Implementasi Fortigate Sd-Wan Menggunakan Link Astinet Dan Vpn Ipsec Pada Perusahaan Fif

1st Agam Vino Syah Putra
Fakultas Teknik Elekro
Universitas Telkom
Bandung, Indonesia
agamvinosp@student.telkomuniversity.ac.id

2nd Leanna Vidya Yovita
Fakultas Teknik Elekro
Universitas Telkom
Bandung, Indonesia
leanna@telkomuniversity.ac.id

3rd Lia Hafiza
Fakultas Teknik Elekro
Universitas Telkom
Bandung, Indonesia
liahfza@telkomuniversity.ac.id

***Abstrak* – Penelitian ini bertujuan (1) untuk mengetahui tingkat keamanan jaringan (2) untuk mengetahui seberapa lama koneksi yang teputus saat lalu lintas data (3) untuk mengetahui penggunaan lalu lintas pada link Astinet dan VPN IPsec berdasarkan aplikasi ini untuk layanan kinerja tersebut. Sehingga peneliti memiih untuk menggunakan dua metodelogi: metodelogi active/passive dan metodelogi firewall filtering yang bertujuan untuk menguji perangkat fortigate dengan konfigurasi auto link failover menggunakan jaringan Astinet dan VPN IPsec. Kemudian, Metodelogi firewall filtering digunakan untuk melindungi keamanan jaringan data. Hasil pengujian menunjukkan bahwa Auto Link Failover memiliki persentase paket loss VPN IPsec 11% dan astinet 6%. Kemudian perbandingan hasil kecepatan transfer data setiap 4 pengguna akses link Astinet dan VPN IPsec dalam kondisi terhubung dengan satu link saja, adalah 36,41, 24,79, 7,95, dan 5,35 bps pada link Astinet, sedangkan link VPN IPsec adalah 1860, 9,28, 31,63, dan 2,63 bps. Bandwidth yang digunakan pada traffic streering rata-rata yang digunakan adalah 1980 bps VPN IPsec 1980 bps sedangkan Astinet 3180 bps sedikit lebih besar dan tetap dapat load balancing. Selanjutnya Fitur web filtering yang pada fortigate dapat membatasi akses ke situs web/URL dan memblokir file download yang terproteksi sebagai data yang teridentifikasi tidak diizinkan pada perangkat fortigate SD-WAN.**

Kata Kunci: **SD-WAN, fortigate, link astinet, VPN IPsec, QoS**

I. PENDAHULUAN

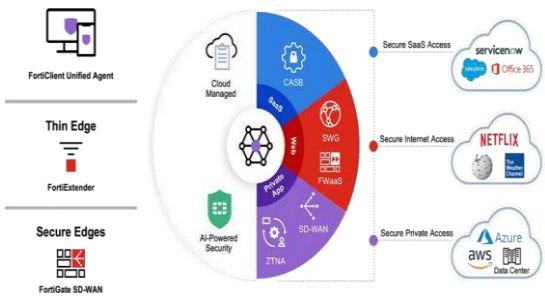
Di era teknologi yang serba online ini, kebutuhan akses internet sangat diperlukan bagi dunia bisnis. Umumnya perusahaan memiliki jaringan infrastruktur yang mendukung keperluan operasional. Namun kenyataannya infrastruktur jaringan WAN pada perusahaan FIF tidak cukup mampu untuk memenuhi kebutuhan komunikasi bisnis multi lokal perusahaan tersebut. Banyaknya aplikasi dan *website* yang digunakan sebagai sarana penunjang bisnis pada perusahaan FIF juga membuat beban *traffic steering* pada jaringan menjadi tidak *balance*. Pada kasus ini komunikasi antara kantor pusat dan kantor cabang pada perusahaan FIF hanya menggunakan satu jalur saja yaitu koneksi MPLS (*Multi-Protokol Label Switching*). Selain kebutuhan *bandwidth* terhadap koneksi jaringan internet pada perusahaan FIF, maka diperlukan juga teknologi yang handal dalam mengatur penggunaan trafik dari link itu sendiri sehingga dapat bekerja optimal.

