

IMPLEMENTASI DAN PERANCANGAN VPN (VIRTUAL PRIVATE NETWORK) MENGGUNAKAN PRITUNL (STUDI KASUS DI PT. TRANS BURGER)

PENULIS

¹⁾Abdul Hamid, ²⁾Rino Subekti, ³⁾Johan Bastari, ⁴⁾Devi Puspita Sari

ABSTRAK

Keamanan data merupakan faktor penting dalam operasional perusahaan, terutama dengan meningkatnya ancaman siber dan kebutuhan akan akses jarak jauh. Penelitian ini bertujuan untuk mengimplementasikan dan merancang *Virtual Private Network* (VPN) menggunakan Pritunl di PT. Trans Burger. Implementasi VPN ini diharapkan dapat meningkatkan keamanan data perusahaan dan memberikan akses yang aman bagi karyawan yang bekerja dari jarak jauh. Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif dan kualitatif. Proses instalasi dan konfigurasi Pritunl dilakukan di server PT. Trans Burger. Uji coba koneksi VPN dilakukan dari berbagai perangkat dan lokasi untuk mengukur kinerja dan stabilitas koneksi. Data kinerja VPN dikumpulkan menggunakan alat monitoring jaringan, sementara wawancara dan kuesioner digunakan untuk mendapatkan *feedback* dari pengguna. Hasil penelitian menunjukkan bahwa VPN yang diimplementasikan menggunakan Pritunl mampu memberikan kinerja yang baik dalam hal kecepatan koneksi, latensi, dan stabilitas. Enkripsi data dan otentikasi pengguna yang diterapkan oleh Pritunl berhasil meningkatkan keamanan data yang ditransmisikan. Penelitian ini memberikan kontribusi praktis dalam bentuk panduan implementasi VPN menggunakan Pritunl dan evaluasi kinerjanya. Selain itu, penelitian ini juga memberikan rekomendasi bagi PT. Trans Burger dalam penggunaan VPN untuk meningkatkan keamanan data mereka. Secara keseluruhan, Pritunl terbukti sebagai solusi VPN yang efektif dan efisien untuk memenuhi kebutuhan keamanan data perusahaan.

Kata Kunci

VPN (*Virtual Private Network*), Pritunl, Keamanan Data, Kinerja Jaringan

AFILIASI

Program Studi
Nama Institusi
Alamat Institusi

¹⁻⁴⁾Teknik Informatika, Fakultas Ilmu Komputer

¹⁻⁴⁾Institut Bisnis dan Informatika (IBI) Kosgoro 1957

¹⁻⁴⁾Jl. M. Kahfi II No. 33, Jagakarsa, Jakarta Selatan, DKI Jakarta

KORESPONDENSI

Penulis
Email

Abdul Hamid
abdulhamid271997@gmail.com

LICENSE



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

I. PENDAHULUAN

Keamanan data merupakan aspek yang sangat penting untuk melindungi kerahasiaan informasi, terutama pada kumpulan data yang bersifat sensitif atau penting. Oleh karena itu, diperlukan mekanisme pengamanan tambahan untuk memastikan bahwa informasi tersebut tetap aman dan terlindungi. Tanpa adanya perlindungan tambahan, data menjadi rentan terhadap berbagai ancaman, termasuk potensi serangan dari pihak yang tidak berwenang, seperti pencurian data atau akses ilegal lainnya[1]. Perusahaan perlu memastikan bahwa data yang mereka miliki terlindungi dari akses yang tidak sah dan ancaman siber lainnya. PT. Trans Burger, sebagai perusahaan yang bergerak di bidang makanan cepat saji, memiliki berbagai transaksi dan komunikasi data yang harus dilindungi dari potensi ancaman.

Dalam operasional sehari-hari, PT. Trans Burger mengandalkan jaringan komputer untuk menghubungkan berbagai cabang dan kantor pusatnya. Selain itu, dengan semakin banyaknya karyawan yang bekerja dari jarak jauh, kebutuhan akan akses jaringan yang aman dan terenkripsi menjadi semakin penting. Salah satu solusi untuk mengatasi masalah ini adalah dengan mengimplementasikan Virtual Private Network (VPN).

VPN adalah teknologi yang memungkinkan pembuatan koneksi yang aman dan terenkripsi melalui jaringan publik. Penggunaan VPN dapat dianggap lebih aman karena data yang dikirimkan melalui jaringan publik akan dienkripsi terlebih dahulu, sehingga kerahasiaannya tetap terjaga. Meskipun data melewati jaringan umum, enkripsi memastikan bahwa informasi tidak dapat diakses oleh pihak yang tidak berwenang. VPN bekerja dengan menciptakan jaringan virtual yang aman di dalam jaringan yang sudah ada, suatu mekanisme yang dikenal sebagai tunneling atau terowongan. Tunneling ini memungkinkan data untuk dikirimkan melalui jalur privat dengan memanfaatkan infrastruktur pihak ketiga, sehingga pengguna dapat menikmati koneksi yang aman dan terlindungi[2]. Pritunl adalah salah satu perangkat lunak open-source yang dapat digunakan untuk mengimplementasikan VPN. Pritunl menawarkan berbagai fitur keamanan dan fleksibilitas yang dapat membantu perusahaan dalam menjaga kerahasiaan dan integritas data.

