ANALISA PERBANDINGAN ALGORITMA ENKRIPSI DATA PADA JARINGAN VIRTUAL PRIVATE NETWORK (VPN) (STUDI KASUS PT iFORTE GLOBAL INTERNET)

TUGAS AKHIR

AYU AZIZAH PUTRI
41517110093

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2021

ANALISA PERBANDINGAN ALGORITMA ENKRIPSI DATA PADA JARINGAN VIRTUAL PRIVATE NETWORK (VPN) (STUDI KASUS PT iFORTE GLOBAL INTERNET)

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
AYU AZIZAH PUTRI
41517110093

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2021

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	:	41517110093
Nama	:	Ayu Azizah Putri
Judul Tugas Akhir	:	Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet)

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 29 Agustus 2021

Ayu Azizah Putri

ii

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Ayu Azizah Putri
NIM	:	41517110093
Judul Tugas Akhir	:	Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet)

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 29 Agustus 2021

Ayu Azizah Putri

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Ayu Azizah Putri
NIM	:	41517110093
Judul Tugas Akhir	:	Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet)

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	✓
		Jurnal Nasional Terakreditasi	✓		
		Jurnal International Tidak Bereputasi		Diterima	
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: Jurnal Teknologi dan Sistem Komputer (JTSiskom)		
		ISSN	: 2338-0403		
		Link Jurnal	: https://jtsiskom.undip.ac.id/index.php/jtsiskom/author/submissionReview/14284		
		Link File Jurnal Jika Sudah di Publish	:		

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 29 Agustus 2021

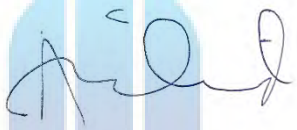
Ayu Azizah Putri

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517110093
Nama	:	Ayu Azizah Putri
Judul Tugas Akhir	:	Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet)

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 18 Agustus 2021



(Anis Cherid, SE, MTI)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517110093
Nama	:	Ayu Azizah Putri
Judul Tugas Akhir	:	Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet)

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 18 Agustus 2021

(Vina Ayumi, S.Kom., M.Kom)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517110093
Nama	:	Ayu Azizah Putri
Judul Tugas Akhir	:	Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet)

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 18 Agustus 2021

(Wawan Gunawan, S.Kom., MT)

LEMBAR PENGESAHAN

NIM	:	41517110093
Nama	:	Ayu Azizah Putri
Judul Tugas Akhir	:	Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet)

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 18 Agustus 2021

Menyetujui,

(Dr. Ida Nurhaida, MT)
Dosen Pembimbing

Mengetahui,

(Wawan Gunawan, S.Kom., MT)	(Herry Derajad Wijaya, S.Kom., MM)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

ABSTRAK

Nama	:	Ayu Azizah Putri
NIM	:	41517110093
Pembimbing TA	:	Dr. Ida Nurhaida, MT
Judul	:	Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet)

Jaringan komputer menjadi salah satu kebutuhan yang penting bagi kehidupan manusia untuk melakukan proses pertukaran data antar komputer di dalam instansi maupun diluar instansi. Jaringan VPN (*Virtual Private Network*) dibutuhkan untuk memberikan layanan koneksi akses secara *private* dimana data tersebut dienkapsulasi dengan header yang berisi informasi routing dan dienkripsi untuk menjaga kerahasiaan data. Penelitian ini dilakukan untuk menguji algoritma enkripsi data dengan parameter QoS (*Quality of Service*) yaitu *delay*, *throughput* dan *packet loss* pada jaringan VPN L2TP/IPSec. Nilai-nilai yang didapatkan dari parameter tersebut dibandingkan dengan standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Networks*) dengan tujuan untuk mengetahui algoritma enkripsi yang optimal. Setelah dilakukan proses perancangan jaringan, pengujian serta analisa, didapatkan hasil algoritma AES 256 unggul pada parameter *delay* dan *throughput*. Pada parameter *packet loss* algoritma 3DES memiliki nilai rata-rata *packet loss* yang lebih tinggi dibandingkan dengan algoritma AES 128 dan AES 256.

Kata kunci:
VPN, QoS, AES 256, AES 128, 3DES

ABSTRACT

Name	:	Ayu Azizah Putri
Student Number	:	41517110093
Counsellor	:	Dr. Ida Nurhaida, MT
Title	:	Comparative Analysis of Data Encryption Algorithms in Virtual Private Network (VPN) (Case Study of PT iForte Global Internet)

VPN (Virtual Private Network) network is one of the needs in the process of exchanging data between computers both inside and outside the agency that provides private access connections where the data is encapsulated with headers containing routing information and encrypted to maintain data confidentiality. This research was conducted to test the data encryption algorithm with QoS (Quality of Service) parameters delay, throughput, and packet loss on the L2TP/IPSec. The values obtained from these parameters are compared with the TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) standard to determine the optimal encryption. After the process of network design, testing, and analysis, the results of the AES 256 algorithm has the best performance to the delay and throughput parameters. In the packet loss parameter, the 3DES algorithm has a higher average packet loss value than the AES 128 and AES 256 algorithms.

Key words:
VPN, QoS, AES 256, AES 128, 3DES

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Allah swt., karena atas karunia yang telah diberikan kepada penulis sehingga penulis dapat menyelesaikan Laporan Tugas Akhir tepat waktu, dimana Laporan Tugas Akhir ini merupakan salah satu persyaratan untuk dapat menyelesaikan Program Studi Strata Satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa Laporan Tugas Akhir ini masih belum dapat dikatakan sempurna. Karena itu, kritikan dan saran yang membangun sangat penulis harapkan demi sempurnanya laporan ini kedepan. Penulis juga menyadari bahwa Laporan Tugas Akhir ini tidak dapat selesai tepat pada waktunya tanpa bantuan, bimbingan, dan motivasi dari berbagai pihak. Ucapan terima kasih ini penulis tujukan kepada:

1. Ibu Dr. Ida Nurhaida, MT selaku Dosen Pembimbing Tugas Akhir yang telah membimbing penulis dengan semua nasihat, semangat dan ilmunya dalam menyusun laporan tugas akhir ini.
2. Bapak Herry Derajad Wijaya, S.Kom., MM selaku Kepala Program Studi Informatika Universitas Mercu Buana.
3. Bapak Wawan Gunawan, S.Kom., MT selaku Koordinator Tugas Akhir Teknik Informatika Universitas Mercu Buana.
4. Kedua orang tua yang selama ini telah membesarkan penulis.
5. Keluarga, teman-teman serta semua pihak yang telah memotivasi dan ikut memberikan bantuannya kepada penulis yang namanya tidak dapat penulis sebutkan satu per satu.