Teknologi SD-WAN bekerja dengan cara menggabungkan beberapa jalur jaringan yang berbeda, seperti koneksi internet dan jaringan VPN IPsec. Fortigate SD-WAN juga dilengkapi dengan fitur-fitur seperti QoS (*Quality of Services*), yang memastikan bahwa aplikasi yang penting mendapatkan prioritas dalam penggunaan sumber daya jaringan. Adapun tujuan dari penelitian ini yaitu meningkatkan performansi operasional dengan *lead time* yang singkat, mudah, cepat tanpa gangguan dan hemat dalam pembiayaan infrastrukturnya dibandingkan dengan jaringan WAN tradisional.

II. KAJIAN TEORI

A. SD-WAN

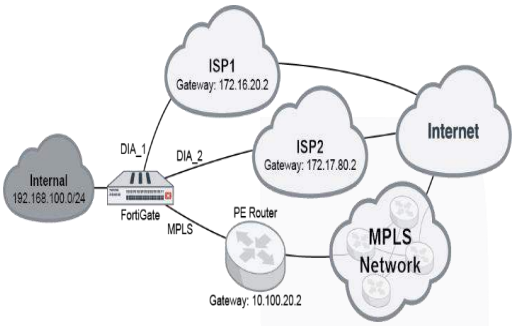
SD-WAN (Jaringan Area Luas yang Didefinisikan oleh Perangkat Lunak) adalah arsitektur overlay yang menciptakan konektivitas terpadu yang aman di atas berbagai jenis transportasi dan menyederhanakan operasi dengan memungkinkan manajemen terpusat, kontrol kebijakan, dan visibilitas aplikasi [1]. Teknologi SD-WAN bekerja dengan cara menggabungkan beberapa jalur jaringan yang berbeda, seperti koneksi internet dan jaringan seluler. SD-WAN juga dilengkapi dengan fitur – fitur seperti QoS (Quality of Services), yang memastikan bahwa aplikasi yang penting mendapatkan prioritas dalam penggunaan sumber daya jaringan. Selain itu, teknologi ini juga dilengkapi dengan fitur auto failover, yang akan beralih ke jalur cadangan jika jalur utama mengalami gangguan atau kegagalan koneksi, memonitor aktivitas cabang, membloking situs/web yang tidak diizinkan, melakukan load balance aplikasi sesuai dengan prioritasnya [2]. Teknologi SD-WAN dianggap sebagai teknologi yang berpotensi merevolusi penggunaan layanan WAN [3].



GAMBAR 1
Teknologi Fortigate SD-WAN.

B. Trafic Steering

Traffic Streering adalah protocol tambahan digunakan untuk lalu lintas jaringan, terutama protocol filtering, modifikasi atau optimasi diperlukan. Teknik ini digunakan untuk mengontrol penggunaan trafik yang berasal dari koneksi sesuai dengan kebutuhan pelanggan, sehingga lebih mengoptimalkan penggunaan fungsional dari koneksi itu sendiri. SD-WAN Fortigate mempunyai konsep protocol lalu lintas cerdas yang memungkinkan lalu lintas aplikasi dan protocol tertentu dialihkan untuk memastikan bahwa hanya koneksi yang diperlukan saja yang digunakan.

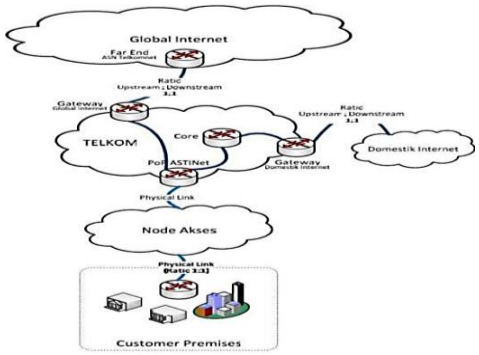


GAMBAR 2.
Alur Traffic Steering 2 ISP.

