pengguna yang memiliki akses ke jaringan tertentu. Dengan adanya organisasi, administrator dapat dengan mudah mengatur hak akses dan membatasi koneksi berdasarkan kebijakan perusahaan.



Sumber : Hasil Penelitian

Gambar IV. 8. *Web Page Add User*

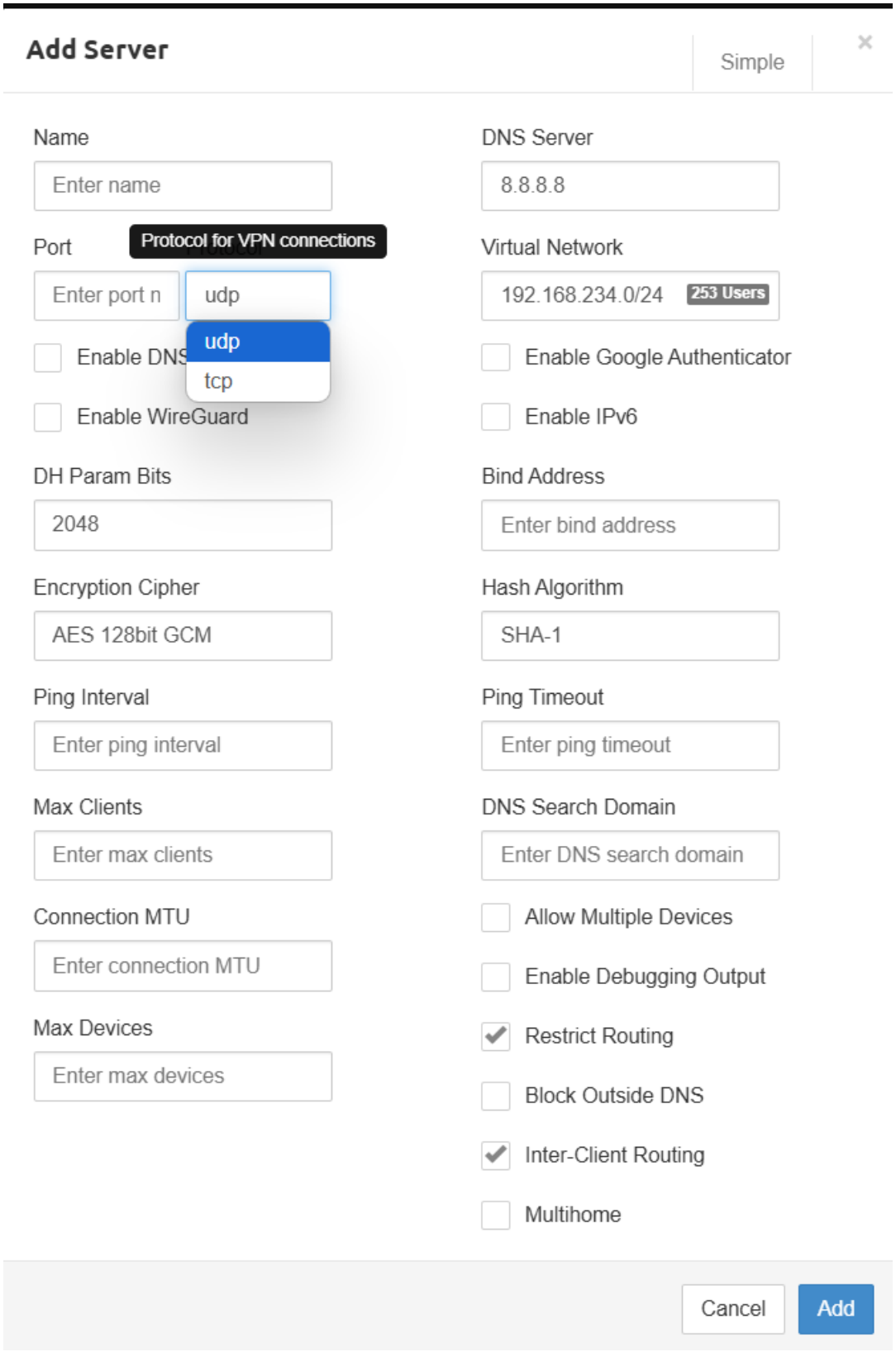
Gambar IV.8 menampilkan halaman penambahan pengguna di *Pritunl*. Administrator dapat membuat akun baru bagi pengguna yang akan mengakses VPN, menentukan metode autentikasi yang digunakan, serta menetapkan organisasi yang sesuai. Dengan sistem ini, pengelolaan pengguna dapat dilakukan dengan lebih fleksibel dan aman.