Akhir kata, penulis berharap semoga Allah swt. membalas kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua. Amin.

Jakarta, 06 Maret 2021
Penulis

DAFTAR ISI

NASKAH JURNAL

Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (Studi Kasus PT iForte Global Internet)

Comparative Analysis of Data Encryption Algorithms in Virtual Private Network (Case Study of PT iForte Global Internet)

Ayu Azizah Putri*1), Ida Nurhaida2)

*1,2) Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana, Jl. Meruya Selatan No. 1, Kembangan, Jakarta Barat, Indonesia 11650

Cara sitasi: A. A. Putri and I. Nurhaida, "Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private (Studi Kasus PT iForte Global Internet)" *Jurnal Teknologi dan Sistem Komputer*, vol. x, no. x, pp. xx-xx, 202x. doi: 10.14710/jtsiskom.x.x.202x.xx-xx, [Online].

Abstract *- VPN (Virtual Private Network) network is one of the needs in the process of exchanging data between computers both inside and outside the agency that provides private access connections where the data is encapsulated with headers containing routing information and encrypted to maintain data confidentiality. This research was conducted to test the data encryption algorithm with QoS (Quality of Service) parameters delay, throughput, and packet loss on the L2TP/IPSec. The values obtained from these parameters are compared with the TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) standard to determine the optimal encryption. After the process of network design, testing, and analysis, the results of the AES 256 algorithm has the best performance to the delay and throughput parameters. In the packet loss parameter, the 3DES algorithm has a higher average packet loss value than the AES 128 and AES 256 algorithms.*

Keywords *– VPN; QoS; AES 256; AES 128; 3DES*

Abstrak *- Jaringan VPN (Virtual Private Network) menjadi salah satu kebutuhan dalam proses pertukaran data antar komputer baik didalam maupun diluar instansi yang memberikan layanan koneksi akses secara private dimana data tersebut dienkapsulasi dengan header yang berisi informasi routing dan dienkripsi untuk menjaga kerahasiaan data. Penelitian ini dilakukan untuk menguji algoritma enkripsi data dengan parameter QoS (Quality of Service) yaitu delay, throughput dan packet loss pada jaringan VPN L2TP/IPSec. Nilai-nilai yang didapatkan dari parameter tersebut dibandingkan dengan standar TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) dengan tujuan untuk mengetahui algoritma enkripsi yang optimal. Setelah dilakukan proses perancangan jaringan, pengujian serta analisa, didapatkan hasil algoritma AES 256 unggul pada parameter delay dan throughput. Pada parameter packet loss algoritma 3DES memiliki nilai rata-rata packet loss yang lebih tinggi dibandingkan dengan algoritma AES 128 dan AES 256.*

Kata kunci *– VPN; QoS; AES 256; AES 128; 3DES*

*) Penulis korespondensi (Ayu Azizah Putri)
Email: 41517110093@student.mercubuana.ac.id

I. Pendahuluan

Semakin berkembangnya teknologi informasi, maka meningkat pula akan kebutuhan komunikasi dan pertukaran data. Jaringan komputer menjadi salah satu kebutuhan yang penting bagi kehidupan manusia untuk melakukan proses pertukaran data antar komputer di dalam instansi maupun diluar instansi. Teknologi VPN (*Virtual Private Network*) adalah layanan koneksi yang memberikan akses secara *private* sehingga saat melakukan proses pertukaran data dapat dilakukan lebih cepat dan efisien serta lebih aman [1], [2]. VPN menggunakan metode *tunneling* untuk melakukan proses transfer data dari satu jaringan ke jaringan yang lain menggunakan jaringan publik [3], [4]. Hal ini disebut sebagai *tunneling* dikarenakan data yang melewati tunneling hanya melihat dua titik endpoint saja dan kedua titik *endpoint* harus menggunakan protokol *tunneling* yang sama agar dapat saling berkomunikasi sehingga pertukaran data dapat dilakukan [5], [6]. Data dienkapsulasi atau dibungkus dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi point to point sehingga data dapat melewati jaringan publik dan dapat mencapai tujuan akhir [7]. Sedangkan untuk mendapatkan koneksi bersifat *private*, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi [8]. Keamanan merupakan syarat yang paling penting dalam suatu jaringan. Dalam teknologi VPN, IPSec menyediakan layanan keamanan pada jaringan untuk melakukan enkripsi dan dekripsi data [9], [10].

Pada saat ini PT. iForte Global Internet menggunakan teknologi VPN dengan protokol L2TP dan ditambahkan algoritma enkripsi IPSec yaitu AES 256 karena AES (*Advanced Encryption Standard*) merupakan standar enkripsi dengan kunci-simetris dan menurut Andriani dkk. [11] dinilai sebagai algoritma kunci simetris yang

sangat baik. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaannya [12].

Masing-masing algoritma enkripsi memiliki perbedaan proses dalam melakukan enkripsi dan dekripsi data. Seperti penelitian yang sudah dilakukan [13]–[16] membandingkan kecepatan proses enkripsi-dekripsi dengan beberapa algoritma yang digunakan. Hasil dari penelitian tersebut menunjukkan adanya perbedaan waktu yang dibutuhkan tergantung dari ukuran file.

Penelitian yang dilakukan oleh Elezi dan Raufi [17] dimana melakukan perbandingan algoritma enkripsi yang diterapkan pada jaringan VPN menggunakan protokol IPSec menyatakan bahwa algoritma 3DES lebih cepat 3,3% dibandingkan algoritma AES128 ketika menjalankan remote query database hingga 1 juta record. Pada penelitian lainnya [18], telah menguji beberapa algoritma enkripsi IPSec dengan metode pengiriman data yang berbeda yaitu menggunakan TFTP dan video streaming. Untuk pengiriman data menggunakan TFTP memberikan hasil algoritma AES membutuhkan waktu yang lebih lama dibandingkan algoritma 3DES dan DES. Sedangkan untuk video streaming dengan ukuran video yang berbeda, algoritma AES memiliki kinerja yang lebih baik. Di sisi lain, pada penelitian [7] menyatakan algoritma 3DES merupakan algoritma yang optimal dalam pengujian kecepatan transfer data sedangkan algoritma yang lambat yaitu AES 192.