C. ASTINET

Astinet adalah layanan jaringan internet dedicated yang menghadirkan solusi terbaik dalam kecepatan dan stabilitas konektivitas untuk kebutuhan bisnis pada perusahaan dengan covarege yang luas. Layanan dari Astinet Telkom mempunyai beberapa kategori: Astinet Lite, Astinet Premium, Astinet Beda *Bandwidth*, dan Astinet Burstable. ASTINet LITE merupakan perpanjangan dari produk ASTINet, layanan Internet khusus namun menawarkan rasio uplink *bandwidth* 1:4 dan *rasio bitrate* rendah untuk koneksi global asimetris [4]. ASTINet memiliki *Network Management System* (NMS), yang dibangun untuk mengendalikan banyak perangkat secara bersamaan. Untuk melakukan setting perangkat dan monitoring gangguan, cukup dilakukan melalui NMS. ASTINet memiliki manfaat sebagai berikut:

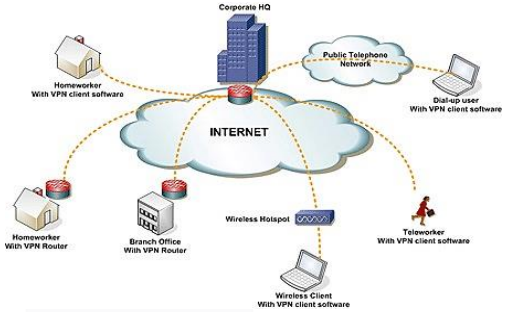
1. *Downstream* lebih baik dibandingkan akses internet rumahan dan biaya lebih sedikit terjangkau dibandingkan akses internet bisnis namum memerlurkan ip static untuk mengelola server aplikasi klien.
2. Cocok untuk pelanggan SME, Usaha Warnet, *Small Office*, dan pelanggan yang membutuhkan IP static.
3. *Ratio Downstream: Upstream* = 1:4.
4. Diberikan 1 IP static.
5. Dimonitoring online 7 x 24 jam oleh *network monitoring*.
6. *SLA Network* mencapai 98%[5].



GAMBAR 3.
Layanan Astinet Link.

D. VPN

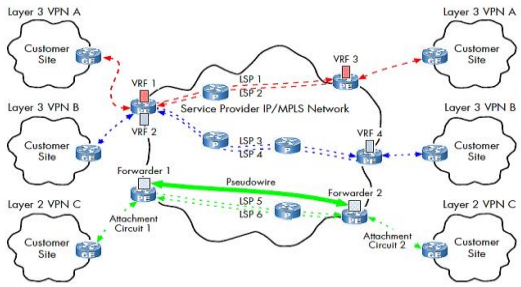
VPN (*Virtual Private Network*) adalah teknologi komunikasi yang memungkinkan anda terhubung ke jaringan public dan menggunakannya untuk terhubung ke jaringan local[6]. VPN memungkinkan banyak site pelanggan terhubung tetapi tidak dapat diakses dari site pelanggan lainnya. Keuntungan dari VPN adalah memungkinkan lokasi terpencil pelanggan untuk terhubung dengan aman melalui jaringan publik tanpa perlu membeli jalur jaringan khusus [7].



GAMBAR 4.
Layanan VPN.

E. MPLS

MPLS (*Multi-Protocol Label Switching*) adalah standar *Internet Engineering Task Force* (IETF) yang muncul berdasarkan *Tag Switching*[8]. MPLS banyak digunakan di jaringan perusahaan besar diberbagai bidang organisasi seperti bisnis, pemerintah, rumah sakit, call center, bank, dan kampus [7]. MPLS hadir sebagai teknologi yang menjanjikan yang akan meningkatkan skalabilitas routing dan forwarding hop-by-hop, dan menyediakan kemampuan rekayasa lalu lintas untuk penyediaan jaringan yang lebih baik. Tetapi MPLS bukan lah untuk masalah yang ada saat ini atau yang akan mendatang, melainkan teknologi yang memungkinkan untuk mengatasi beberapa masalah skala ini [9]. Berikut adalah beberapa terminologi MPLS: 1). LSR (*Label Switch Router*), 2). Label, 3). Edge LSR (*Edge Label Switch Router*), 4). LSP (*Label Switched Path*), 5). LVC (*Label Virtual Circuit*), 6). LDP (*Label Distribution Protocol*).



