IMPLEMENTASI *SECURE SOCKET TUNNELING PROTOCOL* (SSTP) UNTUK KEAMANAN DATA PADA JARINGAN KOMPUTER

PROJEK

Sebagai salah satu syarat untuk menyelesaikan studi di

Program Studi Teknik Komputer DIII

Oleh :

Rifki Firmansyah

09040581822014

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

JULI 2023

HALAMAN PENGESAHAN

IMPLEMENTASI *SECURE SOCKET TUNNELING PROTOCOL* (SSTP) UNTUK KEAMANAN DATA PADA JARINGAN KOMPUTER

PROJEK

Sebagai salah satu syarat untuk penyelesaian studi di Program Studi Teknik Komputer DIII

Oleh :

Rifki Firmansyah
NIM 09040581822014

Palembang, 31 Juli 2023

Pembimbing I,	**Pembimbing II,**
Ahmad Heryanto, M.T.	**Adi Hermansyah, M.T.**
NIP 198701222015041002	**NIK 1613033004890001**

Mengetahui
Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Jum'at**

Tanggal : **28 Juli 2023**

Tim Penguji :

1. Ketua : Aditya Putra P P, M.T.
2. Pembimbing I : Ahmad Heryanto, M.T.
3. Pembimbing II : Adi Hermansyah, M.T.
4. Penguji : Nurul Afifah, M.Kom.

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.

NIP 198106162012121003

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: Rifki Firmansyah
NIM	: 09040581822014
Program Studi	: Teknik Komputer
Peminatan	: Teknik KomputerJaringan
Judul	: Implementasi Secure Socket Tunneling Protocol (SSTP) Untuk Keamanan Data Pada Jaringan Komputer

Hasil Pengecekan Software iThenticate/Turnitin : 17%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 31 Juli 2023

Rifki Firmansyah

NIM 09040581822014

HALAMAN PERSEMBAHAN

MOTTO

وَمَنْ يَتَّقِ اللَّهَ يَجْعَلْ لَهُ مَخْرَجًا وَيَرْزُقْهُ مِنْ حَيْثُ لَا يَحْتَسِبُ

Barang siapa yang bertakwa kepada Allah, niscaya Dia akan mengadakan baginya jalan keluar, dan memberinya rezeki dari arah yang tiada disangka-sangkanya. – (QS. At-Thalaq: 2-3)

مَنْ جَدَّ وَجَدَ

"Barang siapabersungguh-sungguh, makaiaakanberhasil."

Alhamdulillah bersyukur kepada Allah Subhanahu Wata'ala atas nikmat dan kesempatan, sehingga dapat terselesaikan sedikit karya saya yang akan kupersembahkan untuk…

Kedua orang tua tercinta

(Bapak Makruf dan Ibu Suparmi)

Kedua saudaraku tercinta

(M. Ali Basnakir dan M. Amirrullah)

Teman-teman seperjuanganku

(Teknik KomputerJaringan 2018)

Almamater perjuangan

(Universitas Sriwijaya)

Juli 2023

KATA PENGANTAR

Segala puji dan syukur penulis ucapkan kepada Allah SWT, karena berkat nikmat rahmat dan karunia-Nyalah penulis dapat menyelesaikan penulisan projek akhir dengan judul "**IMPLEMENTASI SECURE SOCKET TUNNELING PROTOCOL (SSTP) UNTUK KEAMANAN DATA PADA JARINGAN KOMPUTER**". Penulisan projek akhir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan di Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperolehgelar Ahli Madya Komputer.

Pada kesempatan ini, penulis mengucapkan terima kasih kepada seluruh pihak yang telah membantu, membimbing, dan terus mendukung penulis dalam menyelesaikan laporan kerja praktik ini di antaranya:

1. Allah SWT, yang selalu memberikan rencana dan jalan yang terbaik, mempermudah segala urusan, yang telah memberikan kesehatan, ilmu dan rizki yang tak dapat di hitung jumlahnya.
2. Nabi Muhammad SAW, yang mana mengingatnya membuat hati terasatenang, kata-kata dalam riwayat hadistnya selalu memberikan semangat serta motivasi untuk terus menuntutilmu dan berlomba dalam kebaikan.
3. Kedua Orang tua, ketiga saudara, serta keluarga tercinta, yang senantiasa untuk mendidik serta memberikan dukungan kepada penulis dalam menyelesaikan projek akhir.
4. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing I Projek Akhir, yang telah memberikan bimbingan dan semangat kepada penulis dalam menyelesaikan projek akhir.
5. Bapak Adi Hermansyah, S.Kom., M.T. selaku Dosen Pembimbing II Projek Akhir, yang telah memberikan support dan referensi kepada penulis dalam menyelesaikan projek akhir.

