IMPLEMENTASI TUNNELING MENGGUNAKAN WIREGUARD UNTUK MEMBANGUN FASILITAS LABORATORIUM KOMPUTER ONLINE

TUGAS AKHIR

Sebagai salah satu syarat untuk memperoleh gelar Sarjana S-1

Program Studi Informatika

MUHAMMAD BINTANG ELAN YUSYAFI

NIM 20106050011

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA

2024

PENGESAHAN TUGAS AKHIR

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-2302/Un.02/DST/PP.00.9/12/2024

Tugas Akhir dengan judul : Implementasi Tunneling menggunakan Wireguard Untuk Membangun Fasilitas Laboratorium Komputer Online

yang dipersiapkan dan disusun oleh:

Nama : MUHAMMAD BINTANG ELAN YUSYAFI
Nomor Induk Mahasiswa : 20106050011
Telah diujikan pada : Kamis, 12 Desember 2024
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 67614c26e8582

Penguji I

Mandahadi Kusuma, M.Eng.
SIGNED

Valid ID: 67620fb23206f

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 6760fe1882be6

Yogyakarta, 12 Desember 2024
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6763797577a86

SURAT PERNYATAAN KEASLIAN

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Muhammad Bintang Elan Yusyafi
NIM	: 20106050011
Program Studi	: Informatika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 9 Desember 2024

Muhammad Bintang Elan Yusyafi

NIM. 20106050011

SURAT PERSETUJUAN TUGAS AKHIR

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhammad Bintang Elan Yusyafi
NIM : 20106050011
Judul Skripsi : Implementasi Tunneling Menggunakan Wireguard Untuk Membangun Fasilitas Laboratorium Komputer Online

sudah dapat diajukan kembali kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 9 Desember 2024

Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM.
NIP. 19751024200912100 2

LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.

INTISARI

Penelitian ini membahas implementasi WireGuard sebagai solusi VPN tunneling untuk meningkatkan aksesibilitas dan keamanan jaringan pada laboratorium komputer di UIN Sunan Kalijaga. Sebelum implementasi, pengguna hanya dapat mengakses sumber daya laboratorium melalui jaringan lokal, yang membatasi fleksibilitas dan efisiensi kerja. WireGuard dipilih karena keunggulannya dalam kecepatan, keamanan, dan kemudahan konfigurasi. Proses implementasi melibatkan pengaturan WireGuard Server, penggunaan WireGuard UI untuk manajemen klien, serta konfigurasi jaringan dengan sertifikat SSL untuk memastikan keamanan akses.

Pengujian dilakukan dengan menghubungkan klien dari jaringan publik ke server laboratorium menggunakan WireGuard. Hasil pengujian menunjukkan bahwa koneksi VPN berhasil terjalin dengan stabil dan aman, memungkinkan pengguna mengakses sumber daya laboratorium dari luar jaringan lokal. Setelah implementasi WireGuard, sistem menunjukkan peningkatan signifikan dalam aksesibilitas, fleksibilitas, dan efisiensi operasional. Pengguna dapat mengakses sumber daya laboratorium dengan latensi yang rendah, stabilitas koneksi yang baik, serta keamanan data yang terjamin melalui enkripsi yang kuat. Hal ini juga membuka potensi pengembangan lebih lanjut untuk mendukung akses jaringan yang lebih luas.

Penelitian ini menyimpulkan bahwa WireGuard mampu memberikan solusi efektif untuk mengatasi keterbatasan akses jaringan lokal. Saran pengembangan ke depan mencakup optimalisasi lebih lanjut dari konfigurasi dan eksplorasi potensi WireGuard dalam skenario jaringan yang lebih kompleks.

Kata kunci : WireGuard, VPN Tunneling, WireGuard UI, Laboratorium computer.

ABSTRACT

This study examines the implementation of WireGuard as a VPN tunneling solution to enhance network accessibility and security in the computer laboratory at UIN Sunan Kalijaga. Prior to the implementation, users could only access laboratory resources through a local network, limiting flexibility and operational efficiency. WireGuard was chosen for its advantages in speed, security, and ease of configuration. The implementation process involved setting up a WireGuard server, utilizing WireGuard UI for client management, and configuring the network with SSL certificates to ensure secure access.

Testing was conducted by connecting clients from a public network to the laboratory server using WireGuard. The results showed that the VPN connection was successfully established with stability and security, enabling users to access laboratory resources from outside the local network. Following the implementation of WireGuard, the system demonstrated significant improvements in accessibility, flexibility, and operational efficiency. Users were able to access laboratory resources with low latency, stable connections, and robust data security through strong encryption. This also opened further development potential to support broader network access.