Sumber : Hasil Penelitian

Gambar IV. 9. Web Page Bulk Add Users

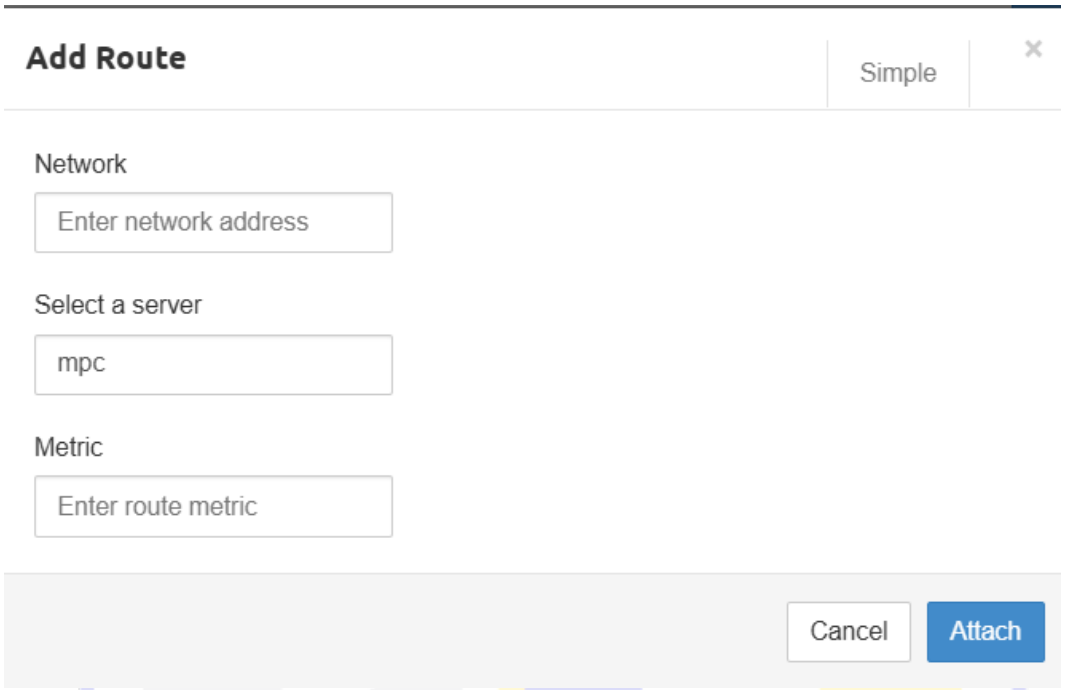
Gambar IV. 9 Menampilkan halaman penambahan bulk user dan pilihan *organization* yang diinginkan