6. Bapak Huda Ubaya, S.T., M.T. selaku Koordinator Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Sarmayanta Sembiring, S.Kom, M.T. selaku Dosen Pembimbing Akademik, yang telah membimbing dari awal masuk hingga selesainya projek akhir.
8. Seluruh Dosen Program Studi Teknik Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Staff di Program Studi Teknik Komputer, khususnya Mbak Faula yang selalu membantu menyelesaikan proses administrasi.
10. Keluarga Besar Fakultas Ilmu Komputer, bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan.
11. Seluruh Pimpinan yang ada di lingkungan Fakultas Ilmu Komputer, Universitas Sriwijaya.
12. Teman-teman seperjuangan angkatan 2018, Sukses selalu untuk kita semua.
13. Serta semua pihak yang telah membatu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian projek akhir ini. Terima kasih semuanya.

Semoga dengan terselesainya projek akhir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua dalamm mempelajari Impelentasi VLAN (Virtual Local Area Network) dan VAP (Virtual Access Point).

Dalam penulisan laporan ini, penulis menyadari bahwa masih banyak terdapat kekurangan dan ketidak sempurnaan, oleh karena itu penulis mohon saran dan kritik yang membangun untuk perbaikan laporan projek akhir ini, agar menjadi lebih baik dimasa yang akan datang.

Palembang, 31 Juli 2023

(Rifki Firmansyah)

IMPLEMENTASI SECURE SOCKET TUNNELING PROTOCOL (SSTP) UNTUK KEAMANAN DATA PADA JARINGAN KOMPUTER

Oleh :

Rifki Firmansyah
09040581822014

Abstrak

Membangun metode secure socket tunneling protocol untuk mengakses layanan port pada routerboard MikroTik. Membatasi port yang mudah di akses remote routerboard MikroTik. Mengetahui langkah-langkah dari metode secure socket tunneling protocol Virtual Private Network (VPN) merupakan salah satucara untuk melindungi pertukaran data informasi penting melalui jaringan internet, khususnya dengan menggunakan metode protokol Secure Socket Tunneling Protokol (SSTP) dapat membuat komunikasi antar beberapa jaringan melalui sebuah Tunneling yang melewati jaringan internet menjadi lebih aman Menggunakan metode pengumpulan data atau informasi dari berbagai sumber seperti jurnal, buku, web, dan dari informasi lainnya yang berhubungan dari penelitian projek ini yang berjudul implementasi secure socket tunneling protocol (SSTP) untuk keamanan data pada jaringan komputer. Hasilnya akan memperlihatkan berapa besar penurunan kecepatan yang terjadi saat koneksi melewati lapisan enkripsi. Pingflood mengukur bagaimana SSTP VPN menangani serangan "pingflood," yaitu mengirimkan sejumlah besar permintaan ping ke server secara bersamaan untuk mengganggu koneksi. Server VPN dapat berjalan dengan baik dengan kondisi yang berbeda-beda tergantung kecepatan dan jumlah paket data yang dikirimkan implementasi Secure Socket Tunneling Protocol (SSTP) adalah Lakukan optimasi pada konfigurasi SSTP VPN dan perangkat MikroTik untuk meningkatkan kinerja.

Kata Kunci : *secure socket tunneling protocol,Virtual Private Network, Pingflood*

IMPLEMENTATION OF SECURE SOCKET TUNNELING PROTOCOL (SSTP) FOR DATA SECURITY ON COMPUTER NETWORKS

By :

Rifki Firmansyah
09040581822014

Abstract

Building a secure socket tunneling protocol method to access port services on the MikroTikrouterboard. Limiting ports that are easy to access remotely on the MikroTikrouterboard. Knowing the steps of the secure socket tunneling protocol Virtual Private Network (VPN) method is one way to protect the exchange of important information data over the internet network, especially by using the Secure Socket Tunneling Protocol (SSTP) protocol method can make communication between multiple networks through a Tunneling through the internet network becomes more secure Using methods of collecting data or information from various sources such as journals, books, the web, and from other related information from this research project entitled implementation of secure socket tunneling protocol (SSTP) for data security on computer networks . The results will show how much speed decrease occurs when the connection passes through the encryption layer. Pingflood measures how an SSTP VPN handles a "pingflood" attack, which is sending a large number of ping requests to a server simultaneously to disrupt a connection. The VPN server can run well under different conditions depending on the speed and number of data packets sent. The implementation of Secure Socket Tunneling Protocol (SSTP) is to optimize the SSTP VPN configuration and MikroTik devices to improve performance.