Implementasi VPN menggunakan Pritunl di PT. Trans Burger diharapkan dapat memberikan solusi yang efektif dalam meningkatkan keamanan data perusahaan. Selain itu, penelitian ini juga bertujuan untuk menganalisis kinerja dan stabilitas koneksi VPN yang diimplementasikan, serta mengidentifikasi kendala yang dihadapi selama proses implementasi dan menemukan solusi untuk mengatasinya.

II. METODE PENELITIAN

1) Wawancara

Wawancara dilakukan dengan tim IT dan manajemen PT. Trans Burger untuk mendapatkan informasi mengenai kebutuhan dan masalah yang dihadapi terkait keamanan data dan akses jaringan.

2) Observasi

Pengamatan langsung ke lapangan (observasi) yang dilakukan oleh penulis, tempat dan waktu pelaksanaannya yaitu pada PT. Trans Burger, Transmart Yasmin Bogor terhitung pada bulan Oktober sampai November.

3) Studi Pustaka

Studi pustaka dapat melengkapi informasi yang dibutuhkan dalam melakukan penelitian. Informasi yang berkaitan dengan topik atau masalah yang dapat mendukung penyelesaian masalah yang dibahas.

4) Kuesioner

Kuesioner disebarkan kepada karyawan yang menggunakan VPN untuk mengumpulkan data mengenai pengalaman mereka, kepuasan, dan tingkat keamanan yang dirasakan.

5) Analisa dan Perancangan

Analisa diperlukan untuk menguraikan proses analisis pembangunan VPN sistem dan perancangan topologi jaringan fisik dan perancangan logis VPN sistem.

- 6) Simulasi
Pada tahap ini penulis membuat simulasi dengan pada aplikasi simulator, seperti Virtualbox, sebagai simulasi dari sistem yang akan diimplementasikan.
- 7) Implementasi
Tahapan selanjutnya adalah implementasi, dimana hasil dari tahap-tahap sebelumnya diimplementasikan. Proses implementasi yang akan dilakukan adalah instalasi dan konfigurasi.
- 8) Monitoring
Tahap ini akan dilakukan pengujian pada sistem Pritunl. Pengujian mencakup aktivitas pengoperasian sistem untuk memastikan fungsionalitasnya berjalan sesuai harapan, serta pengamatan terhadap kinerja sistem secara menyeluruh.
- 9) Manajemen
Tahap ini mencakup serangkaian kegiatan untuk memastikan sistem yang telah dibangun tetap berfungsi secara optimal dan sesuai dengan kebutuhan operasional. Aktivitas yang dilakukan meliputi perawatan, pemeliharaan, dan pemantauan berkelanjutan.

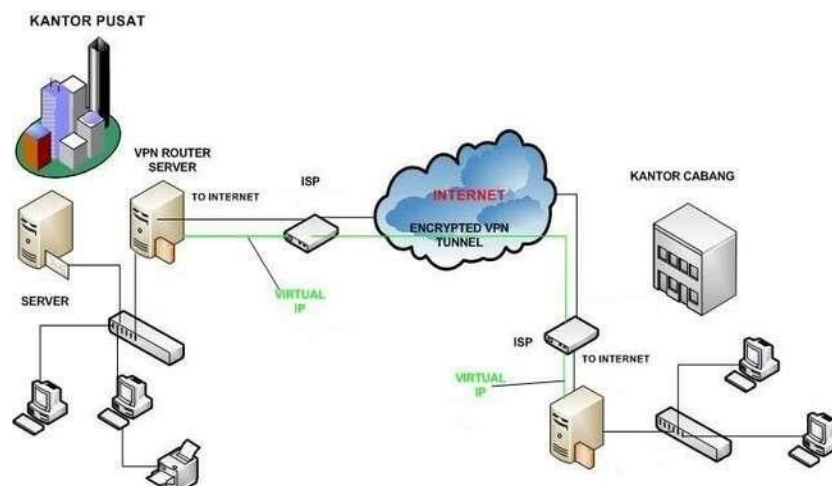
III. HASIL DAN PEMBAHASAN

3.1 Analisis sistem

Pada tahap ini, dilakukan analisis terhadap sistem VPN yang akan dibangun dengan fokus pada kebutuhan perangkat keras, perangkat lunak, dan konektivitas yang diperlukan. Sistem VPN dirancang untuk menghubungkan kantor cabang dengan kantor pusat, dalam hal ini PT. Trans Burger sebagai kantor pusat. Konsep yang digunakan adalah VPN jenis Remote Access, di mana pengguna di kantor cabang dapat langsung terhubung ke jaringan kantor pusat tanpa memerlukan perangkat tambahan seperti router di lokasi cabang. Implementasi ini bertujuan untuk memberikan akses yang aman dan efisien kepada pengguna, memungkinkan mereka untuk terhubung ke jaringan kantor pusat melalui internet dengan protokol enkripsi yang memastikan kerahasiaan data tetap terjaga.