Pada penelitian lainnya [19] menyatakan bahwa terdapat hubungan yang kuat antara pengaruh *security* yang digunakan terhadap Qos (*Quality of Service*) pada jaringan dimana mekanisme keamanan akan menambah waktu untuk pemprosesan data dan menyebabkan *delay*.

Perbedaan penelitian ini dengan penelitian yang sudah dilakukan sebelumnya adalah melakukan perbandingan algoritma enkripsi IPSec yaitu AES 256, AES 128 dan 3DES terhadap QoS (*Quality of Service*) pada jaringan VPN menggunakan protokol L2TP/IPSec. QoS (*Quality of Service*) merupakan teknik untuk mengelola *bandwidth*, *throughput*, *delay*, *jitter*, dan *packet loss* dalam jaringan dengan tujuan untuk memastikan *user* mendapat layanan yang lebih baik pada jaringan tersebut [20]. Tujuan dalam penelitian ini untuk mengetahui algoritma enkripsi data yang optimal dari segi parameter QoS yaitu *delay*, *throughput* dan *packet loss* serta dapat menjadi acuan bagi perusahaan dalam memilih algoritma enkripsi data untuk jaringan VPN L2TP/IPSec.

II. METODE PENELITIAN

Pada penelitian ini merupakan jenis penelitian komparatif kualitatif dan metode penelitian yang digunakan yaitu studi kasus. Dalam penelitian ini, penulis menggunakan metode perancangan jaringan PPDIOO (*Prepare, Plan, Design, Implement, Operate and Optimize*). Metode ini merupakan metode yang diterapkan oleh Cisco untuk mendukung jaringan berkembang [21].

Gambar 1. Metode PPDIOO

A. Prepare

Prepare merupakan tahapan awal dalam penelitian untuk melakukan rencana kerja yang berhubungan dengan analisa pokok pembahasan, seperti masalah yang dihadapi, topologi jaringan yang akan dibangun, dan kebutuhan dari sisi *hardware* maupun *software* [22]. Data perangkat serta spesifikasinya dirangkum pada Tabel 1 dan Tabel 2.

Tabel 1. Kebutuhan Perangkat Keras/*Hardware*

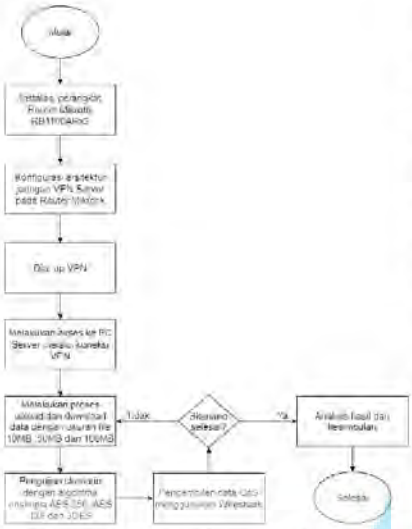
No	Deskripsi	Spesifikasi
1	Laptop	Lenovo, Intel Core i5, RAM 8GB
2	PC	Lenovo ThinkStation P320, Intel Core i7, RAM 8GB
3	Router	RB1100AHx2

Tabel 2. Kebutuhan Perangkat Lunak/*Software*

No	Deskripsi	Spesifikasi
1	Sistem operasi Laptop	Windows 10, 64-bit
2	Sistem operasi PC	Windows 10, 64-bit
3	Sistem operasi Router	Winbox v3.1.9
4	Aplikasi Wireshark	v3.2.7
5	Aplikasi GNS3	v.2.2.0
6	Aplikasi Oracle VM Virtual Box	v6.0.10

B. Plan

Plan adalah tahapan perencanaan jaringan untuk mengidentifikasi persyaratan jaringan yang sesuai dengan kebutuhan, tujuan dan fasilitas dalam proses penelitian [22]. Berikut *flowchart* diagram yang menjelaskan tahapan perancangan penelitian :

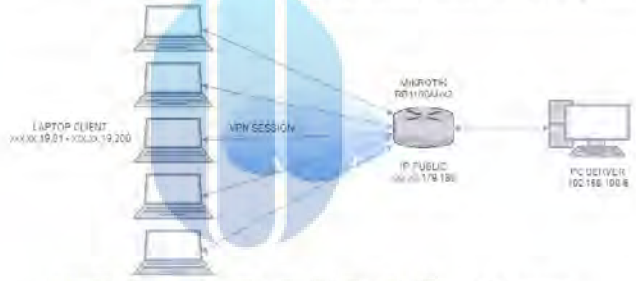


Gambar 2. Flowchart Perancangan Penelitian

Gambar 2 menunjukkan alur perancangan penelitian yang dimulai dengan instalasi perangkat Router Mikrotik RB1100AHx2 pada simulator GNS3, konfigurasi arsitektur jaringan VPN Server sehingga laptop *client* dapat melakukan akses ke PC Server. Perangkat serta spesifikasi PC Server dan laptop *client* yang dibutuhkan telah dirangkum pada tabel 1 dan tabel 2. Selanjutnya melakukan proses *upload* dan *download* data dengan ukuran file 10MB, 50MB dan 100MB pada masing-masing algoritma enkripsi yang dilakukan sebanyak sepuluh kali percobaan, pengambilan data QoS menggunakan aplikasi Wireshark. Setelah data selesai diambil, maka dilakukan analisa hasil dan membuat kesimpulan.

C. Design

Tahapan ini membuat topologi jaringan yang akan dilakukan pada penelitian. Pada gambar 3 menunjukkan topologi *remote access* VPN pada PT iForte Global Internet. Topologi tersebut dibangun menggunakan satu unit router Mikrotik RB1100AHx2 dengan protokol L2TP/IPSec agar dapat mengakses file server melalui service server message block (SMB) melalui alamat IP Public. Konfigurasi *device client* dilakukan oleh staff administrator jaringan dengan membuat *remote access* VPN menggunakan protokol L2TP pada setiap perangkat dengan mendaftarkan username dan password VPN.