Keywords: *secure socket tunneling protocol, Virtual Private Network, Pingflood*

DAFTAR ISI

Halaman

HALAMAN JUDUL i
HALAMAN PENGESAHAN ii
HALAMAN PERSETUJUAN iii
HALAMAN PERNYATAAN iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
Abstrak viii
Abstract ix
DATAR ISI x
DAFTAR GAMBAR xiii
DAFTAR TABEL xv
DAFTAR LAMPIRAN xvi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Tujuan 2
1.3 Manfaat 2
1.4 Rumusan Masalah 2
1.5 Batasan Masalah 3
1.6 Metodologi Penelitian 3
1.7 Sistematika Penelitian 4
BAB II LANDASAN TEORI 5
2.1 Keamanan Komputer 5
2.1.1 Fungsi Keamanan Komputer 5
2.2 Model Referensi OSI 5
2.2.1 Karakteristik Lapisan OSI 6
2.2.2 OSI Layer 7
2.3 TCP/IP *(Transmision Control Protocol) / (Internet Protocol)* 9

2.4 VPN (Virtual Private Network) 9
2.4.1 Fungsi VPN 10
2.5 Tunneling 11
2.6 SSTP (Secure Socket Tunneling Protocol) 11
2.6.1 Karakteristik *Port SSTP* 12
2.6.2 Cara Kerja SSTP 12
2.7 *Router* 13
2.8 Mikrotik 13
2.8.1 Sejarah Mikrotik 13
2.8.2 Macam-macam Mikrotik 14
2.8.3 Mikrotik RB951-2nD 14
2.10 Winbox 15
BAB III METODOLOGI PENELITIAN 16
3.1 Kerangka Kerja Penelitian 16
3.2 Perancangan Sistem 17
3.2.1 Perancangan Topologi 17
3.2.2 Desain Topologi 17
3.2.3 Pengalamatan IP Topologi Penelitian 18
3.2.4 Komponen Perangkat Keras 18
3.2.5 Komponen Perangkat Lunak 19
3.2.6 Setting Certificate CA (Certificate Authority) 20
3.2.7 Konfigurasi PPP Secret 25
3.3 Skenario Pengujian Implementasi SSTP (*Secure Socket TunnelingProtocol)* 26
3.3.1 Skenario Pengujian Ping Speed 27
3.3.2 Skenario Pengujian Pingflood 28
3.3.3 Pengujian Packet Loss 28
3.3.4 Skenario Pengambilan Data 28
3.4 Flowchart Skenario SSTP (Secure Socket Tunneling Protocol). 29
BAB IV HASIL DAN PEMBAHASAN 30
4.1 Pendahuluan 30
4.2 VPN 30

4.3 Tahapan Pengujian *Ping Speed* MikroTik 31
4.3.1 Ping Speed Server 31
4.3.2 Ping Speed Client 32
4.3.3 Hasil Pengujian Ping Speed 32
4.4 Tahapan Pengujian Pingflood 32
4.4.1 Pingflood IP Server 33
4.4.2 Pingflood IP Client 34
4.4.3 Hasil Pengujian Pingflood 35
4.5 Tahapan Pengujian Ping Terminal 35
BAB V KESIMPULAN DAN SARAN 37
5.1 Kesimpulan 37
5.2 Saran 37
DAFTAR PUSTAKA 38
LAMPIRAN 40