This study concludes that WireGuard provides an effective solution to overcome the limitations of local network access. Future development suggestions include further optimization of configurations and exploration of WireGuard's potential in more complex network scenarios.

Keywords : WireGuard, VPN Tunneling, WireGuard UI, Computer Laboratory.

PERSEMBAHAN

Karya ini dipersembahkan untuk:

Kedua orang tua penulis

Ayahanda Syafiq Mahmadah Hanafi

Ibunda Yuniati Faizah

KATA PENGANTAR

Penulis mengucapkan puji dan syukur kepada Allah Swt. karena telah melimpahkan berkah dan nikmat yang tidak terhingga, sehingga tugas akhir "Implementasi Tunneling Menggunakan Wireguard Untuk Membangun Fasilitas Laboratorium Komputer Online" dapat diselesaikan. Tugas akhir ini juga dapat diselesaikan atas bantuan berbagai pihak. Untuk itu penulis ingin menyampaikan terima kasih kepada semua pihak yang berjasa berikut ini.

1. Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., selaku dosen pembimbing skripsi yang selalu bersedia meluangkan waktu untuk memberikan arahan, bimbingan, dan motivasi untuk menyelesaikan dan menyempurnakan penulisan tugas akhir ini;

2. Mandahadi Kusuma, M.Eng., selaku yang senantiasa membantu dan mengarahkan penulis selama berada di bangku perkuliahan;

3. Eko Hadi Gunawan, M.ENG.selaku dosen pembimbing penasehat akademik yang senantiasa membantu dan mengarahkan penulis selama berada di bangku perkuliahan;

4. Bapak dan Ibu dosen pada Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta, yang telah memberikan banyak ilmu;

5. Ibunda Yuniati Faizah, yang selalu memberi dukungan dan do'a serta dorongan agar tugas akhir ini cepat terselesaikan;

6. Ayahanda Syafiq Mahmadah Hanafi, yang tidak pernah berhenti berdo'a untuk kebaikan anaknya;

7.Sahabat yang tergabung di dalam koalisi tronjal tronjol, Setiawan, Satria, Tegar, Fajar, dan Ammar yang tidak lelah membersamai, menyangati, dan memotivasi;

Akhirnya, besar harapan penulis agar tugas akhir ini dapat memberikan kontribusi positif dalam kajian ilmu informatika. Penulis menyadari banyak kekurangan yang terdapat di dalam tugas akhir ini. Oleh sebab itu, penulis menerima kritik dan saran yang membangun sebagai upaya perbaikan dan pengembangan ke arah yang lebih baik.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju ini, teknologi informasi dan komunikasi telah menjadi tulang punggung utama dalam berbagai aspek kehidupan, termasuk dalam dunia pendidikan. Proses pembelajaran yang dahulu bergantung pada interaksi tatap muka secara fisik kini mulai bertransformasi menuju metode yang lebih fleksibel dan terdesentralisasi. Salah satu inovasi yang mendukung perubahan ini adalah kemampuan untuk mengakses laboratorium jaringan komputer secara online[1]. Dengan adanya fasilitas ini, siswa, mahasiswa, serta pengajar dapat mengakses perangkat dan perangkat lunak yang tersedia di laboratoriumoratorium dari jarak jauh, tanpa perlu kehadiran fisik[2]. Hal ini tidak hanya menghemat waktu dan sumber daya, tetapi juga memberikan fleksibilitas yang lebih besar dalam proses pembelajaran.

Laboratorium komputer online bisa menjadi opsi dalam dunia pendidikan modern[3], terutama ketika akses ke laboratorium jaringan komputer fisik di kampus tidak memungkinkan. Kondisi ini sering terjadi, misalnya, mahasiswa melakukan penelitian yang membutuhkan akses 24 jam, atau pada saat hari libur dan jam operasional laboratorium jaringan komputer yang terbatas. Selain itu, laboratorium jaringan komputer online juga memainkan peran penting dalam mendukung pembelajaran jarak jauh, memberikan akses tanpa batas kepada para mahasiswa untuk terus berlatih dan mengembangkan keterampilan teknologi mereka tanpa terhalang oleh batasan waktu dan lokasi.