Gambar 3. Topologi Remote Access VPN pada PT iForte Global Internet

D. Implement

Pada tahap ini melakukan implementasi sesuai dengan perencanaan dan *design* topologi yang sudah dibuat. Tahapan tersebut dimulai dari instalasi perangkat Router pada *tools* GNS3, melakukan konfigurasi jaringan VPN Server dan VPN *Client*, melakukan sepuluh kali pengujian dengan *upload* dan *download* file pada masing-masing algoritma enkripsi data, serta pengambilan data QoS dengan aplikasi Wireshark.

E. Operate

Tahapan ini melakukan percobaan skenario yang telah disiapkan. Percobaan dilakukan dengan melakukan *upload* dan *download* file dari laptop *client* ke PC Server melalui akses VPN L2TP/IPSec yang terdapat pada perangkat router Mikrotik RB1100AHx2 dengan tiga algoritma enkripsi data, yaitu AES 256, AES 128 dan 3DES yang masing-masing dilakukan sebanyak sepuluh kali pengujian. Setiap pengujian dilakukan dengan tiga ukuran file yang berbeda, yaitu 10MB, 50MB dan 100MB saat kondisi trafik *idle* dan *peak*. Pada laptop *client* melakukan capture wireshark untuk menguji QoS dari skenario yang sudah ditetapkan. Dalam menguji kehandalan algoritma enkripsi IPSec, maka dalam pengambilan data terdapat tiga parameter QoS yang dilakukan pengukuran yaitu *delay*, *throughput* dan *packet loss*. Hasil yang ditampilkan merupakan nilai rata-rata dari keseluruhan percobaan.

Delay

Delay mengukur lamanya waktu yang dibutuhkan antara saat informasi dikirim dan ketika diterima [23]. *Delay* dapat dipengaruhi oleh jarak, media fisik, *congestion* atau juga waktu proses yang lama.

Berikut adalah cara menghitung *Delay*:

$$Delay = \frac{Total\ delay}{Total\ paket\ yang\ diterima} \quad (1)$$

Persamaan (1), nilai *delay* didapat dari lamanya waktu yang dibutuhkan dibagi dengan total paket yang diterima dengan kategori *delay* yang diukur berdasarkan standar TIPHON pada tabel 3.

Tabel 3. Kategori Delay

Kategori	*Delay*	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 ms - 300 ms	3
Sedang	300 ms - 450 ms	2
Buruk	>450 ms	1

(Sumber: TIPHON)

Throughput

Throughput adalah jumlah total kedatangan paket yang sukses diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut [23].

Berikut adalah cara menghitung *Throughput*:

$$Throughput = \frac{jumlah\ paket\ yang\ diterima}{jumlah\ waktu\ pengiriman} \quad (2)$$

Throughput diperoleh melalui persamaan (2) dan kategori yang diukur berdasarkan standar TIPHON pada tabel 4.

Tabel 4. Kategori Throughput

Kategori	*Throughput*	Indeks
Sangat Bagus	>2,1 Mbps	4
Bagus	1200 kbps – 2,1 Mbps	3
Sedang	700 – 1200 kbps	2
Buruk	338 – 700 kbps	1
Sangat Buruk	0 – 338 kbps	0

(Sumber: TIPHON)

Packet Loss

Packet loss menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang dapat terjadi dari titik satu ke titik lainnya [23]. *Packet loss* dapat terjadi karena *collision* dan *congestion* pada jaringan sehingga mempengaruhi kinerja jaringan secara langsung. *Collision* merupakan kondisi dimana terjadi tabrakan data dalam jaringan yang diakibatkan oleh dua atau lebih perangkat mengirim data pada saat yang bersamaan [24], sedangkan *congestion* adalah kondisi dimana terjadi penumpukan paket data dalam jaringan yang diakibatkan oleh paket data yang melewati jaringan melebihi kapasitas dari jaringan tersebut [25].

Berikut adalah cara menghitung *Packet Loss*.

$$Packet\ Loss = \frac{Total\ Tx - Total\ Rx}{Total\ Tx} x100\% \quad (3)$$

Pada persamaan 3, Total Tx adalah total paket data yang dikirim dan Total Rx adalah total paket data yang diterima. Kategori *packet loss* yang diukur berdasarkan standar TIPHON pada tabel 5.

Tabel 5. Kategori Packet Loss

Kategori	*Packet Loss*	Indeks
Sangat Bagus	0 - 2%	4
Bagus	3 - 14%	3
Sedang	15 - 24%	2
Buruk	>25%	1

(Sumber: TIPHON)

F. Optimize

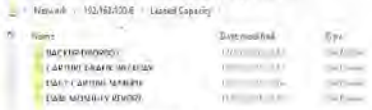
Pada tahap ini dapat dilakukan *network auditing* pada jaringan jika terlalu banyak masalah pada jaringan yang timbul atau kinerja yang tidak sesuai. Hal ini dilakukan untuk memastikan kinerja jaringan berjalan sesuai dengan perencanaan.

III. HASIL DAN PEMBAHASAN

Pada penelitian ini setelah melalui tahapan perancangan jaringan dengan metode PPDIOO (*Prepare, Plan, Design, Implement, Operate and Optimize*), konfigurasi jaringan VPN Server dan VPN *Client*, uji coba *upload* dan *download* file dengan algoritma enkripsi data yang dilakukan sebanyak sepuluh kali dalam kondisi jaringan *peak* dan *idle*, maka didapatkan nilai QoS dari masing-masing skenario pengujian. Nilai QoS yang diuji pada penelitian ini yaitu *delay*, *throughput* dan *packet loss*.

A. Akses PC Server

Setelah dilakukan konfigurasi jaringan VPN Server dan VPN *Client*, maka laptop *client* melakukan *dial-up* VPN dan mengakses ke file server untuk melakukan proses pertukaran data. Pada gambar 4 menunjukkan file server berhasil diakses oleh laptop *client*.

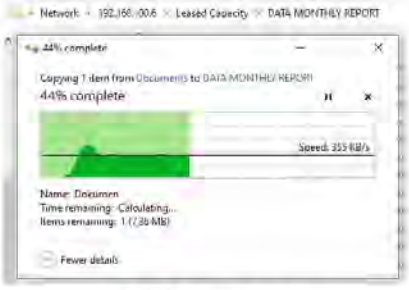


Gambar 4. Akses File Server

B. Proses Upload dan Download

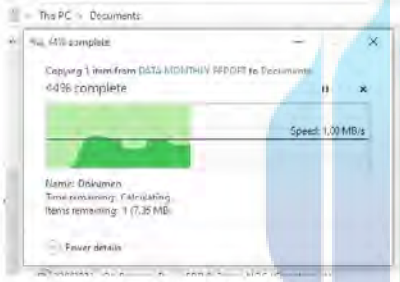
Pada saat *client* sudah dapat mengakses PC Server, maka dilakukan proses uji coba *upload* dan *download* file

sebanyak sepuluh kali dan melakukan pengambilan data QoS dengan aplikasi Wireshark.