DAFTAR GAMBAR

Halaman

Gambar 2.1 KarakteristikLapisan OSI Layers 6
Gambar 2.2 Lapisan OSI layer 7
Gambar 2.3 TCP/IP (*Transmision Control protocol/Internet Protocol*) 9
Gambar 2.4 KonsepIlustrasi Tunneling 11
Gambar 2.5 Cara Kerja SSTP 12
Gambar 2.6 Mikrotik RB951Ui-2ND 14
Gambar 2.7AplikasiWinbox 15
Gambar 3.1 Flowchart KerangkaKerjaPenelitian 16
Gambar 3.2 Desain Topologi*Secure Socket Tunneling Protocol* (SSTP) 17
Gambar 3.3 Konfigurasi CA (Certificate Authority) 20
Gambar 3.4 Key Usage 20
Gambar 3.5 Konfigurasi Certificate Client 21
Gambar 3.6 Konfigurasi Certificate Server 21
Gambar 3.7 *Certificate* 22
Gambar 3.8 *Export Certificate* 23
Gambar 3.9 MMC (Microsoft Management Console) 24
Gambar 3.10 *Import Certificates* 24
Gambar 3.11 SSTP Server 25
Gambar 3.12 Konfigurasi PPP Secret 26
Gambar 3.13 Proses PengujianSSTP (*Secure Socket Tunneling Protocol)* 27
Gambar 3.14 Flowchart Skenario SSTP 29
Gambar 4.1 Konfigurasi VPN 30
Gambar 4.2 Connected to SSTP Mikrotik 30
Gambar 4.3 Client di Server 31

Gambar 4.4 Ping Speed Server 31
Gambar 4.5 Ping Speed Client 32
Gambar 4.6 Pingflood IP Server 33
Gambar 4.7 Hasil Pingflood IP server 33
Gambar 4.8 Pingflood IP Client 34
Gambar 4.9 Hasil Pingflood IP Client 34
Gambar 4.10 IP Percobaan Ping ke Server 35
Gambar 4.11 Percobaan Ping IP Client 36

DAFTAR TABEL

Halaman

Tabel 3.1 IP Address Topologi..... 18
Tabel 3.2 KomponenPerangkatKeras 18

DAFTAR LAMPIRAN

Halaman

Lampiran 1 - SKTA 40
Lampiran 2 - Kartu Konsul Pembimbing 1 41
Lampiran 3 - Kartu Konsul Pembimbing 2 43
Lampiran 4 - Hasil Pengecekan Turnity 45
Lampiran 5 - From Revisi Penguji 46
Lampiran 6 - From Revisi Pembimbing 1 47
Lampiran 7 - From Revisi Pembimbing 2 48

BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan pada dunia Teknologi dan Informasi sekarang ini jauh lebih pesat terutamanya pada dunia internet, yang memungkinkan banyak sekali aktifitas pada manusia dapat diselesaikan dengan cepat berkat adanya bantuan teknologi internet tersebut. Pertukaran informasi dari satutempat ke tempat yang lain menjadi sangat mudah dan lebih cepat dengan adanya internet [1].

Namun dari segi keamanan meskipun internet memiliki berbagai jenis *protocol* keamanan tetapi masih ada saja orang – orang atau dari kelompok tertentu yang dapat menembus ke dalam sistem keamanan sehingga dapat terjadi suatu pencurian data dan informasi yang sangat penting.

Misalnya seperti di lembaga pemerintahan, perusahaan, atau universitas begitu banyak informasi penting yang dapat dicuri oleh orang yang tidak bertanggung jawab,tentu saja hal ini sangat merugikan pihak tersebut,sehingga dibutuhkan suatu cara atau metode yang dapat mengurangi bahkan menghilangkan berbagai jenis tindak kejahatan pencurian data dan informasi penting yang dapat dilakukan melalui jaringan internet [2].

Virtual Private Network (VPN) merupakan salah satu cara untuk melindungi pertukaran data informasi penting melalui jaringan internet, khususnya dengan menggunakan metode protocol *Secure Socket Tunneling Protokol* (SSTP) dapat membuat komunikasi antar beberapa jaringan melalui sebuah *Tunneling* yang melewati jaringan internet menjadi lebih aman[3].

Teknologi VPN mempunyai system kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi *enkripsi*, maka kerahasiaan klien menjadi lebih terjaga walaupun ada pihak yang dapat menyadap data klien yang lalu-lalang, tapi belum tentu bias dibaca dengan mudah karena memang sudah diacak [4]. Dengan menerapkan system enkripsi, tidak ada yang dapat mengakses dan membaca isi jaringan data klien dengan mudah.