Sumber : Hasil Penelitian

Gambar IV. 10. Web Page Add Server Advanced

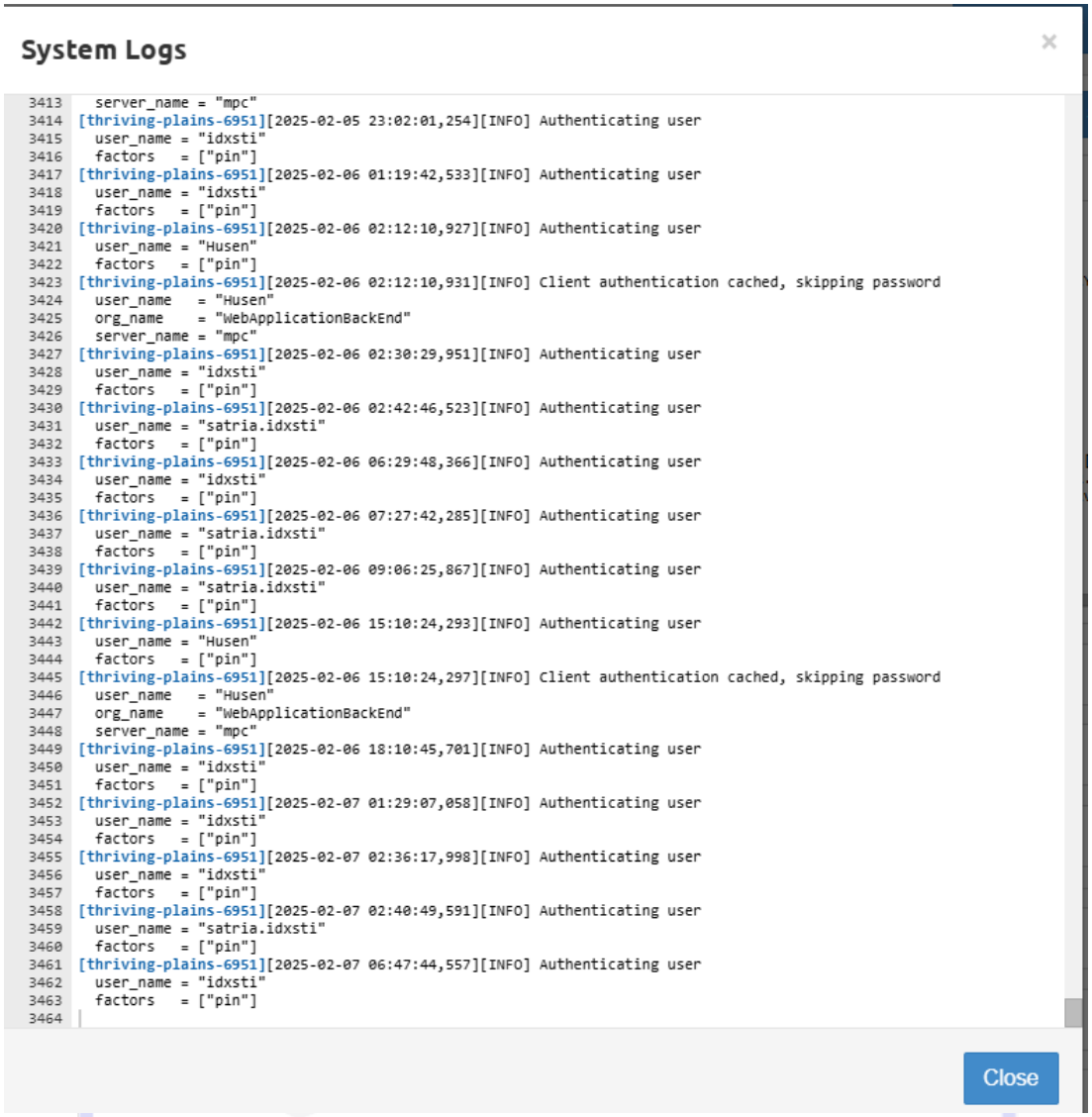
Gambar IV. 10 Menampilkan halaman untuk penambahan server lanjutan dimana ada formulir yang harus diisi mulai dari nama, DNS, Port, *Viritual Network*, dan sebagainya.



Sumber : Hasil Penelitian

Gambar IV. 11. Web *Page Add Route Advanced*

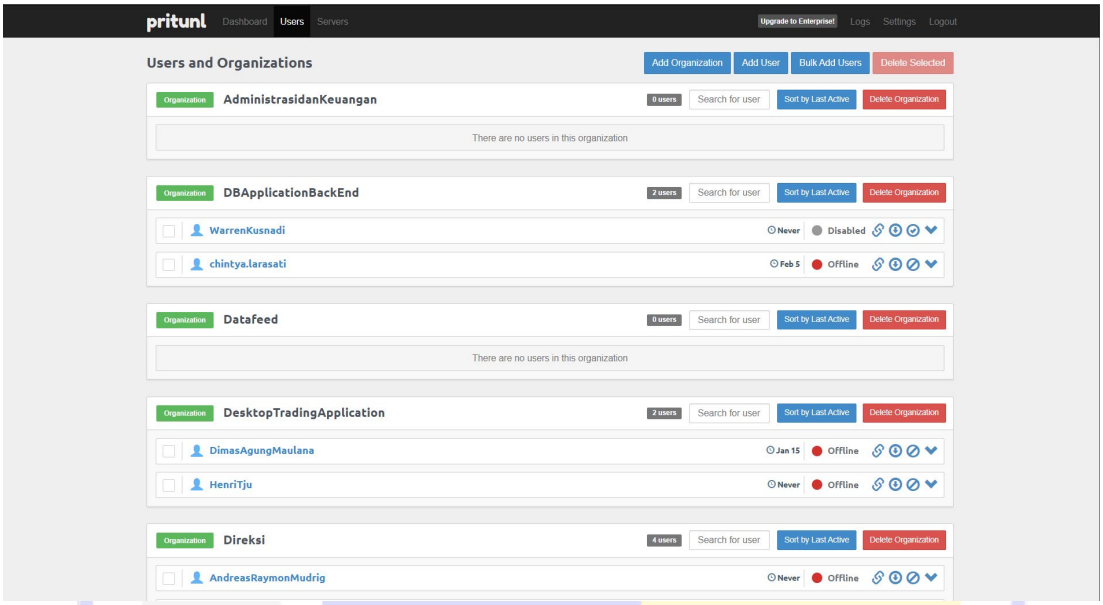
Gambar IV. 11 Menampilkan halaman penambahan Route dengan mengisi formulir yang telah tersedia seperti *Network*, *server,* dan *metric.*