Teknologi VPN (Virtual Private Network) telah lama digunakan sebagai solusi untuk menciptakan koneksi yang aman di atas jaringan publik[4]. Dengan VPN, pengguna dapat terhubung ke jaringan kampus seolah-olah mereka berada di lokasi fisik yang sama, meskipun sebenarnya mereka mengakses dari jarak jauh. Tunneling,

salah satu komponen utama dalam VPN, memungkinkan data yang dikirimkan melalui jaringan publik dilindungi dengan lapisan enkripsi, sehingga data tersebut aman dari intersepsi atau manipulasi oleh pihak yang tidak berwenang[5]

WireGuard adalah solusi VPN lintas platform pada layer 3 yang dirancang untuk menggantikan solusi VPN berbasis SSL yang umum digunakan. Dengan fokus pada keamanan, kemudahan penggunaan, dan performa yang lebih baik, WireGuard menawarkan keunggulan dibandingkan teknologi lama seperti OpenVPN[6]. WireGuard memiliki pendekatan yang minimalis namun sangat efektif. Dengan hanya sekitar 4.000 baris kode saja. WireGuard adalah protokol komunikasi sumber terbuka yang dirancang untuk menciptakan jaringan VPN terenkripsi yang ringan. Dengan memerlukan konfigurasi minimal dari pengguna, protokol ini mudah diimplementasikan. Setiap peer dalam jaringan diidentifikasi melalui pasangan kunci, di mana pengguna bertanggung jawab untuk menukar kunci publik mereka dengan peer lain dan mengonfigurasi endpoint peer dengan alamat yang benar. WireGuard memanfaatkan algoritma kriptografi canggih, termasuk ChaCha20 untuk enkripsi simetris, Poly1305 untuk otentikasi, Curve25519 untuk protokol kesepakatan kunci Diffie-Hellman, serta SipHash24 dan BLAKE2 untuk manajemen kunci pribadi[2].

Perangkat lunak yang berada didalam laboratorium jaringan komputer dapat di akses atau di gunakan dari luar jaringan atau jaringan publik ialah dengan menggunakan teknologi tunnel atau bisa disebut tunneling, tunneling sendiri merupakan teknik yang memungkinkan data bergerak melalui jaringan dengan membungkus, atau encapsulating, data dalam protokol lain. Ini memungkinkan data bergerak melalui jaringan dengan aman dan efektif. Tunneling adalah proses membuat jalur komunikasi virtual yang memungkinkan pertukaran informasi antara dua atau lebih lokasi yang terpisah, baik secara fisik maupun logis, dalam jaringan komputer. Sementara jalur ini, yang sering disebut sebagai "tunnel", memiliki kemampuan untuk melalui jaringan publik seperti internet, ia tetap menjaga kerahasiaan dan keamanan data yang ditransmisikan[7].

Laboratorium jaringan komputer (jarkom) di Universitas Islam Negeri (UIN) Sunan Kalijaga memiliki sumber daya komputasi yang secara aktif dimanfaatkan oleh mahasiswa untuk menyelesaikan berbagai tugas dan proyek akademik. Namun, salah satu kendala utama dari sumber daya ini adalah aksesibilitasnya yang terbatas hanya dalam lingkungan jaringan internal kampus. Hal ini mengakibatkan pemanfaatannya hanya dapat dilakukan secara langsung di lokasi dan dalam jam operasional tertentu dan hari kerja saja, sehingga mengurangi fleksibilitas mahasiswa dalam mengakses fasilitas tersebut sesuai kebutuhan.

Untuk mengatasi keterbatasan ini, teknologi tunneling dapat menjadi solusi strategis. Teknologi ini memungkinkan koneksi jarak jauh yang aman dan terenkripsi[8], sehingga sumber daya komputasi di laboratorium jaringan komputer dapat diakses oleh mahasiswa dari luar jaringan kampus[9]. Implementasi tunneling tidak hanya meningkatkan fleksibilitas, tetapi juga memaksimalkan pemanfaatan sumber daya laboratorium jaringan komputer dengan memperluas cakupan akses hingga di luar jam kerja[10]. Dengan demikian, mahasiswa dapat mengakses laboratorium kapan saja sesuai kebutuhan, tanpa terikat pada lokasi fisik atau jadwal tertentu, sehingga mendukung efisiensi dan produktivitas dalam proses belajar.