GAMBAR 5.
Layanan MPLS.

F. QoS

QoS (*Quality of Service*) adalah suatu parameter pengukuran tentang seberapa baik lalu lintas data dan merupakan upaya untuk mendefinisikan karakteristik dan sifat layanan. Tujuan dari QOS adalah untuk memenuhi kebutuhan berbagai layanan tetapi dengan menggunakan infrastruktur yang sama [10]. Variabel utama yang mempengaruhi kinerja layanan jaringan adalah *packet loss*, *throughput* dan *jitter* [11].

Packet Loss merupakan persentase hilangnya paket saat pengiriman data. Adapun persamaan yang digunakan adalah sebagai berikut [12]:

$$Packet\ Loss = \frac{Packets\ Send - Packets\ Received}{Packets\ Send} \text{x}100\% \quad (1).$$

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Delay dapat dipengaruhi oleh media fisik, jarak, kongesti atau juga proses lamanya waktu [12]. Empat kategori degradasi jaringan didefinisikan seperti pada gambar Tabel Tingkat degradasi jaringan standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Networks*) [11].

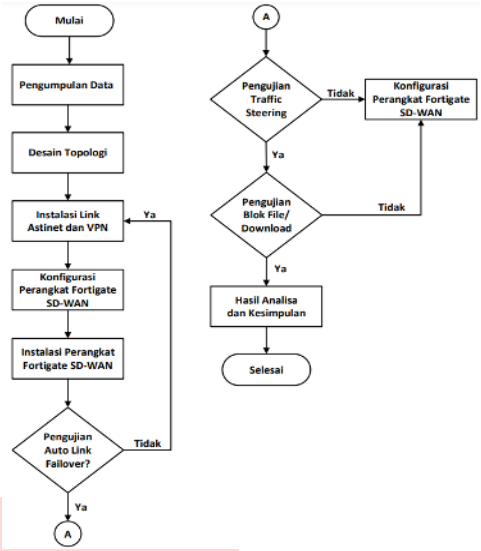
Degradation Category	Packet loss (note 2)	Peak jitter(note 3)
Perfect	zero	0 ms
Good	3 %	75 ms
Medium	15 %	125 ms
Poor	25 %	225 ms
NOTE 1: These figures are provisional. NOTE 2: Assuming the packet loss distribution is Gaussian. NOTE 3: Assuming the jitter distribution is Gaussian (with a standard deviation of half the peak).		

GAMBAR 6.
Tabel Standarisasi Tingkat Degradasi Jaringan.

III. METODE

A. Diagram Alir

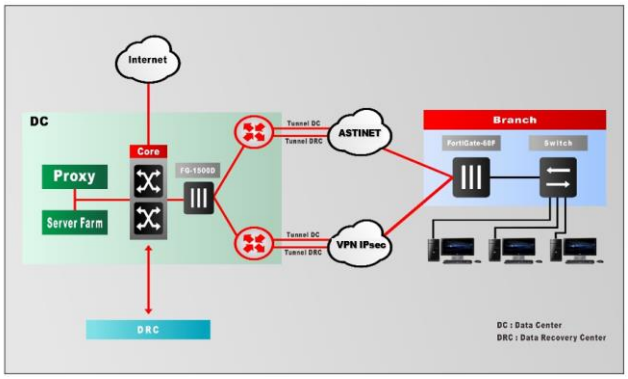
Penulis menguraikan skenario dalam pelaksanaan kerja dengan diagram alir seperti pada gambar 7:



GAMBAR 7.
Diagram Alir.