Sumber : Hasil Penelitian

Gambar IV. 12. *Web Page Logs*

Gambar IV. 12 Menampilkan halaman pencatatan system logs yang terjadi serta informasi user manapun yang terhubung.



Sumber : Hasil Penelitian

Gambar IV. 13. *Web Page Users*

Gambar IV. 13 Menampilkan halaman utama untuk *user* dalam *organization* serta memberikan informasi umum dari status aktif, terakhir aktif, serta banyaknya user yang terhubung.

4.1.5. Manajemen Jaringan

Manajemen jaringan mencakup pemantauan, pemeliharaan, dan pengelolaan akses pengguna. Administrator jaringan bertanggung jawab untuk memastikan bahwa server VPN beroperasi dengan optimal dan setiap koneksi yang masuk telah diverifikasi. Selain itu, pencatatan log akses digunakan untuk melacak aktivitas pengguna guna mencegah potensi penyalahgunaan atau ancaman keamanan.

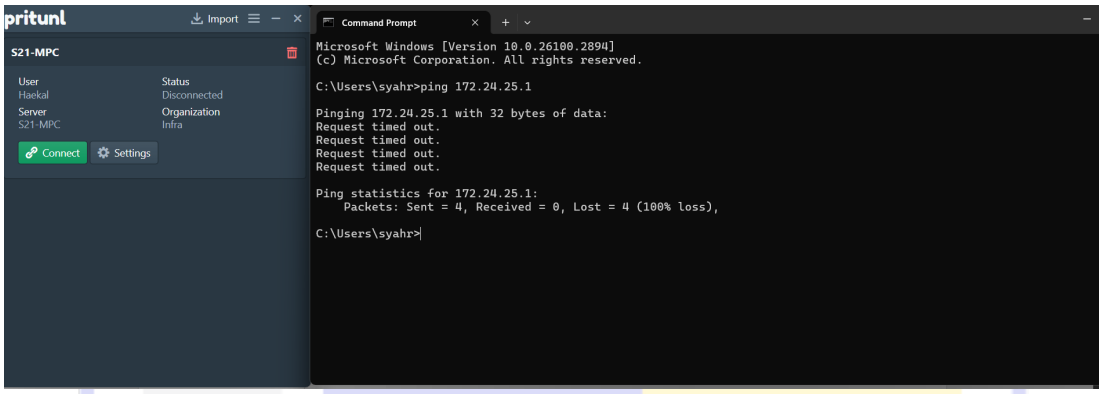
4.2. Pengujian Jaringan

Pengujian Jaringan

Untuk memastikan bahwa implementasi VPN berbasis Pritunl dapat berjalan dengan baik, dilakukan serangkaian pengujian jaringan. Pengujian ini bertujuan untuk mengevaluasi performa koneksi, kestabilan jaringan, serta efektivitas keamanan yang

diterapkan. Hasil pengujian ini akan digunakan sebagai dasar untuk melakukan penyempurnaan lebih lanjut.