Gambar 5. Proses Upload File

Gambar 5 menunjukkan proses laptop *client* sedang melakukan *upload* file ke file server dengan menggunakan metode *copy file* atau menyalin file antar host di jaringan VPN. Ukuran file yang disalin bervariasi yaitu file dengan ukuran 10MB, 50MB dan 100MB.



Gambar 6. Proses Download File

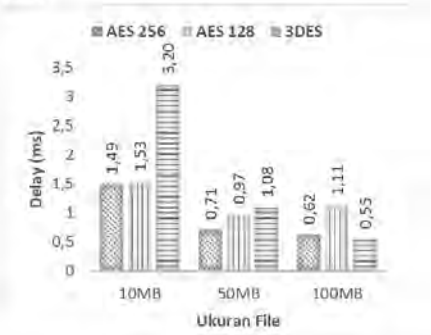
Gambar 6 menunjukkan proses laptop *client* sedang melakukan *download* file dari file server dengan menggunakan metode *copy* file atau menyalin file antar host di jaringan VPN. Ukuran file yang disalin bervariasi yaitu file dengan ukuran 10MB, 50MB dan 100MB seperti proses *upload* pada gambar 5.

C. Analisa Parameter QoS

Proses Upload

Pada proses ini dilakukan pengujian *upload* file dari laptop *client* ke PC Server sebanyak sepuluh kali dengan ukuran file 10MB, 50MB dan 100MB pada masing-masing algoritma enkripsi data.

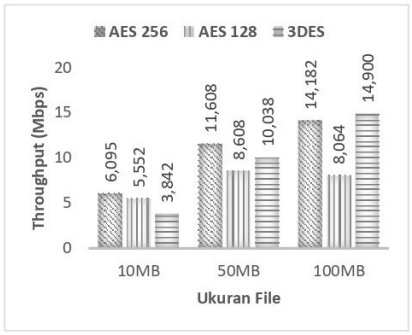
Delay



Gambar 7. Grafik Pengujian Delay Pada Proses Upload

Gambar 7 menunjukkan grafik hasil rata-rata pengujian *upload* yang dilakukan sebanyak sepuluh kali dalam kondisi trafik *idle* dan *peak* untuk ketiga algoritma enkripsi memiliki kategori yang sangat bagus menurut standar TIPHON pada tabel 3 dengan penilaian rata-rata antara 0,55 dan 3,20 ms. Nilai rata-rata *delay* terendah pada pengujian file 10MB adalah AES 256 (1,49 ms). Nilai rata-rata *delay* terendah pada pengujian file 50MB adalah AES 256 (0,71 ms). Nilai rata-rata *delay* terendah pada pengujian file 100MB adalah 3DES (0,55 ms). Pada hasil keseluruhan pengujian yang memiliki nilai rata-rata *delay* tertinggi yaitu algoritma 3DES. Hal ini dikarenakan dalam proses algoritma 3DES melakukan enkripsi perputaran *round* sebesar 48 *round* dibandingkan dengan AES 128 yang hanya memiliki perputaran *round* sebesar 10 *round* dan AES 256 yang memiliki 14 *round* [7]. Penelitian ini memberikan hasil yang berbeda dengan penelitian sebelumnya [7], dimana pada penelitian tersebut algoritma 3DES memiliki nilai *delay* yang paling rendah dibandingkan AES 128 dan AES 256 dari sisi *upload* data. Namun, pada penelitian tersebut tidak dijelaskan kondisi trafik jaringan saat pengukuran data.

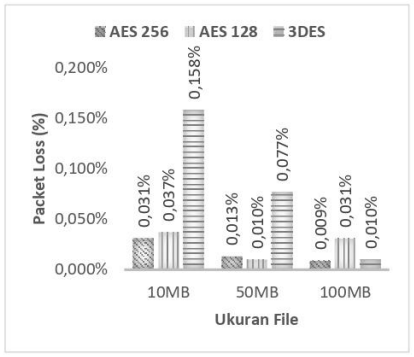
Throughput



Gambar 8. Grafik Pengujian Throughput Pada Proses Upload

Gambar 8 menunjukkan grafik hasil rata-rata pengujian *upload* yang dilakukan sebanyak sepuluh kali dalam kondisi trafik *idle* dan *peak* untuk ketiga algoritma enkripsi memiliki kategori yang sangat bagus menurut standar TIPHON pada tabel 4 dengan penilaian rata-rata antara 3,842 dan 14,900 Mbps. Nilai rata-rata *throughput* terbaik pada pengujian file 10MB adalah AES 256 (6,095 Mbps). Nilai rata-rata *throughput* terbaik pada pengujian file 50MB adalah AES 256 (11,608 Mbps). Nilai rata-rata *throughput* terbaik pada pengujian file 100MB adalah 3DES (14,900 Mbps). Pada hasil keseluruhan pengujian yang memiliki nilai rata-rata *throughput* terbaik untuk proses *upload* adalah algoritma AES 256 karena AES 256 menggunakan *block size* 256 bit yang jauh lebih besar daripada AES 128 yang memiliki 128 bit sedangkan 3DES hanya 64 bit [7]. Seperti pada penelitian [18] yang menyatakan bahwa algoritma enkripsi AES merupakan algoritma yang optimal dari sisi *throughput* dibandingkan algoritma 3DES. Namun, pada penelitian tersebut tidak dijelaskan jenis algoritma AES yang digunakan.