Proses dimulai dengan pengumpulan data, yang mencakup informasi tentang bisnis dan kebutuhan pengguna, yang diperlukan untuk mengkonfigurasi jaringan. Setelah pengumpulan data, topologi jaringan direncanakan dan didefinisikan. Pemilihan perangkat, lokasi dan koneksi link adalah bagian dari Desain Topologi. Selanjutnya proses instalasi link Astinet dan VPN IPsec yang digunakan sebagai jalur komunikasi pada implementasi ini. Konfigurasi disini menggunakan template yang dimasukan ke dalam perangkat fortigate yang berisikan sebuah alamat IP untuk pembentukan jalur komunikasi dan lalu lintas jaringan ke arah tujuan. Setelah proses konfigurasi dilakukan, perangkat fortigate SD-WAN dipasang pada cabang kantor FIF dan melakukan pemasangan dengan menghubungkan Link IPsec VPN di port 1 dan Astinet di port 2 pada perangkat Fortigate SD-WAN. Proses *auto link failover* menguji fungsi redudansi link serta konfigurasinya. Apakah paket-paket data tetap dapat berjalan pada saat salah satu link terputus Jika hasil pengujian positif (Ya), proses dilanjutkan. Jika Tidak, kembali ke tahap sebelumnya. Periksa link IPSec VPN dan Astinet serta konfigurasi perangkat. Proses pengalihan lalu lintas antara jalur yang berbeda, mengarahkan lalu lintas melalui jalur yang lebih cepat atau menghindari jalur yang mengalami masalah. Jika hasil pengujian positif (Ya), proses dilanjutkan. Jika Tidak, kembali ke tahap sebelumnya. Periksa konfigurasi perangkat. Pengujian Blok File/Download proses untuk menghentikan atau membatasi akses pengguna ke file tertentu atau menghalangi pengunduhan file dari internet. Jika hasil pengujian positif (Ya), proses dilanjutkan. Jika Tidak, kembali ke tahap sebelumnya. Periksa konfigurasi perangkat. Setelah tahapan proses dan masukan pada diagram alir selesai maka, hasil akan di analisa untuk dapat penulis menarik kesimpulan dari proses penelitian yang telah dilakukan tersebut. Penelitian ini menggunakan dua metodelogi pendekatan: metodelogi *active/passive* dan metodelogi firewall filtering. Metodelogi *active/passive* bertujuan untuk menguji perangkat fortigate dengan konfigurasi *failover* yang memastikan ketersediaan dan keandalan jaringan Astinet dan VPN IPsec. Metodelogi *firewall filtering* digunakan untuk melindungi keamanan jaringan data.

B. Topologi Jaringan



GAMBAR 8.
Topologi Jaringan.

Topologi Jaringan adalah diagram infrastruktur jaringan yang menunjukkan berbagai komponen perangkat dan koneksi yang saling terhubung. Konfigurasi yang dilakukan menggunakan fortigate 60F akan membentuk jaringan SD-WAN dengan 2 akses link ISP. Perancangan ini memungkinkan perangkat untuk mengakses data-data melalui lalu lintas dari link yang tersedia yaitu Astinet dan VPN IPsec. Apabila salah satu link yang tersedia terputus maka lalu lintas akan diarahkan ke salah satu link, Astinet maupun VPN IPsec. Jalur lalu lintas yang mengakses ke arah server di buat 2 tunneling pada kedua link tersebut, di mana dapat memberikan lalu lintas menjadi *load balancing* dan memberikan keamanan di jaringan *public*, sehingga menghindari dari serangan kejahatan yang ada di dunia IT.

Pada gambar 8 penempatan *perangkat proxi server farm, switch core,* FG-1500D dan router terinstal di *data center* dan *data recovery center* milik Telkom, sedangkan perangkat Fortigate 60F terinstal pada kantor cabang Jakarta 1.

C. Skenario Pengujian

1. Auto Link Failover

Pengujian ini melibatkan dua tahap uji coba. Tahap pertama melibatkan pemutusan koneksi link VPN IPsec, sedangkan tahap kedua melibatkan pemutusan koneksi link Astinet. Tujuan dari pengujian auto link failover ini adalah memastikan bahwa perangkat Fortigate dapat secara otomatis beralih ke link cadangan jika salah satu link utama gagal otomatis beralih ke link cadangan.