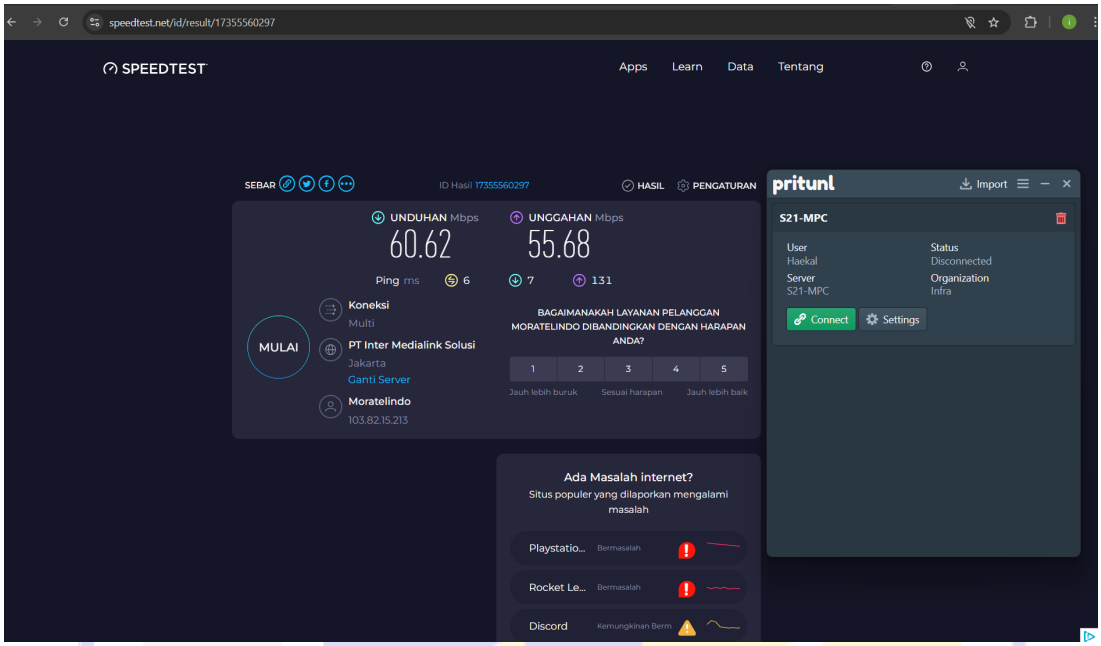
4.2.1. Pengujian Jaringan awal



Sumber : Hasil Penelitian

Gambar IV. 14. Pengujian Ping Awal

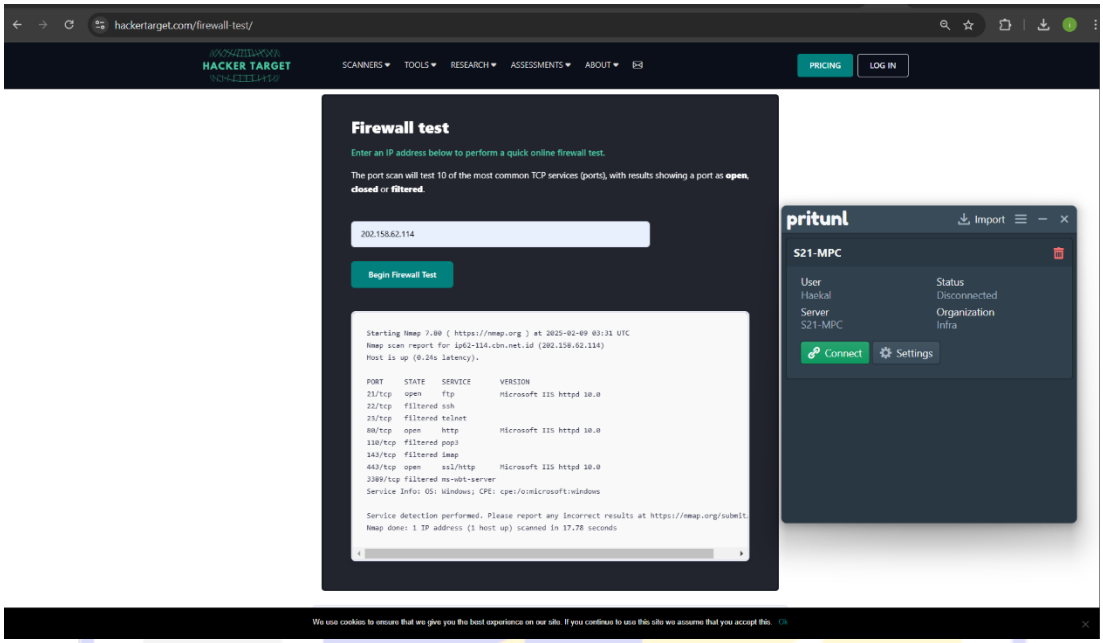
Gambar IV. 14. menampilkan hasil uji ping sebelum koneksi VPN aktif. Hasil ini menunjukkan bahwa perangkat klien belum dapat mengakses jaringan internal perusahaan karena belum terhubung melalui VPN. Dengan adanya pengujian awal ini, dapat dipastikan bahwa akses ke jaringan internal hanya dapat dilakukan melalui koneksi VPN yang telah dikonfigurasi.