Packet Loss



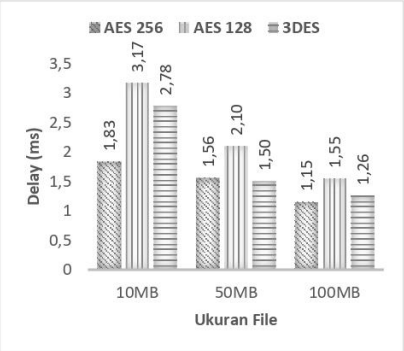
Gambar 9. Grafik Pengujian Packet Loss Pada Proses Upload

Seperti yang ditunjukkan pada gambar 9, hasil pengujian *packet loss* pada proses *upload* yang dilakukan sebanyak sepuluh kali dalam kondisi trafik *idle* dan *peak* untuk ketiga algoritma enkripsi memiliki kategori yang sangat bagus menurut standar TIPHON pada tabel 5 dengan penilaian rata-rata antara 0,009% dan 0,158%. Nilai rata-rata *packet loss* terendah pada pengujian file 10MB adalah AES 256 (0,031%); pada pengujian file 50MB adalah AES 128 (0,010%); dan pada pengujian file 100MB adalah AES 256 (0,009%). Pada hasil keseluruhan pengujian *upload* yang memiliki nilai rata-rata *packet loss* tertinggi adalah algoritma 3DES. Seperti pada penelitian [18] yang menyatakan bahwa algoritma enkripsi 3DES merupakan algoritma yang memiliki nilai *packet loss* tinggi dibandingkan algoritma AES. Hal ini dikarenakan 3DES melakukan tiga kali proses enkripsi pada data yang sama, sehingga membutuhkan waktu yang cukup lama dan antrian data yang banyak [7]. Proses tersebut mengakibatkan tingginya *packet loss* pada algoritma 3DES.

Proses Download

Pada proses ini dilakukan pengujian *download* file dari PC Server ke laptop *client* sebanyak sepuluh kali dengan ukuran file 10MB, 50MB dan 100MB pada masing-masing algoritma enkripsi data.

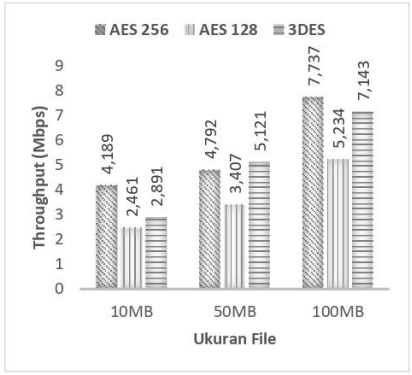
Delay



Gambar 10. Grafik Pengujian Delay Pada Proses Download

Gambar 10 menunjukkan grafik hasil rata-rata pengujian download yang dilakukan sebanyak sepuluh kali dalam kondisi trafik *idle* dan *peak* untuk ketiga algoritma enkripsi memiliki kategori yang sangat bagus menurut standar TIPHON pada tabel 3 dengan penilaian rata-rata antara 1,15 dan 3,17 ms. Nilai rata-rata *delay* terendah pada pengujian file 10MB adalah AES 256 (1,83 ms); pada pengujian file 50MB adalah 3DES (1,50 ms); dan pada pengujian file 100MB adalah AES 256 (1,15 ms). Pada hasil keseluruhan pengujian yang memiliki nilai rata-rata *delay* tertinggi adalah algoritma AES 128 yang seharusnya algoritma tersebut lebih baik daripada 3DES karena memiliki *round trip* yang lebih sedikit daripada 3DES [7]. Hal ini disebabkan karena ditemukan *bottleneck* di jaringan pada saat proses *download* karena pengujian ini dilakukan dengan kondisi *real time*. Penelitian ini memberikan hasil yang berbeda dengan penelitian sebelumnya [7], dimana pada penelitian tersebut algoritma 3DES memiliki nilai *delay* yang paling rendah dibandingkan AES 128 dan AES 256 dari sisi *download* data. Namun, tidak dijelaskan kondisi trafik jaringan saat pengukuran data.

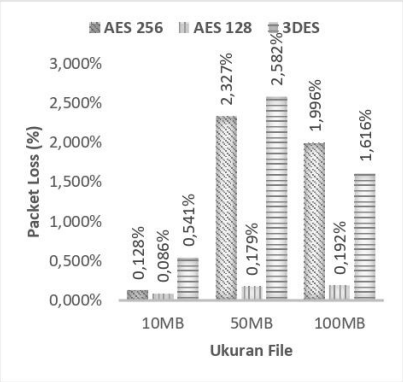
Throughput



Gambar 11. Grafik Pengujian Throughput Pada Proses Download

Gambar 11 menunjukkan grafik hasil rata-rata pengujian *download* yang dilakukan sebanyak sepuluh kali dalam kondisi trafik *idle* dan *peak* untuk ketiga algoritma enkripsi memiliki kategori yang sangat bagus menurut standar TIPHON pada tabel 4 dengan penilaian rata-rata antara 2,461 dan 7,737 Mbps. Nilai rata-rata *throughput* terbaik pada pengujian file 10MB adalah AES 256 (4,189 Mbps). Nilai rata-rata *throughput* terbaik pada pengujian file 50MB adalah 3DES (5,121 Mbps). Nilai rata-rata *throughput* terbaik pada pengujian file 100MB adalah AES 256 (7,737 Mbps). Pada hasil keseluruhan pengujian yang memiliki nilai rata-rata *throughput* terbaik untuk proses *download* adalah algoritma AES 256, untuk analisanya tidak jauh berbeda dengan analisa *throughput* pada proses *upload* merujuk pada penelitian [18].

Packet Loss



Gambar 12. Grafik Pengujian Packet Loss Pada Proses Download

Seperti yang ditunjukkan pada gambar 12, hasil pengujian *packet loss* pada proses *download* yang dilakukan sebanyak sepuluh kali dalam kondisi trafik *idle* dan *peak* untuk ketiga algoritma enkripsi memiliki kategori yang sangat bagus menurut standar TIPHON pada tabel 5 dengan penilaian rata-rata antara 0,086% dan 2,585%. Nilai rata-rata *packet loss* terendah pada ketiga pengujian file yaitu AES 128 dengan hasil 0,086% pada pengujian file 10MB; 0,179% pada pengujian file 50MB; dan 0,192% pada pengujian file 100MB. Namun nilai rata-rata *packet loss* tertinggi yaitu pada algoritma 3DES, untuk analisanya tidak jauh berbeda dengan analisa *packet loss* pada proses *upload* merujuk pada penelitian [18].