3.2 Perancangan

Pada bagian ini akan dibahas secara rinci mengenai perencanaan infrastruktur VPN, termasuk proses konfigurasi dan instalasi perangkat keras maupun perangkat lunak yang digunakan dalam jaringan untuk mendukung implementasi VPN. Infrastruktur yang dirancang mencakup komponen-komponen utama, yaitu server yang berfungsi sebagai pusat pengelolaan koneksi VPN dan klien berupa perangkat PC yang digunakan oleh pengguna. Selain itu, perangkat lunak pendukung juga menjadi bagian penting dalam memastikan koneksi VPN dapat berjalan dengan baik, meliputi aplikasi untuk server VPN, perangkat lunak klien, serta protokol enkripsi yang digunakan untuk menjamin keamanan data selama transmisi.

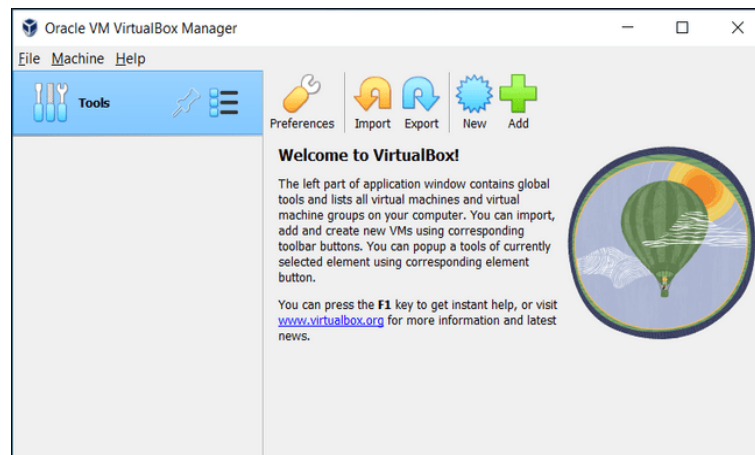


Gambar 1. Simulasi Jaringan yang Akan Dirancang

3.3 Implementasi

1) Inisialisasi VirtualBox Version 7.0.6

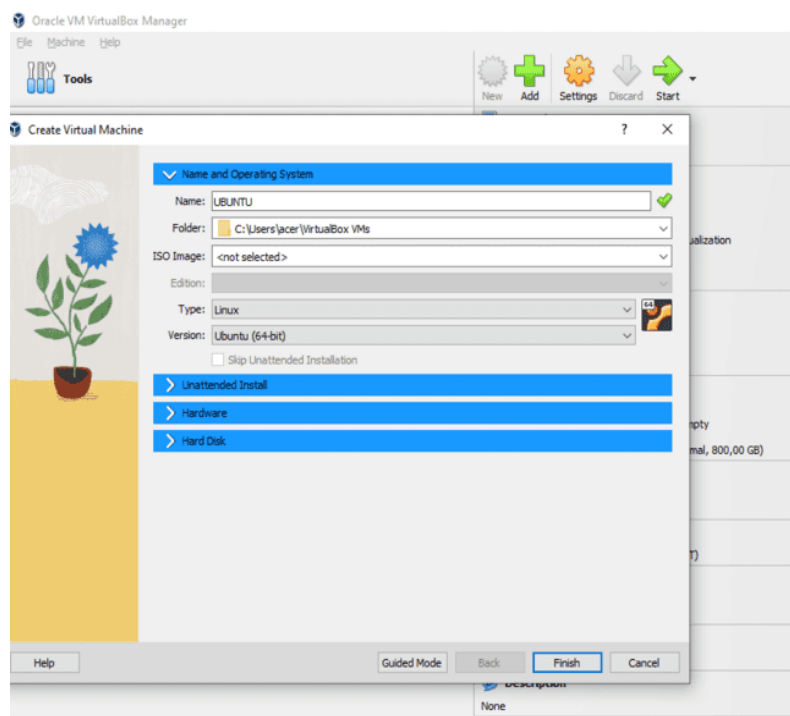
VirtualBox merupakan perangkat lunak virtualisasi yang dirancang untuk memungkinkan pengguna menjalankan beberapa sistem operasi secara bersamaan pada satu komputer fisik. Dikembangkan oleh Oracle, VirtualBox mendukung berbagai platform sistem operasi, termasuk Windows, Linux, dan macOS. Dengan menggunakan VirtualBox, pengguna dapat membuat lingkungan virtual yang berfungsi seperti komputer fisik, sehingga memungkinkan instalasi, konfigurasi, dan pengujian sistem operasi atau aplikasi tanpa memengaruhi sistem utama.[3]. Tahap dimulai dengan mendownload virtual box pada website https://www.virtualbox.org/wiki/Download_Old_Builds_7_0, lalu setelah itu dilakukan proses penginstalan.



Gambar 2. Tampilan Setelah Penginstalan

2) Konfigurasi Ubuntu pada VirtualBox

Ubuntu adalah sistem operasi open-source berbasis Linux yang dikembangkan oleh Canonical Ltd. Dirancang untuk kemudahan penggunaan, Ubuntu adalah salah satu distribusi Linux yang paling populer dan banyak digunakan di seluruh dunia. Pada tahapan ini diawali dengan mendownload file ISO Ubuntu di website <https://ubuntu.com/download/server>, lalu di lanjutkan dengan melakukan setting Ubuntu pada virtualbox.