1.2 Rumusan Masalah

1. Bagaimana implementasi WireGuard sebagai VPN tunneling dapat memungkinkan akses laboratorium jaringan komputer di luar jam kerja?
2. Apa saja langkah yang diperlukan untuk membangun fasilitas laboratorium jaringan komputer online menggunakan WireGuard?
3. Sejauh mana solusi wireguard ini dapat meningkatkan aksesibilitas dan efisiensi penggunaan laboratorium?

1.3 Batasan

Penelitian ini menambahkan beberapa batasan masalah agar fokus penelitian tidak bergeser dan tidak menyebar. Beberapa batasan masalah yang ditambahkan adalah sebagai berikut:

1. Penelitian ini hanya akan fokus pada implementasi tunneling menggunakan protokol Wireguard sebagai teknologi utama yang digunakan untuk membangun fasilitas laboratorium online
2. Teknologi tunneling yang digunakan hanya wireguard
3. Penelitian ini hanya terhubung dengan satu server aktif
4. Wireguard server di install di linux
5. Pengujian hanya menggunakan 1 pengguna
6. Penelitian ini tidak akan mencakup analisis mendalam terkait aspek keuangan atau kelayakan bisnis dari implementasi Wireguard dalam konteks fasilitas laboratorium jaringan komputer online

1.4 Tujuan

Tujuan dari penelitian ini adalah untuk mengimplementasikan Tunneling pada laboratorium jaringan kompter agar laboratorium tersebut tidak hanya dapat diakses dari jaringan local, namun juga bisa digunakan dari luar jaringan. Model sistem seperti ini diharapkan mempu menjadi solusi atas terbatasnya waktu akses terhadap sumber daya laboratorium. Dengan demikian tingkat kegunaan laboratorium jaringan komputer sebagai fasilitas penelitian meningkat dan lebih efektif.

1.5 Manfaat

Mahasiswa dan dosen dapat mengakses laboratorium jaringan komputer secara online, Dan Dengan adanya penelitian ini penulis dapat memberikan manfaat kepada pembaca yang ingin mencari solusi untuk membangun fasilitas laboratorium online menggunakan wireguard.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan dan pengujian yang telah dilakukan dalam penelitian dengan judul "IMPLEMENTASI TUNNELING MENGGUNAKAN WIREGUARD UNTUK MEMBANGUN FASILITAS LABORATORIUM KOMPUTER ONLINE," dapat disimpulkan sebagai berikut:

1. Penerapan WireGuard sebagai solusi VPN tunneling telah berhasil memperluas cakupan akses laboratorium jaringan komputer. Kini, akses yang sebelumnya terbatas hanya pada jaringan lokal telah diperluas hingga mencakup jaringan publik. Dengan demikian, mahasiswa dan dosen dapat memanfaatkan fasilitas laboratorium tanpa terikat oleh batasan waktu operasional, termasuk di luar jam kerja. Hal ini memberikan fleksibilitas yang lebih besar bagi para pengguna untuk menjalankan penelitian, pembelajaran, atau tugas lainnya dengan efisien, terlepas dari lokasi fisik mereka.
2. membangun fasilitas laboratorium jaringan komputer online menggunakan WireGuard mencakup beberapa tahapan penting. Tahapan tersebut meliputi pengaturan WireGuard Server sebagai inti dari sistem VPN, konfigurasi sertifikat SSL untuk memastikan keamanan akses, serta penggunaan WireGuard UI untuk manajemen klien yang lebih efisien. Implementasi ini berhasil mengubah akses laboratorium yang sebelumnya terbatas pada jaringan lokal menjadi dapat diakses melalui jaringan publik. Hasil pengujian menunjukkan bahwa sistem yang dibangun mampu memberikan akses yang aman, stabil, dan fleksibel, sehingga meningkatkan efisiensi dan

kegunaan fasilitas laboratorium bagi mahasiswa dan dosen, termasuk di luar jam operasional.

3. Solusi yang diterapkan melalui implementasi WireGuard sebagai VPN tunneling terbukti secara signifikan meningkatkan aksesibilitas dan efisiensi penggunaan laboratorium jaringan komputer. Sebelum implementasi, akses laboratorium terbatas pada jaringan lokal, yang membatasi penggunaannya di luar jam operasional. Setelah implementasi, pengguna, termasuk mahasiswa dan dosen, dapat mengakses sumber daya laboratorium dari jaringan publik kapan saja dengan koneksi yang stabil, aman, dan efisien. Dengan demikian, solusi ini berhasil mengatasi keterbatasan sebelumnya, meningkatkan fleksibilitas penggunaan, serta mendukung penelitian dan pembelajaran dengan lebih optimal.