Sumber : Hasil Penelitian

Gambar IV. 15. Pengujian Kecepatan Awal

Gambar IV.15 menunjukkan hasil uji kecepatan koneksi sebelum VPN diaktifkan. Data ini diambil untuk membandingkan performa jaringan sebelum dan sesudah implementasi VPN. Dari hasil ini, dapat diketahui kecepatan transfer data pada kondisi normal tanpa enkripsi tambahan dari VPN.

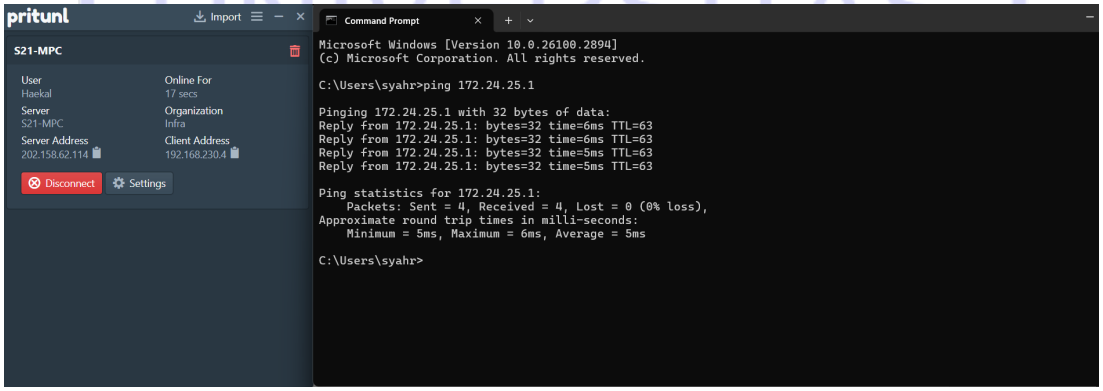


Sumber : Hasil Penelitian

Gambar IV. 16. Pengujian Firewall awal

Gambar IV.16 menampilkan pengujian *firewall* sebelum VPN diaktifkan. *Firewall* diuji untuk memastikan bahwa semua akses dari jaringan luar ditolak kecuali yang telah mendapatkan izin. Pengujian ini bertujuan untuk memastikan keamanan jaringan tetap terjaga sebelum implementasi VPN.