Gambar 3. Tampilan Setting Ubuntu

3) Konfigurasi Mongodb dan Pritunl

Konfigurasi dilakukan pada server Ubuntu yang telah terinstall pada virtualbox, proses instalasi dilakukan pada terminal Ubuntu dengan syntax berikut.

```

• sudo tee /etc/apt/sources.list.d/mongodb-org.list << EOF
deb[signed-by=/usr/share/keyrings/mongodb-server-8.0.gpg]
https://repo.mongodb.org/apt/ubuntu noble/mongodb-org/8.0
multiverse EOF

• sudo tee /etc/apt/sources.list.d/openvpn.list << EOF
deb[signed-by=/usr/share/keyrings/openvpn-repo.gpg]
https://build.openvpn.net/debian/openvpn/stable noble
main EOF

• sudo tee /etc/apt/sources.list.d/pritunl.list << EOF
deb[signed-by=/usr/share/keyrings/pritunl.gpg]
https://repo.pritunl.com/stable/apt noble
main EOF

• sudo apt --assume-yes install gnupg
curl -fsSL https://www.mongodb.org/static/pgp/server-8.0.asc |
sudo gpg -o /usr/share/keyrings/mongodb-server-8.0.gpg --dearmor --yes

• curl -fsSL https://swupdate.openvpn.net/repos/repo-public.gpg |
sudo gpg -o /usr/share/keyrings/openvpn-repo.gpg --dearmor --yes

• curl -fsSL https://raw.githubusercontent.com/pritunl/pgp/master/pritunl_repo_pub.asc |
sudo gpg -o /usr/share/keyrings/pritunl.gpg --dearmor --yes

• sudo apt update

• sudo apt --assume-yes install pritunl openvpn mongodb-org wireguard wireguard-tools

• sudo ufw disable

• sudo systemctl start pritunl mongod

• sudo systemctl enable pritunl mongod

```

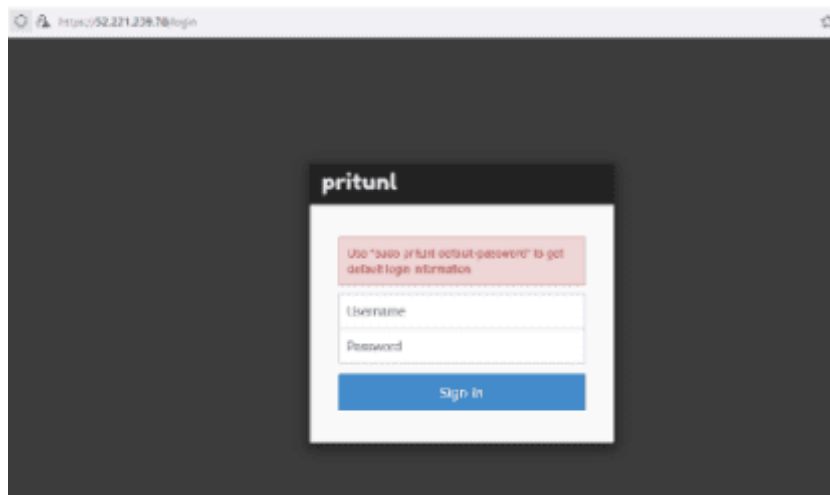
Gambar 4. Syntax Instalasi Mongodb dan Pritunl

```

root@ip-172-31-25-183:/home/ubuntu# sudo apt-get --assume-yes install pritunl mongo
db-server
sudo: unable to resolve host ip-172-31-25-183
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libboost-filesystem1.65.1 libboost-iostreams1.65.1
  libboost-program-options1.65.1 libboost-system1.65.1 libgoogle-perftools4
  libipsecpp8v5 libipsecv1-helper1 libpython-stdlib libpython2.7-minimal
  libpython2.7-stdlib libsnappy1v5 libstemmer0d libtcmalloc-minimal4
  libyaml-cpp0.5v5 mongo-tools mongodb-clients mongodb-server-core openvpn
  pritunl-ndppd python python-minimal python2.7 python2.7-minimal
Suggested packages:
  easy-rsa resolvconf python-doc python-tk python2.7-doc binutils binfmt-support
The following NEW packages will be installed:
  libboost-filesystem1.65.1 libboost-iostreams1.65.1
  libboost-program-options1.65.1 libboost-system1.65.1 libgoogle-perftools4
  libipsecpp8v5 libipsecv1-helper1 libpython-stdlib libpython2.7-minimal
  libpython2.7-stdlib libsnappy1v5 libstemmer0d libtcmalloc-minimal4
  libyaml-cpp0.5v5 mongo-tools mongodb-clients mongodb-server-core
  openvpn pritunl pritunl-ndppd python python-minimal python2.7 python2.7-minimal
0 upgraded, 25 newly installed, 0 to remove and 0 not upgraded.
Need to get 96.8 MB of archives.
After this operation, 492 MB of additional disk space will be used.
Get:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64
  libpython2.7-minimal amd64 2.7.17-1~18.04ubuntu1.6 [335 kB]
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64
  python2.7-minimal amd64 2.7.17-1~18.04ubuntu1.6 [1291 kB]
Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu bionic/main amd64 python-
  minimal amd64 2.7.15~rc1-1 [28.1 kB]
Get:4 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64
  libpython2.7-stdlib amd64 2.7.17-1~18.04ubuntu1.6 [1917 kB]