5.2 Saran

Penelitian ini masih memiliki sejumlah keterbatasan yang dapat ditingkatkan di masa mendatang. Potensi penggunaan WireGuard sebagai protokol VPN Tunneling sangat luas dan belum sepenuhnya dieksplorasi dalam penelitian ini. Oleh karena itu, diperlukan upaya pengembangan lebih lanjut agar semua fitur dan kapabilitas yang dimiliki WireGuard dapat dimanfaatkan secara optimal. Pengembangan lanjutan ini diharapkan mampu menghadirkan solusi yang lebih komprehensif, efektif, dan sesuai dengan kebutuhan pengguna serta kondisi jaringan yang terus berkembang.

1. Pengujian dengan Skala Lebih Besar, Penelitian di masa mendatang dapat memperluas skala pengujian dengan melibatkan lebih banyak pengguna dan perangkat untuk menguji stabilitas dan performa sistem dalam kondisi beban tinggi.
2. Optimalisasi Kinerja dan Keamanan WireGuard, Disarankan untuk melakukan pengujian lebih lanjut terkait kinerja dan keamanan

WireGuard dalam berbagai skenario jaringan. Fokus pada pengaturan keamanan tambahan, seperti penggunaan firewall dan monitoring trafik, dapat meningkatkan perlindungan data pengguna.

3. Pengujian Skala Besar dan Latensi Jaringan, Penelitian lanjutan bisa mencakup pengujian pada skala pengguna yang lebih besar untuk mengukur latensi, throughput, dan stabilitas koneksi, sehingga dapat menilai kemampuan WireGuard dalam menangani trafik yang tinggi.

Daftar pustaka

[1] H. Rachmah, “BLENDED LEARNING: MEMUDAHKAN ATAU MENYULITKAN?,” vol. 3, 2019.

[2] M. Valks, “Peer-to-peer VPN solution for eduVPN using WireGuard”.

[3] L. Nasution, “Pengaruh Teknologi pada Dunia Pendidikan,” vol. 3, no. 1, 2024.

[4] R. Mujiastuti and I. Prasetyo, “Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE”.

[5] B. F. Audrey, “Virtual Private Network Menggunakan Point To Point Tunnel Protocol Berbasis Mikrotik,” vol. 1, no. 1, 2022.

[6] S. Saukkonen, “Implementing WireGuard to a home office environment”.

[7] V. Mulder, A. Mermoud, V. Lenders, and B. Tellenbach, Eds., *Trends in Data Protection and Encryption Technologies*. Cham: Springer Nature Switzerland, 2023. doi: 10.1007/978-3-031-33386-6.

[8] N. Bayu and A. Susila, “Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan VPN Berbasis SSL-VPN (Studi Kasus: Kementerian PANRB),” vol. 2, no. 1, 2023.

[9] E. Mufida, D. Irawan, and G. Chrisnawati, “Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta,” *Matrik*, vol. 16, no. 2, p. 9, Jul. 2017, doi: 10.30812/matrik.v16i2.7.

[10] M. Arif and A. S. Budiman, “Interkoneksi Site-to-Site dan Remote Access Menggunakan Virtual Private Network dan IP Security,” *JSI*, vol. 12, no. 1, Apr. 2020, doi: 10.36706/jsi.v12i1.9413.

[11] K. A. Farly, X. B. N. Najoan, and A. S. M. Lumenta, “Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi”.

[12] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, “Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan,” *komtekinfo*, pp. 169–175, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.128.

[13] I. K. S. Satwika, “ANALISIS QUALITY OF SERVICE JARINGAN VIRTUAL PRIVATE NETWORK (VPN) DI STMIK STIKOM INDONESIA,” *oai*, vol. 7, no. 01, p. 60, Mar. 2019, doi: 10.33884/jif.v7i01.1016.

[14] “What is tunneling? | Tunneling in networking.” Accessed: Nov. 20, 2024. [Online]. Availaboratoriumle: https://www.cloudflare.com/learning/network-layer/what-is-tunneling/

[15] “WireGuard: fast, modern, secure VPN tunnel.” Accessed: Nov. 20, 2024. [Online]. Availaboratoriumle: https://www.wireguard.com/

[16] J. A. Donenfeld, “WireGuard: Next Generation Kernel Network Tunnel,” in *Proceedings 2017 Network and Distributed System Security Symposium*, San Diego, CA: Internet Society, 2017. doi: 10.14722/ndss.2017.23160.