Berdasarkan pembahasan latar belakang penulis bermaksud untuk membuat penelitian sebagai laporan akhir yang berjudulkan“Implementasi *Secure Socket Tunneling Protocol (SSTP)* Untuk Keamanan Data Pada Jaringan Komputer”. Tujuan dari penelitian ini guna meningkatkan keamanan dengan membangun sebuah *virtual private network* pada MikroTik dengan menggunakan metode *secure socket tunneling protocol* untuk melindungi data informasi penting dan membatasi hak akses, sehingga hanya *user* tertentu yang dapat mengakses *server* secara penuh.

1.2 Tujuan

Tujuan daripenulisan dan pembuatanprojek ini adalah:

1. Membangun metode *secure socket tunneling protocol* untuk mengakses layanan *port* pada *routerboard* MikroTik.
2. Membatasi *port* yang mudah di akses *remote routerboard* MikroTik.
3. Mengetahui langkah-langkah dari metode *secure socket tunneling protocol.*

1.3 Manfaat

Manfaat daripenulisan dan pembuatanprojek ini adalah:

1. Meningkatkan keamanan layanan jaringan pada *routerboard* mikrotik agar terhindar dari penyalahgunaan data.
2. Mengurangi penyalah gunaan akses layanan *port* pada *routerboard* MikroTik.
3. Memberikan manfaat bagi penulis dari metode *secure socket tunneling protocol.*

1.4 RumusanMasalah

Rumusan masalah dari projek ini adalah:

1. Bagaimana cara mengimplementasikan *secure socket tunneling protocol.*
2. Bagaimana cara mengamankan layanan jaringan pada *routerboard* MikroTik.

1.5 Batasan Masalah

Penulis telah membatasi masalah dari projek ini adalah:

1. Membuat *rules* keamanan, hanya *user* yang telah ditentukan yang dapat memiliki akses masuk pada *router* MikroTik.
2. Menutup *port-port* yang penting pada *router* MikroTik dan hanya *user/client* yang telah mengetahui langkah-langkahnya yang dapat memasuki layanan jaringan tersebut.

1.6 MetodologiPenelitian

Dari projek ini diselesaikan dengan menggunakan urutan metodologi sebagai berikut:

1. Tahapan *Literature*

   Menggunakan metode pengumpulan data atau informasi dari berbagai sumber seperti jurnal, buku, web, dan dari informasi lainnya yang berhubungan dari penelitian projek ini yang berjudul implementasi *secure socket tunneling protocol (SSTP)*untuk keamanan data pada jaringan komputer.
2. Tahapan Konsultasi

   Tahap ini merupakan Tanya jawab dengan dosen pembimbing atau dengan dosen yang bersangkutan dengan tujuan untuk membatasi kesalahan yang ada pada laporan projek.
3. TahapanPerancangan

   Menjalankan simulasi dengan menerapkan secara langsung menggunakan alat yang dibutuhkan seperti *routerboard* Mikrotik dan alat lainnya, serta menguji coba dari penelitian projek ini.
4. Tahapan Hasil dan Kesimpulan

   Pada tahap ini menjelaskan mengenai hasil dari perancangan penelitian dan dapat mengambil kesimpulan dari pembuatan projek akhir yang telah dibuat.

1.7 SistematikaPenelitian

Untuk pembuatan projek adanya langkah-langkah penjelasan mengenai proses yang akan dilakukan pada setiap BAB yang ada, sebagai berikut:

BAB I PENDAHULUAN

Pada bagian awal dari projek ini merupakan bagian yang bersumber dari penelitian yang akan dibahas mengenai apa yang akan dikerjakan oleh seorang penulis.

BAB II TINJAUAN PUSTAKA

Pada bab ini merupakan dasar teori yang bersangkutan dengan projek yang dibahas yang berdasarkan sejarah dan pengertian yang dapat di buku, jurnal ataupun sumber yang berhubungan dari projek ini.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang perancangan dari penelitian yang akan dilakukan dari *flowchart,*topologi, struktur serta metodologi yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

pada bab ini merupakan hasil dari pembahasan yang telah dilakukan dan sistem yang diterapkan pada implementasi pada alat yang telah dipakai. Hasil berupa data yang telah dilakukan pada bagian sebelumnya.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan kesimpulan dan saran dari projek atau penelitian yang telah dilakukan mengenai pembahasan dari awal bab I pendahuluan hingga bab IV hasil implementasi dan uji coba.