```

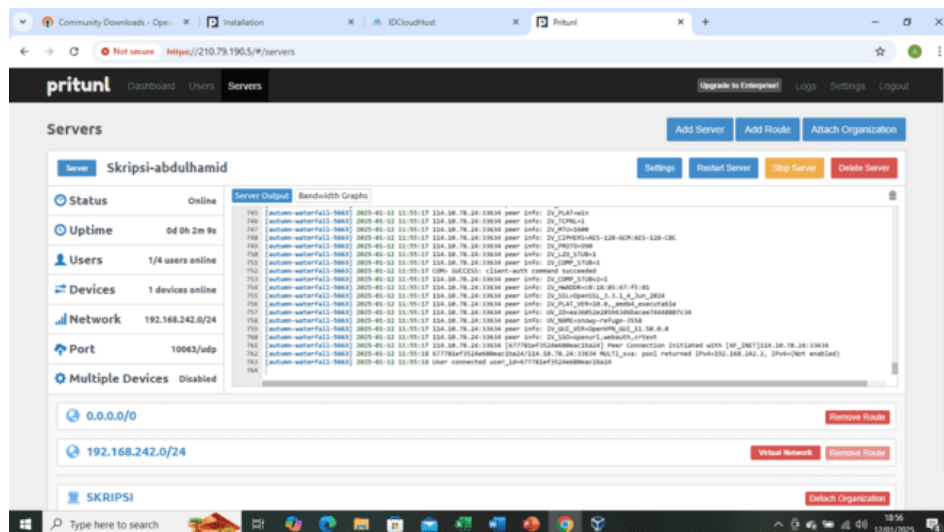
Gambar 5. Proses Instalasi Mongodb dan Pritunl



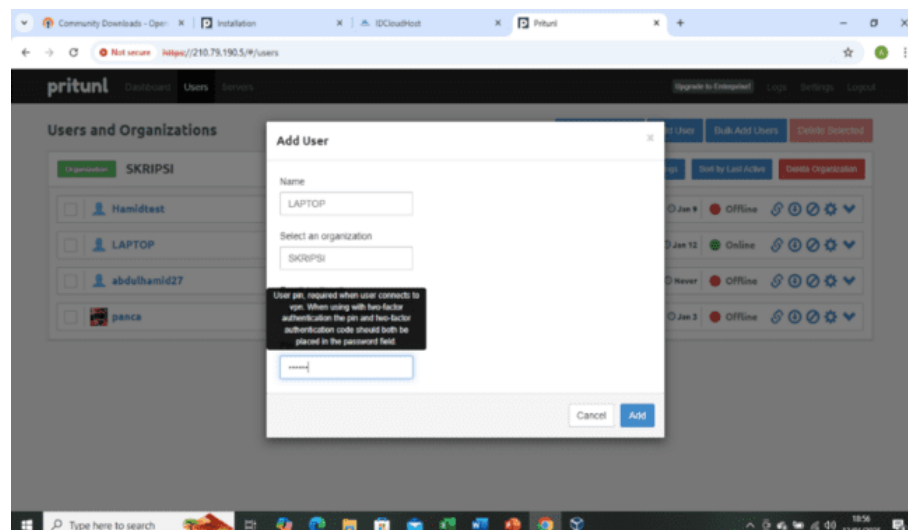
Gambar 5. Proses Halaman Login Pritunl

4) Konfigurasi Server VPN

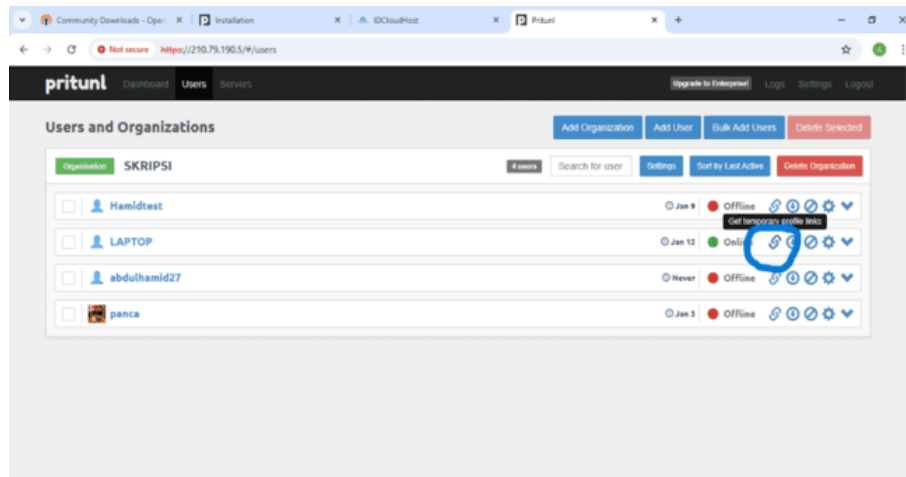
Konfigurasi VPN server ini dirancang untuk memenuhi kebutuhan jenis Remote Access VPN, di mana pengguna dari kantor cabang dapat mengakses jaringan kantor pusat melalui perangkat masing-masing tanpa memerlukan perangkat tambahan seperti router.