IV. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan pada perbandingan algoritma enkripsi data pada jaringan VPN L2TP/IPSec, algoritma AES 256 unggul pada parameter *delay* (1,227 ms) dan *throughput* (8,101 Mbps) dikarenakan algoritma AES 256 memiliki perputaran *round* yang lebih sedikit yaitu 14 *round* dan *block size* yang lebih besar yaitu 256 bit dibandingkan 3DES dan dari segi keamanan AES 256 memiliki tingkat keamanan yang lebih baik dibandingkan AES 128 karena memiliki ukuran kunci yang lebih besar, sedangkan pada parameter *packet loss* algoritma 3DES memiliki nilai rata-rata *packet loss* yang lebih tinggi (0,831%) dibandingkan dengan algoritma AES 128 dan AES 256. Hal ini dikarenakan 3DES melakukan tiga kali proses enkripsi pada data yang sama, sehingga membutuhkan waktu yang cukup lama dan antrian data yang banyak. Sehingga dapat disimpulkan bahwa algoritma AES 256 merupakan algoritma enkripsi yang paling optimal untuk digunakan dalam proses transfer data di jaringan VPN LT2P/IPSec.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada PT iForte Global Internet sebagai pihak yang memfasilitasi penelitian ini dan berbagai pihak yang sudah membantu.

DAFTAR PUSTAKA

[1] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP," *Jurnal Infotel*, vol. 9, no. 3, pp. 265–270, 2017, doi: 10.20895/infotel.v9i3.274.

[2] A. M. Abdulazeez, B. W. Salim, D. Q. Zeebaree, and D. Doghramachi, "Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 18, pp. 157–177, 2020, doi: 10.3991/ijim.v14i18.16507.

[3] Mardianto, "Analisis Quality Of Service (QoS) pada Jaringan VPN dan MPLS VPN Menggunakan GNS3," *Jurnal Sains dan Informatika*, vol. 5, no. 2, pp. 98–107, 2019, doi: 10.34128/jsi.v5i2.191.

[4] A. Rachmawan and A. Prihanto, "Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN," *Jurnal Manajemen Informatika*, vol. 8, no. 2, pp. 53–57, 2018, [Online]. Available: http://docplayer.info/88341583-Perbandingan-protokol-l2tp-dan-pptp-untuk-membangun-jaringan-intranet-di-atas-vpn.html.

[5] F. A. Salman, "Implementation of IPsec-VPN tunneling using GNS3," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 7, no. 3, pp. 855–860, 2017, doi: 10.11591/ijeecs.v7.i3.pp855-860.

[6] B. Santoso, A. Sani, T. Husain, and N. Hendri, "VPN Site To Site Implementation Using Protocol L2TP and IPSec," *TEKNOKOM : Jurnal Teknologi dan Rekayasa Sistem Komputer*, vol. 4, no. 1, pp. 30–36, 2021, doi: 10.31943/teknokom.v4i1.59.

[7] A. H. M. Permana, N. Widiyasono, and A. Rahmatulloh, "Perbandingan Algoritma Pada Virtual Private Network Ipsec Terhadap Kecepatan Data Transfer," *Sistemasi*, vol. 9, no. 2, p. 259, 2020, doi: 10.32520/stmsi.v9i2.713.

[8] F. Sjafrina, "Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional," in *Proc. of the Seminar Nasional Teknologi Informasi dan Komunikasi STI&K (SeNTIK 2019)*, Jakarta, Indonesia, Aug. 2019, vol. 3, pp. 211–217.

[9] D. Deshmukh and B. Iyer, "Design of IPSec Virtual Private Network For Remote Access," in *Proc. of the 2017 International Conference on Computing, Communication and Automation (ICCCA 2017)*, Greater Noida, India, May 2017, pp. 716–719, doi: 10.1109/CCAA.2017.8229894.

[10] *Guide to Virtual Private Networks via the Internet between WMO Information System Centres*. Geneva 2, Switzerland: World Meteorological Organization (WMO), 2016.

[11] R. Andriani, S. E. Wijayanti, and F. W. Wibowo, "Comparision of AES 128, 192 And 256 Bit Algorithm For Encryption And Description File," in *Proc. of the 2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE 2018)*, Yogyakarta, Indonesia, Nov. 2018, pp. 120–124, doi: 10.1109/ICITISEE.2018.8720983.

[12] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda DIY," *Jurnal Teknik Informatika (Jutif)*, vol. 1, no. 2, pp. 69–77, 2020, doi: https://doi.org/10.20884/1.jutif.2020.1.2.21.

[13] Donzilio Antonio Meko, "Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *Jurnal Teknologi Terpadu*, vol. 4, no. 1, pp. 8–15, 2018, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/jtt/article/view/110/93.

[14] M. Muhathir, "Perbandingan Algoritma Blowfish Dan Twofish Untuk Kriptografi File Gambar," *Journal of Informatics and Telecommunication Engineering*, vol. 2, no. 1, p. 23, 2018, doi: 10.31289/jite.v2i1.1673.

[15] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.

[16] F. Muharram, H. Azis, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," in *Proc. of the Seminar Nasional Ilmu Komputer dan Teknologi Informasi*, Samarinda, Indonesia, Dec. 2018, vol. 3, no. 2, pp. 112–115.

[17] M. Elezi and B. Raufi, "Conception of Virtual Private Networks Using IPsec Suite of Protocols, Comparative Analysis of Distributed Database Queries Using Different IPsec Modes of Encryption," *Procedia - Social and Behavioral Sciences*, vol. 195, pp. 1938–1948, 2015, doi: 10.1016/j.sbspro.2015.06.206.

[18] F. A. Daud, R. Ab Rahman, M. Kassim, and A. Idris, "Performance of Encryption Techniques Using Dynamic Virtual Protocol Network Technology," in *Proc. of the 2018 IEEE 8th International Conference on System Engineering and Technology (ICSET 2018)*, Bandung, Indonesia, Oct. 2018, pp. 29–34, doi: 10.1109/ICSEngT.2018.8606381.

[19] A. Hani and M. Houseini, "The Difference Impact on QoS Parameters between the IPSEC and L2TP," *International Journal of Innovative Research in Advanced Engineering*, vol. 11, no. 3, pp. 2349–2763, 2016.

[20] S. Informasi *et al.*, "Analisis Perbandingan Performasi QoS VPN Encryption Protocol Pada Jaringan Berbasis Hybrid Cloud," *Jurnal Ilmiah Komputasi*, vol. 20, no. 1, pp. 69–82, 2021, doi: 10.32409/jikstik.20.1.2695.