2. Traffic Steering

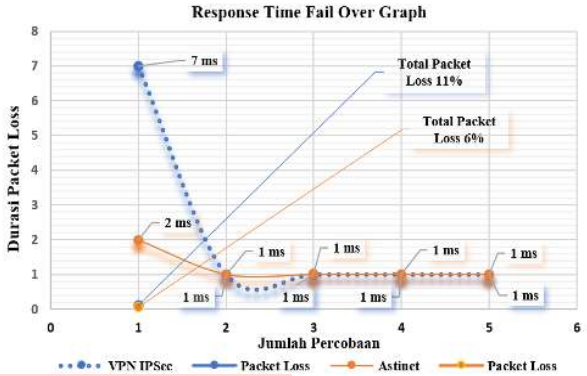
Pengujian ini menjalankan dua uji coba, di mana aplikasi dan Non-aplikasi dijalankan melewati jalur yang telah ditentukan dalam konfigurasi dengan kondisi kedua link VPN IPsec dan Astinet terhubung. Tujuannya adalah untuk mengoptimalkan penggunaan pada link Astinet dan VPN IPsec berdasarkan kebijakan aplikasi perusahaan FIF sehingga membantu mengurangi beban bandwidth pada kedua link Astinet dan VPN IPsec sehingga distribusi data berjalan seimbang pada kedua layanan.

3. Skenario Pengujian Web Filtering

Pada scenario ini melibatkan dua tahap yang dilakukan untuk menguji keamanan bloking web filtering dengan melakukan percobaan mengakses ke situs web dan URL dari laptop. Hal ini bertujuan untuk mengetahui hasil kinerja bloking situs web dan URL pada fortigate SD-WAN sehingga memberi keamanan lalu linyas data pada perusahan FIF.

IV. HASIL DAN PEMBAHASAN

A. Auto Link Failover

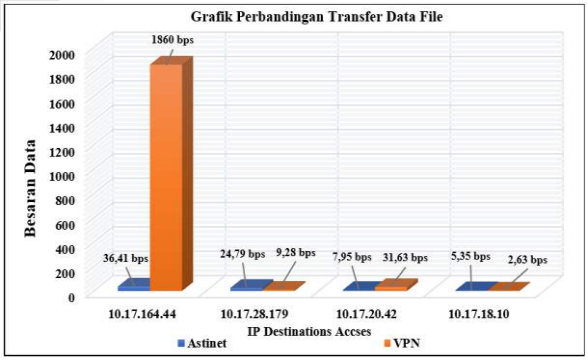


GAMBAR 9.
(Response Time Failover).

Pada gambar 9, pengujian dengan perpindahan jalur koneksi dilakukan sebanyak 10 kali, 5 kali untuk VPN IPsec dan 5 kali untuk Astinet. Hasil pengujian pertama pada VPN IPsec pemutusan koneksi menunjukkan paket loss sebesar 7 *miliseconds*, kemudian pemutusan koneksi selanjut sampai dengan ke lima grafik menunjukan penurunan paket loss sebesar 1 *miliseconds.* Hasil pengujian kedua pada Astinet, hasil pengetesan pemutusan koneksi menunjukan paket loss sebesar 2 *miliseconds*, kemudian pemutusan koneksi jaringan ke dua menunjukan tren positif mencapai nilai 1 *miliseconds* selama lima kali.

Apabila dihitung secara persentase *packet loss*, waktu respon *failover* kedua koneksi link didapatkan hasil 11% untuk VPN IPsec dan 6% untuk Astinet. Sedangkan latensi pada kedua link menunjukan hasil latensi sebesar 33 *miliseconds* untuk VPN IPsec dan 79 *miliseconds* untuk Astinet. Berdasarkan hasil pengujian tersebut masih dalam katagori yang baik menurut standart TIPHON. Hasil perbedaan yang didapatkan pada VPN IPsec maupun Astinet dapat disebabkan oleh beberapa faktor: 1). Jarak Server antara lokasi kantor cabang dan server. 2). Beban Server VPN IPsec yang terlalu banyak digunakan oleh kantor cabang. 3). Kecepatan internet yang disediakan oleh ISP. 4). Media jaringan yang digunakan.