Gambar 6. Tampilan VPN Server setelah Aktif



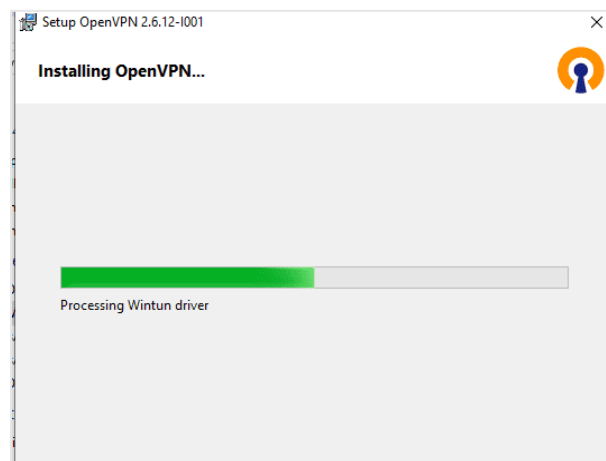
Gambar 7. Pembuatan User Client yang Akan Disambungkan



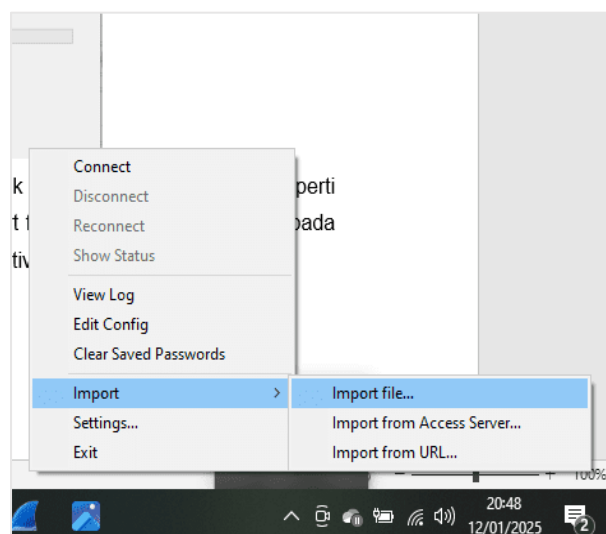
Gambar 8. Pembuatan Key File untuk Akses Masuk Jaringan VPN

5) Konfigurasi VPN Client

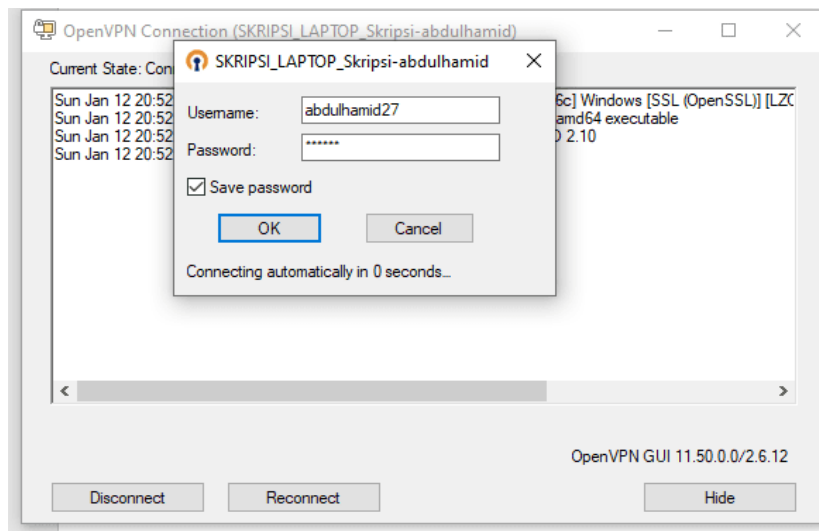
Pada tahap ini akan menyiapkan VPN client pada perangkat yang digunakan oleh pengguna di kantor cabang. Tahap Konfigurasi VPN client ini bertujuan agar perangkat klien dapat terhubung ke server VPN secara aman dan mendapatkan akses ke jaringan. Tahap ini dimulai dengan mendownload aplikasi VPN Client, lalu dilanjutkan dengan proses penginstalan, setelahnya perlu dimasukkan KEY file yang sebelumnya sudah di download, dan akhirnya proses login dengan username dan password.