[21] L. Hernandez and G. Jimenez, "Design and Validation of a Scheme of Infrastructure of Servers, Under the PPDIOO Methodology, in the University Institution - ITSA," in *Proc. of the 2018 7th Computer Science On-line Conference (CSOC 2018)*, Zlin, Czech Republic, Apr. 2018, vol. 2, pp. 367–379, doi: 10.1007/978-3-319-91186-1.

[22] M. R. R. Fernando, L. M. N. Magaly, and C. S. M. Jose, "Analysis of Methodologies of Data Networks LAN," *International Journal of Advanced Engineering Research and Science*, vol. 3, no. 9, pp. 52–61, 2016, doi: 10.22161/ijaers/3.9.9.

[23] A. Darojat and I. Nurhaida, "Analisa QOS Administrative Distance Static Route Pada Failover VPN IPSec," *Jurnal Ilmu Teknik dan Komputer*, vol. 3, no. 1, pp. 11–21, 2019.

[24] M. Mufadhol, G. Aryotejo, and D. E. Kurniawan, "The Network Planning Concept for Increase Quality of Service using Packet Tracer," in *Proc. of the 2019 2nd International Conference on Applied Engineering (ICAE 2019)*, Batam, Indonesia, Oct. 2019, doi: 10.1109/ICAE47758.2019.9221675.

[25] A. Khafidin, T. Andrasto, and Suryono, "Implementation Flow Control To Improve Quality of Service on Computer Networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 3, pp. 1474–1481, 2019, doi: 10.11591/ijeecs.v16.i3.pp1474-1481.

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan judul Analisa Perbandingan Algoritma Enkripsi Data Pada Jaringan Virtual Private Network (VPN) (Studi Kasus PT iForte Global Internet) yang berisi semua material hasil penelitian Tugas Akhir yang tidak dimuat atau disertakan di artikel jurnal. Seluruh langkah-langkah perancangan, tahapan implementasi serta hasil pengujian akan dijelaskan dalam laporan ini.

Pendahuluan

Semakin berkembangnya teknologi informasi, maka meningkat pula akan kebutuhan komunikasi dan pertukaran data. Jaringan komputer menjadi salah satu kebutuhan yang penting bagi kehidupan manusia untuk melakukan proses pertukaran data antar komputer di dalam instansi maupun diluar instansi. Teknologi VPN (*Virtual Private Network*) adalah layanan koneksi yang memberikan akses secara *private* sehingga saat melakukan proses pertukaran data dapat dilakukan lebih cepat dan efisien serta lebih aman [1], [2]. VPN menggunakan metode *tunneling* untuk melakukan proses transfer data dari satu jaringan ke jaringan yang lain menggunakan jaringan publik [3], [4]. Hal ini disebut sebagai *tunneling* dikarenakan data yang melewati tunneling hanya melihat dua titik endpoint saja dan kedua titik *endpoint* harus menggunakan protokol *tunneling* yang sama agar dapat saling berkomunikasi sehingga pertukaran data dapat dilakukan [5], [6]. Data dienkapsulasi atau dibungkus dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi point to point sehingga data dapat melewati jaringan publik dan dapat mencapai tujuan akhir [7]. Sedangkan untuk mendapatkan koneksi bersifat *private*, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi [8]. Keamanan merupakan syarat yang paling penting dalam suatu jaringan. Dalam teknologi VPN,

IPSec menyediakan layanan keamanan pada jaringan untuk melakukan enkripsi dan dekripsi data [9], [10].

Pada saat ini PT. iForte Global Internet menggunakan teknologi VPN dengan protokol L2TP dan ditambahkan algoritma enkripsi IPSec yaitu AES 256 karena AES (*Advanced Encryption Standard*) merupakan standar enkripsi dengan kunci-simetris dan menurut Andriani dkk. [11] dinilai sebagai algoritma kunci simetris yang sangat baik. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaannya [12].

Masing-masing algoritma enkripsi memiliki perbedaan proses dalam melakukan enkripsi dan dekripsi data. Seperti penelitian yang sudah dilakukan [13]–[16] membandingkan kecepatan proses enkripsi-dekripsi dengan beberapa algoritma yang digunakan. Hasil dari penelitian tersebut menunjukkan adanya perbedaan waktu yang dibutuhkan tergantung dari ukuran file.

Penelitian yang dilakukan oleh Elezi dan Raufi [17] dimana melakukan perbandingan algoritma enkripsi yang diterapkan pada jaringan VPN menggunakan protokol IPSec menyatakan bahwa algoritma 3DES lebih cepat 3,3% dibandingkan algoritma AES128 ketika menjalankan remote query database hingga 1 juta record. Pada penelitian lainnya [18], telah menguji beberapa algoritma enkripsi IPSec dengan metode pengiriman data yang berbeda yaitu menggunakan TFTP dan video streaming. Untuk pengiriman data menggunakan TFTP memberikan hasil algoritma AES membutuhkan waktu yang lebih lama dibandingkan algoritma 3DES dan DES. Sedangkan untuk video streaming dengan ukuran video yang berbeda, algoritma AES memiliki kinerja yang lebih baik. Di sisi lain, pada penelitian [7] menyatakan algoritma 3DES merupakan algoritma yang optimal dalam pengujian kecepatan transfer data sedangkan algoritma yang lambat yaitu AES 192.

Pada penelitian lainnya [19] menyatakan bahwa terdapat hubungan yang kuat antara pengaruh *security* yang digunakan terhadap Qos (*Quality of Service*) pada jaringan dimana mekanisme keamanan akan menambah waktu untuk pemprosesan data dan menyebabkan *delay*.

Perbedaan penelitian ini dengan penelitian yang sudah dilakukan sebelumnya adalah melakukan perbandingan algoritma enkripsi IPSec yaitu AES 256, AES 128 dan 3DES terhadap QoS (*Quality of Service*) pada jaringan VPN menggunakan protokol L2TP/IPSec. QoS (*Quality of Service*) merupakan teknik untuk mengelola *bandwidth*, *throughput*, *delay*, *jitter*, dan *packet loss* dalam jaringan dengan tujuan untuk memastikan *user* mendapat layanan yang lebih baik pada jaringan tersebut [20]. Tujuan dalam penelitian ini untuk mengetahui algoritma enkripsi data yang optimal dari segi parameter QoS yaitu *delay*, *throughput* dan *packet loss* serta dapat menjadi acuan bagi perusahaan dalam memilih algoritma enkripsi data untuk jaringan VPN L2TP/IPSec.