DAFTAR PUSTAKA

[1] K. A. Farly, X. B. N. Najoan, and A. S. M. Lumenta, "Perancangan dan Implementasi VPN Server denganmenggunakanProtokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi," *Jurnal Teknik InformatikaUnsrat*, vol. 11, no. 1, p. 143279, 2017.

[2] I. Ruslianto, "Perancangan dan Implementasi Virtual Private Network (VPN) menggunakanProtokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura," *Computer Engineering, Science and System Journal*, vol. 4, no. 1, p. 74, 2019, doi: 10.24114/cess.v4i1.11792.

[3] L. Umaroh and M. Rifauddin, "Implementasi Virtual Private Network (Vpn) Di Perpustakaan Universitas Islam Malang," *Baca: JurnalDokumentasi Dan Informasi*, vol. 41, no. 2, p. 193, 2020, doi: 10.14203/j.baca.v41i2.531.

[4] R. Azhar, "Analisa Qos Pada Jaringan Site To Site Vpn," *Analisa Qos Pada Jaringan Site To Site VpnMenggunakan Protocol Sstp*, pp. 52–60, 2017.

[5] Yudi mulyanto, M. Julkarnain, and A. Jabi Afahar, "Implementasi Port Knocking Untuk KeamananJaringanSmkn 1 Sumbawa Besar," *JurnalInformatikaTeknologi dan Sains*, vol. 3, no. 2, pp. 326–335, 2021, doi: 10.51401/jinteks.v3i2.1016.

[6] A. Widodo, "Implementasi Metode Discovery Pada Game EdukasiKeamananJaringanKomputer," *IJNS – Indonesian Journal on Networking*, vol. 4345, no. 2, pp. 0–412, 2015.

[7] H. Wijoyo, *SistemInformaiManajemen*. 2021.

[8] A. P. Sujana, "PERANGKAT PENDUKUNG FORENSIK LALU LINTAS JARINGAN," 2014.

[9] M. Dody Firmansyah, "Analisa Keamanan Web Server terhadapSerangan Distributed Denial of Service menggunakanModevasive," *Telcomatics*, vol. 6, no. 1, pp. 2541–5867, 2021, doi: 10.37253/telcomatics.v6i1.4990.

[10] Onard, "jurnalGland".

[11] K. Anugrah, "Pengenalan Osi Layer Kata Kunci :Pengenalan Osi Layer," pp. 1–5, 2016.

[12] A. P. A. Kusuma and Asmunin, "Implementasi Simple Port Knocking Pada Dynamic Routing (OSPF) MenggunakanSimulasi GNS3," *JurnalManajemenInformatika*, vol. 5, no. 2, pp. 7–17, 2016.

[13] B. F. Audrey, "… Network Menggunakan Point To Point Tunnel Protocol BerbasisMikrotik: Virtual Private Network Menggunakan Point To Point Tunnel Protocol BerbasisMikrotik," *Journal of Network and Computer Applications (ISSN ...*, vol. 1, no. 1, pp. 1–8, 2022.

[14] K. Khotimah and K. M. Prabowo, "PenerapanLayanan Publik Menggunakan Secure Socket Tunneling Protokol (Sstp)," *Jurnal GERBANG STMIK Bani Saleh*, vol. 12, no. 2, pp. 27–40, 2022.

[15] J. AdministrasiJaringanKomputer*et al.*, "ImplementasiInterkoneksiJaringanDengan Virtual Private Network (Vpn) Berbasis Bridge Control Protocol (Bcp) Pada Mikrotik Di Kantor Upt PondokPesantren Darussalam Blokagung," 2023.

[16] A. Kartiko, "AnalisisPerbandingan Kinerja QosDengan Metode PPTP,L2TP, SSTP Dan IPSEC Pada Jaringan VPN DenganMenggunakanMikrotik Pada Kantor Badan Perwakilan Dan KependudukanKeluargaBerencana Nasional (BKKBN) Pekanbaru," *Repository Universitas Islam Riau*, 2022.

[17] Ridho, "Bab II Landasan Teori," *J Chem Inf Model*, vol. 53, no. 9, pp. 1689–1699, 2018.

[18] S. A. Panu and Musdalifa, "304760997," *JurnalPublikasi Pendidikan*, vol. 9, no. 1, pp. 28–41, 2019.

[19] N. K. Anwar, *Analisis dan PerancanganManajemenJaringandenganMenggunakanMikrotikRouterOS*. 2010.