Gambar 9. Proses Instalasi VPN Client



Gambar 10. Proses Import KEY File untuk Akses ke Jaringan



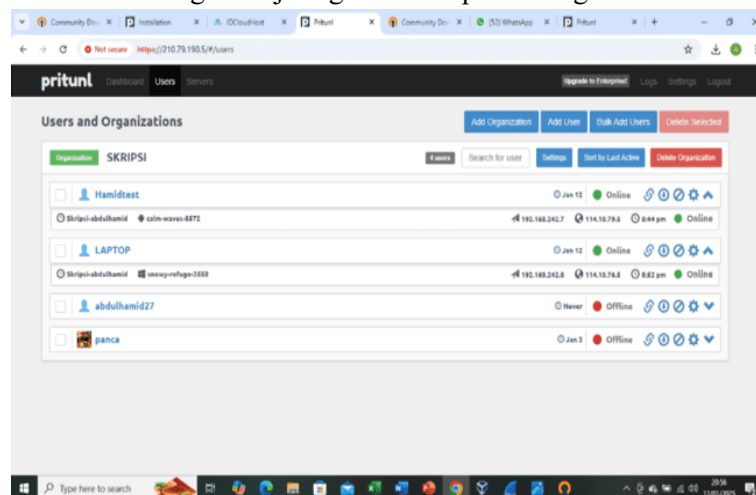
Gambar 11. Proses Login VPN Client

3.4 Pengujian

Pengujian pada VPN dilakukan untuk memastikan bahwa koneksi pengguna telah berhasil melalui jaringan VPN. Pengujian ini mencakup beberapa metode untuk memastikan keandalan dan keamanan koneksi. Pertama, pengujian dilakukan dengan memantau status konektivitas pengguna melalui dashboard Pritunl. Pada dashboard, status pengguna yang terhubung akan ditampilkan sebagai Online, menandakan bahwa perangkat klien telah berhasil terhubung ke server VPN. Selanjutnya, pengujian dilakukan dengan membandingkan hasil tangkapan data menggunakan Wireshark sebelum dan sesudah VPN diaktifkan.

1) Pengujian Konektivitas User

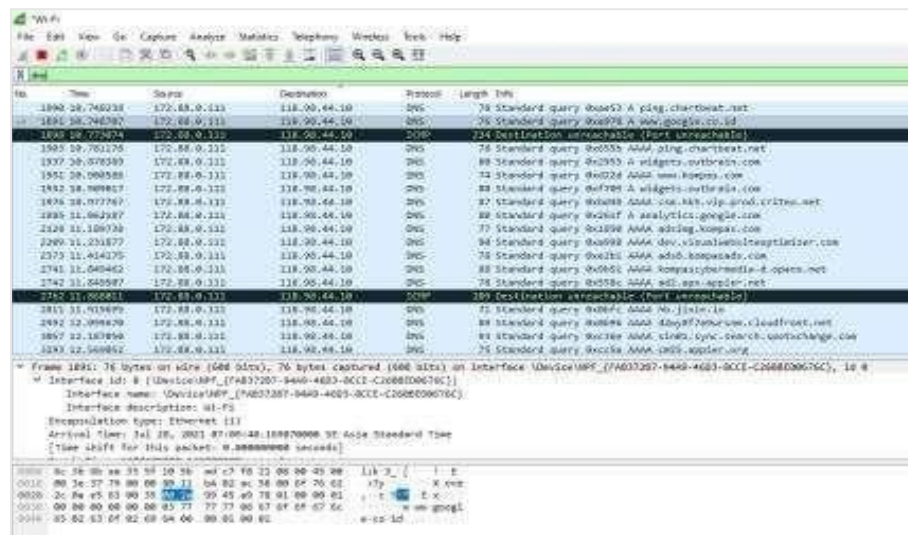
Pada tahap pengujian, konektivitas pengguna VPN diuji untuk memastikan bahwa perangkat klien dapat terhubung ke server VPN dan mengakses jaringan kantor pusat dengan stabil.



Gambar 12. Dashboard Konektivitas User Pritunl

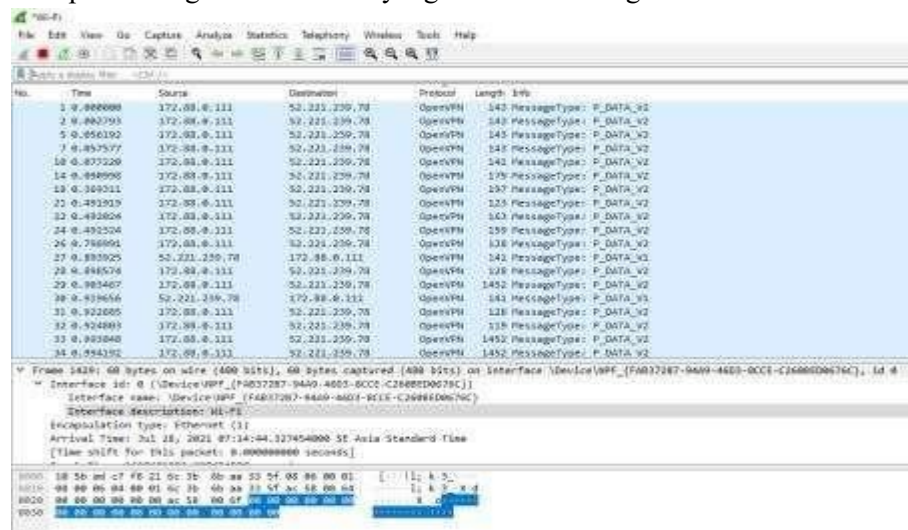
2) Pengujian Perbandingan dengan Wireshark

Pengujian ini dilakukan untuk memastikan keamanan data yang dikirimkan melalui VPN, dilakukan pengujian dengan menggunakan aplikasi Wireshark. Wireshark adalah perangkat lunak yang digunakan untuk menganalisis lalu lintas data dalam jaringan. Perangkat lunak ini berfungsi untuk menangkap setiap paket data yang melintas di jaringan dan menampilkan informasi paket tersebut secara rinci. Dengan kemampuan mendukung berbagai jenis protokol, Wireshark memungkinkan pengguna untuk dengan mudah menangkap, memantau, dan menganalisis berbagai format paket data[4]. Pengujian ini bertujuan untuk membandingkan paket data yang dikirimkan sebelum dan sesudah mengaktifkan VPN.