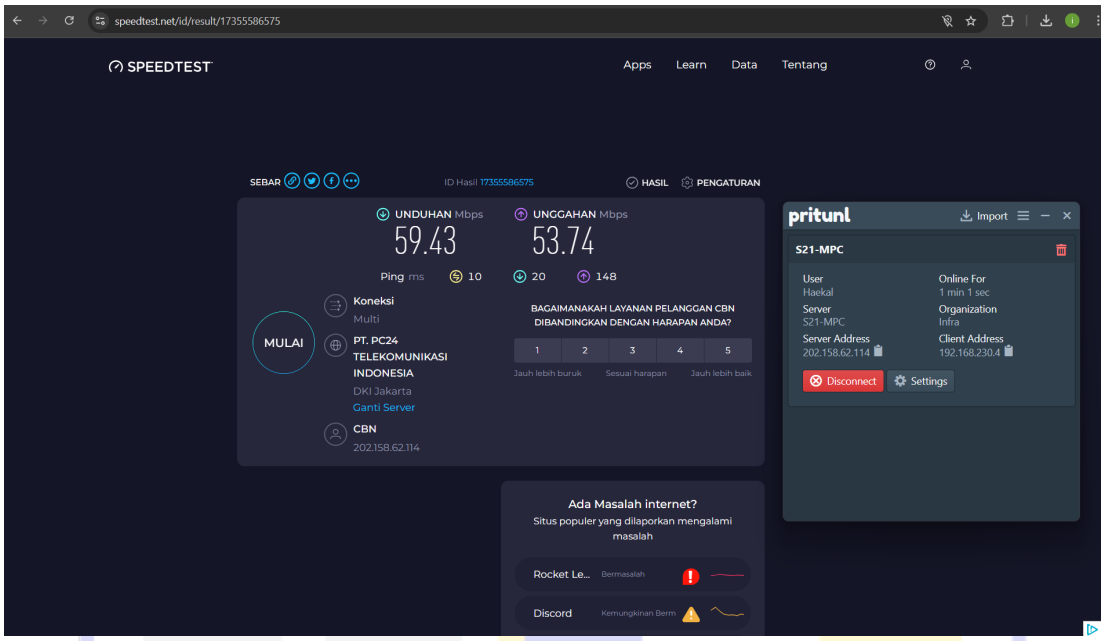
4.2.2. Pengujian Jaringan Akhir



Sumber : Hasil Penelitian

Gambar IV. 17. Pengujian Ping Akhir

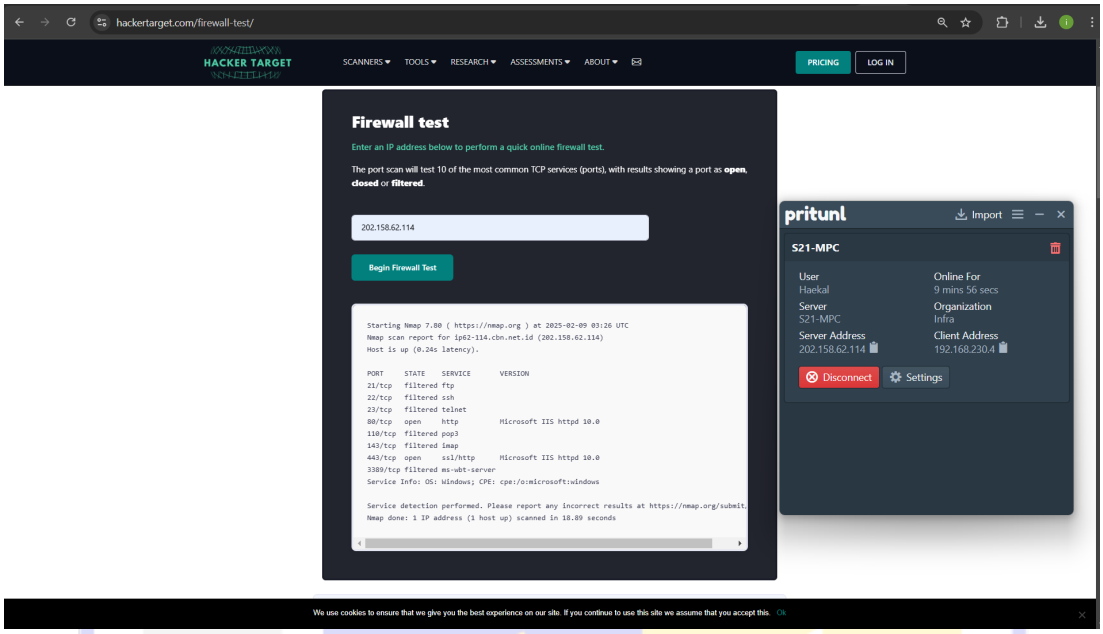
Gambar IV.17 menunjukkan hasil uji ping setelah VPN diaktifkan. Hasilnya menunjukkan bahwa perangkat klien kini dapat mengakses jaringan internal perusahaan dengan aman dan tanpa gangguan. Pengujian ini membuktikan bahwa VPN bekerja dengan baik dalam menyediakan koneksi yang stabil dan terlindungi.



Sumber : Hasil Penelitian

Gambar IV. 18. Pengujian Kecepatan Akhir

Gambar IV.18 menampilkan hasil pengujian kecepatan setelah VPN diaktifkan. Dengan adanya VPN, terjadi sedikit peningkatan latensi karena proses enkripsi yang menyebabkan kecepatan menurun, namun kecepatan transfer data tetap dalam batas optimal. Pengujian ini menunjukkan bahwa implementasi VPN tidak menghambat koneksi secara signifikan dan tetap memberikan pengalaman pengguna yang baik.



Sumber : Hasil Penelitian

Gambar IV. 19. Pengujian *Firewall*

Gambar IV.19 menampilkan hasil pengujian *firewall* setelah VPN diterapkan. Pengujian ini bertujuan untuk memastikan bahwa hanya lalu lintas data yang melalui VPN yang diizinkan masuk ke jaringan perusahaan. Hasilnya menunjukkan bahwa *firewall* bekerja dengan sangat baik dalam membatasi akses yang tidak sah, memastikan bahwa hanya pengguna yang terautentikasi dapat terhubung ke jaringan.