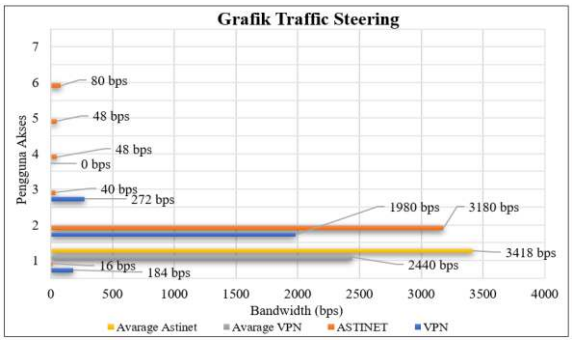
B. Perbandingan Akses Transfer Data



GAMBAR 10
(Grafik Perbandingan Transfers Data File).

Pengujian ini dilakukan pada saat setiap koneksi hanya aktif disatu jalur link saja sehingga dapat terlihat perbedaannya. Pada gambar 10 menunjukkan grafik perbandingan dalam user pengguna mengakses dalam transfer data antara link Astinet dan VPN IPsec. Di mana pada saat pengguna mengakses keempat IP tujuan, besaran data yang diakses didapat sebesar 36,41 bps, 24,79 bps, 7,95 bps, dan 5,35 bps pada link Astinet sedangkan besaran data yang diakses pada link VPN IPsec didapat sebesar 1860 bps, 9,28 bps, 31,63 bps, dan 2,63 bps.

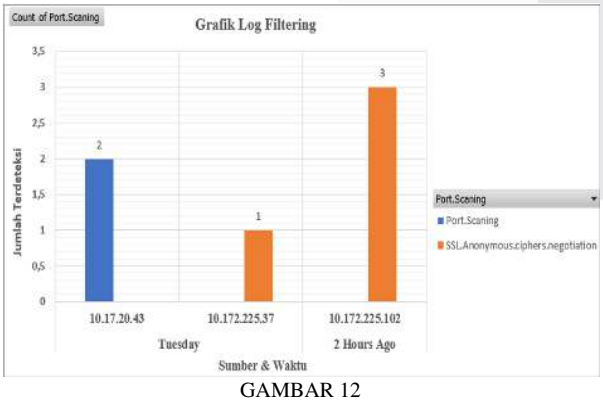
C. Traffic Sterring



GAMBAR 11
(Traffic Steering).

Pada gambar 11 grafik *traffic steering* baris bar warna oranye yang mewakili *bandwidth* Astinet dan baris bar berwarna biru mewakili *bandwidth* VPN IPsec, dapat lihat bahwa *traffic steering* dapat digunakan mengelola data pada jaringan antara kedua layanan, di mana pada gambar 4.6 aktivitas pengguna banyak melakukan akses data melalui jaringan Astinet. Apabila dihitung secara rata- rata, *bandwidth* yang digunakan pada jaringan Astinet 3418 bps sedangkan VPN IPsec 2440 bps. Hal ini terjadi karena kedua layanan jaringan dan fortigate mampu bekerja menyesuaikan alokasi *bandwidth* sesuai kebutuhan kondisi jaringan serta dapat memungkinkan lalu lintas, aplikasi dan Non aplikasi melewati jalur yang sudah ditetapkan pada konfigurasi.

D. Web Filtering



GAMBAR 12
(Grafik Log Filtering)

Hasil pada gambar 12 grafik log filtering mendeteksi *port.scanning* dan *SSL.Anonymous.ciphers.negotiation* sedang menancam keamanan jaringan pada dua waktu terpisah dengan tiga sumber ip yang berbeda. Pengujian ini dilakukan untuk mengetahui hasil kinerja bloking akses situs web dan URL pada fortigate SD-WAN agar dapat memberikan keamanan data. Hal ini bisa terjadi karena adanya pengaturan *policy* dan didukung dengan lisensi perangkat fortigate, maka fitur web filtering pada fortigate dapat berfungsi dengan baik sesuai standar *benefit* pada perangkat fortigate SD-WAN.