Gambar 13. Pengujian Koneksi Tanpa VPN

Dari gambar di atas, dapat disimpulkan bahwa koneksi yang digunakan oleh pengguna tidak memiliki tingkat keamanan yang memadai. Hal ini terlihat dari informasi pada paket data yang dapat diakses dengan mudah, seperti alamat website tujuan yang dikunjungi oleh pengguna. Situasi ini menunjukkan bahwa data yang dikirim melalui koneksi tersebut tidak terenkripsi, sehingga rentan terhadap pengawasan oleh pihak ketiga atau individu yang tidak berwenang.



Gambar 14. Pengujian Koneksi dengan VPN

Setelah menggunakan VPN, data terenkripsi dan informasi sensitif dilindungi selama transmisi. Hal ini menunjukkan bahwa VPN memberikan lapisan keamanan tambahan pada koneksi jaringan, sesuai dengan tujuan implementasinya.

IV. KESIMPULAN

Kesimpulan berdasarkan hasil evaluasi simulasi VPN menggunakan Virtual Box dan Implementasi VPN menggunakan Pritunl adalah dengan menggunakan server VPN, akses ke website menjadi lebih aman dari serangan seperti Man In The Middle (MITM). Seluruh paket data yang dikirim melalui jaringan VPN akan dienkripsi terlebih dahulu, sehingga isi data tidak dapat dibaca atau diakses oleh pihak yang tidak berwenang. Hal ini meningkatkan tingkat kerahasiaan dan keamanan data pengguna. VPN dapat memblokir iklan online yang mengganggu selama pengguna berselancar di internet. Hal ini memberikan pengalaman pengguna yang lebih nyaman dan fokus, terutama ketika mengakses website atau platform tertentu. Agar koneksi dari klien ke server VPN dan website tujuan tetap stabil, disarankan untuk menggunakan penyedia layanan internet (ISP)

atau infrastruktur server VPN yang memiliki koneksi yang andal. Stabilitas koneksi ini penting untuk memastikan kelancaran dalam penggunaan VPN. Untuk meningkatkan efektivitas VPN, diperlukan pembaruan rutin pada daftar domain yang akan diblokir. Pembaruan ini bertujuan untuk memblokir domain iklan baru yang belum terdaftar. Selain itu, pemeliharaan sistem secara berkala diperlukan untuk mengurangi kemungkinan false positives saat memblokir domain, sehingga akses ke situs yang valid tetap berjalan tanpa gangguan.

REFERENSI

- [1] B. Anwar, N. B. Nugroho, J. Prayudha, A. Stmik, and T. Dharma, "Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam," vol. 18, no. SAINTIKOM, pp. 30–34, 2019.
- [2] D. Novianto, Y. S. Japriadi, and L. Tommy, "Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik," *Jurnal Ilmiah Informatika Global*, vol. 13, no. 2, Aug. 2022, doi: 10.36982/jiig.v13i2.2308.
- [3] F. Gratianus and N. Larosa, "PEMANFAATAN VIRTUAL BOX DALAM PRAKTIKUM ADMINISTRASI SERVER MENGGUNAKAN TEKNIK DHCP PADA MIKROTIK ROUTER OS," 2016.
- [4] M. Hasbi and N. R. Saputra, "ANALISIS QUALITY OF SERVICE (QOS) JARINGAN INTERNET KANTOR PUSAT KING BUKOPIN DENGAN MENGGUNAKAN WIRESHARK," 2021. [Online]. Available: <https://jurnal.umj.ac.id/index.php/just-it/index>
- [5] F. Angellia, W. Cahya, R. Ramadhan, and I. Hariyansah, "Sosialisasi Penggunaan Virtual Meeting Untuk Mendukung Kegiatan Bisnis UMKM di Masa Pandemic Covid 19," *J. Pengabd. Teratai*, vol. 1, no. 2, pp. 206–213, 2020, doi: 10.55122/teratai.v1i2.153.
- [6] B. Firmansyah, "Implementasi Teknologi Qr-Code Sebagai Pencarian Data Ruangan Pada Ibi Kosgoro 1957 Berbasis Android," *JunifJurnal Nas. Inform.*, vol. 1, no. 1, pp. 30–42, 2020.
- [7] S. Hidayat, W. Cahya, and H. Rifiyanti, "Bimbingan Teknis Pengelolaan Konten Pemasaran Digital Pada Lembaga Bimbingan Belajar Ahe Tanah Baru," vol. 4, no. 2, pp. 189–194, 2023.