V. KESIMPULAN

Hasil dari penelitian ini menunjukkan persentase waktu respon *auto link failover* kedua koneksi link sebesar 11% VPN IPsec dan 6% pada Astinet. Perbandingan besaran data diakses pengguna sebesar 36,41 bps, 24,79 bps, 7,95 bps, dan 5,35 bps pada link Astinet besaran data yang diakses dengan link VPN IPsec sebesar 1860 bps, 9,28 bps, 31,63 bps, dan 2,63 bps. *Traffic steering* pada koneksi link Astinet 3418 bps dan VPN IPsec 2440 bps, sehingga dapat mengarahkan lalu lintas melalui jalur yang paling efisien, dalam penggunaan *bandwidth* keseluruhan. Kemudian, pada web filtering fitur firewall dapat memblok dan dapat memeriksa keamanan lalu lintas data yang tidak diizinkan sesuai pengaturan konfigurasi pada perangkat fortigate SD-WAN.

REFERENSI

[1] F. Husayn Amir Aldeeb And A. Ali Ahmed, “Software Defined Wide Area Network Sd-Wan: Principles And Architecture,” *4th Int. African Conf. Curr. Stud.*, No. October, 2021.

[2] Fortinet, “Administration Guide 日本語版”, [Online]. Available: Https://Docs.Fortinet.Com/Document/Fortigate/6.4.12/Administration-Guide/954635/Getting-Started

[3] Michael Cooney And Keith Shaw, “What Is Sd-Wan, And What Does It Mean For Networking, Security, Cloud?,” *Networkworld*, 2022. Https://Www.Networkworld.Com/Article/3031279/Sd-Wan-What-It-Is-And-Why-You-Ll-Use-It-One-Day.Html (Accessed Oct. 17, 2023).

[4] Pt Telkom Indonesia, “Astinet,” 2018. Https://Mycarrier.Telkom.Co.Id/Id/Astinet (Accessed Jun. 16, 2023).

[5] Pt Telekomunikasi Indonesia, “Penyediaan Koneksi Internet Astinet & Astinet Lite,” *Propos. Prod.*, No. 021, P. 6, 2018, [Online]. Available: Https://Smartbisnis.Id/Solusi-Bisnis/Astinet-Lite

[6] Zaenal Mustofa M.Kom, “Pengertian Vpn, Manfaat, Dan Cara Cerja Vpn,” *Universitas Stekom*, 2023. Https://Teknik-Informatika-S1.Stekom.Ac.Id/Informasi/Baca/Pengertian-Vpn-Manfaat-Dan-Cara-Cerja-Vpn/F2449cc99eb4796cefb0fb368f5a7874e7251a19 (Accessed Jun. 16, 2023).

[7] E. Awais Khan And I. Khan Babar, “Implementing Vpn Over Mpls,” *Iosr J. Electron. Commun. Eng.*, Vol. 10, No. 3, Pp. 2278–2834, 2015, Doi: 10.9790/2834-10314853.

[8] H. F. Badran, “Service Provider Networking Infrastructures With Mpls,” *Ieee Symp. Comput.*

Commun. - Proc., Pp. 312–318, 2001, Doi: 10.1109/Iscc.2001.935392.

[9] A. Viswanathani, B. L. Technologies, And Z. Wang, "Evolution Of Multi Protocol Label Switching," No. May, Pp. 165–173, 1998.

[10] I. P. Sari And S. Sukri, "Analisis Penerapan Metode Antrian Hirarchical Token Bucket Untuk Management Bandwidth Jaringan Internet," *J. Resti (Rekayasa Sist. Dan Teknol. Informasi)*, Vol. 2, No. 2, Pp. 522–529, 2018, Doi: 10.29207/Resti.V2i2.458.

[11] Etsi, "Telecommunications And Internet Protocol Harmonization Over Networks (Tiphon); General Aspects Of Quality Of Service (Qos)," *Etsi Tr 101 329 V2.1.1*, Vol. 1, Pp. 1–37, 2020.

[12] Y. A. Pranata, I. Fibriani, And S. B. Utomo, "Analisis Optimasi Kinerja Quality Of Service Pada Layanan Komunikasi Data Menggunakan Ns - 2 Di Pt . Pln (Persero) Jember," Pp. 149–156, 2015.