Analisis Penerapan Teknologi *Traffic Steering* SD-WAN Menggunakan Perangkat *Forti Gate*

Andi Dinda Nurul Fauziah[1)], Hafsah Nirwana[2)], Arni Litha[3)], Ichsan Mahjud[4)]
Program Studi Teknologi Rekayasa Jaringan Telekomunikasi, Jurusan Teknik Elektro, Politeknik Negeri Ujung Pandang
02dindafauziah@gmail.com[1], hanir@poliupg.ac.id[2], arnilitha@poliupg.ac.id[3], ichsan_mahjud@poliupg.ac.id[4]

Abstract

In the current digital transformation era, network providers have long relied on WAN technology to support the business communications of their multi-local companies; however, in terms of infrastructure, cost, and even effectiveness, WAN technology is no longer sufficient to meet the needs and demands of telecommunications customers. In addition, given the magnitude of the company's need for internet network connections, technology is also needed to manage the use of traffic from rental links in the company so that it can optimize bandwidth usage from the link itself. Therefore one of the technological innovations to improve information processes is cloud-based digital innovation such as SD-WAN Traffic Steering technology. In this paper, the SD-WAN network design will be carried out on FortiGate series 50e devices by implementing traffic steering technology which can adjust a link's traffic flow according to the client's wishes. The results of the data obtained indicate that the utilization of ISP links owned by companies (Lintasarta and MNC) has been able to be used optimally, as evidenced by the use of bandwidth on each link successfully used according to the desired settings, where the settings provided have also been adjusted according to parameters of the type of each ISP service so that functionally the existing service link can be used optimally by the company.

Keywords: *SD-WAN, Traffic Steering, FortiGate, ISP, Link*

Abstrak

Di era transformasi digital sekarang perusahaan penyedia jaringan telah lama mengandalkan teknologi WAN untuk mendukung komunikasi bisnis multi-lokal mereka, namun ternyata dari segi infrastruktur, biaya, dan bahkan efektivitasnya teknologi WAN sudah tidak cukup mampu untuk memenuhi kebutuhan dan permintaan dari pelanggan telekomunikasi. Selain itu, mengingat besarnya kebutuhan perusahaan terhadap koneksi jaringan internet maka diperlukan pula teknologi yang mampu menngatur pengguanaan trafik dari penyewaan link yang terdapat pada perusahaan sehingga dapat mengoptimalkan penggunaan bandwidth dari link itu sendiri. Maka dari itu salah satu inovasi teknologi guna meningkatkan proses penyaluran informasi adalah inovasi digital berbasis cloud seperti teknologi Traffic Steering SD-WAN. Pada makalah ini perancangan jaringan SD-WAN akan dilakukan pada perangkat FortiGate serie 50e dengan melakukan penerapan teknologi traffic steering yang dimana mampu mengatur alur trafik sebuah link sesuai dengan keinginan client. Hasil data yang didapatkan menunjukkan bahwa pemanfaatan dari link ISP yang dimiliki perusahaan (Lintasarta dan MNC) sudah mampu digunakan secara optimal yang dibuktikan dengan penggunaan bandwidth pada masing-masing link berhasil digunakan sesuai dengan pengaturan yang diinginkan, dimana pengaturan yang diberikan tersebut juga sudah disesuaikan dengan parameter dari jenis masing-masing layanan ISP sehingga secara fungsional layanan link yang ada dapat digunakan dengan optimal oleh pihak perusahaan.

KataKunci: *SD-WAN, Traffic Steering, FortiGate, ISP, Link*

I. PENDAHULUAN

Inovasi teknologi telekomunikasi berkembang dengan sangat pesat selaras dengan tingginya kebutuhan manusia dalam komunikasi itu sendiri. Peningkatan kinerja, kecepatan, ketepatan, keamanan, dan juga efisiensi biaya menjadi standar dalam mengadopsi teknologi baru. Terlebih di tengah kondisi pandemi *covid*-19 sekarang, kebanyakan perusahaan menerapkan *Work From Home* sehingga proses komunikasi baik berupa pertukaran informasi data antar kantor pusat dengan kantor cabang, hingga rapat atau *meeting* akan lebih intens dilakukan secara daring (online) oleh karena itu ketersediaan dan keandalan jaringan sangat penting adanya, sehingga penerapan konsep teknologi yang mampu mengoptimalkan penggunaan *bandwidth* internet pada sebuah perusahaan akan sangat dibutuhkan.

http://dx.doi.org/10.31963/elekterika.v6i2.3478

Software Defined - Wide Area Network (SD-WAN) adalah sebuah pendekatan yang menggunakan *software* untuk membuat jaringan area luas yang lebih cerdas dan fleksibel. SD-WAN mampu menghubungkan area jaringan perusahaan dari kantor cabang ke *data center* yang ada walaupun terhalangi oleh area geografis yang luas [1].

Produk yang sekarang kerap digunakan untuk menerapkan teknologi SD-WAN adalah perangkat FortiGate. FortiGate merupakan produk unggulan Fortinet yang memang sudah terkenal sebagai platform keamanan terpercaya yaitu dengan 38% total pengiriman di tahun 2022 yang merupakan lebih dari 1/3 total pengiriman perangkat *firewall* secara global [2] melalui FortiGate penerapan SD-WAN dapat dilakukan dengan cepat dan mudah baik itu aktivitas yang dilakukan melalui jaringan inti maupun sumber daya lain dengan berbasis internet.

Traffic Steering pada SD-WAN FortiGate digunakan untuk mengatur jalur tujuan pencarian sesuai dengan interface link ISP (*Internet Service Provider*) yang diinginkan, hal ini dapat mengoptimalkan penggunaaan *bandwidth* link yang ada dan mencegah terjadinya *over load* trafik pada sebuah link sehingga kecepatan koneksi link bisa tetap terjaga dan stabi .

Penelitian ini akan berfokus melakukan penerapan teknologi *traffic steering* pada jaringan SD-WAN FortiGate, dimana akan menjawab bagaimana konsep kerja dari SD-WAN FortiGate, bagaimana penerapan *traffic steering* pada jaringan dan pengaruhnya terhadap performa jaringan SD-WAN pada perangkat FortiGate itu sendiri.

II. KAJIAN LITERATUR

2.1. *Software Define Wide Area Network* Pada Perangkat FortiGate

SD-WAN adalah sebuah pendekatan untuk membuat arsitektur WAN yang lebih mudah digunakan, dioperasikan dan dikelola. SD-WAN mampu meningkatkan efisiensi proses transfer data pada WAN secara keseluruhan dengan memindahkan lalu lintas ke link MPLS, 4G/5G LTE, ataupun ke koneksi lainnya secara mandiri. Dengan SD-WAN kita mampu melakukan perutean, perlindungan data dari ancaman, meningkatkan kinerja jaringan, dan menyederhanakan manajemen jaringan pada WAN itu sendiri [3]. Kemudian perangkat yang digunakan dalam penerapan teknologi SD-WAN ini adalah FortiGate. Perangkat FortiGate merupakan sebuah sistem keamanan berupa hardware maupun software yang dikeluarkan oleh perusahaan Fortinet. FortiGate mampu mengatur *traffic* jaringan sekaligus mampu menjaga keamanan dari traffic jaringan itu sendiri [4]. Dimana dalam penelitian ini, seri FortiGate yang digunakan adalah FortiGate 50e.

2.2. *Policies For* SD-WAN FortiGate

Perangkat FortiGate merupakan jenis router *firewall*, sehingga dibutuhkan konfigurasi *policy* yang berfungsi untuk memberikan izin akses trafik dari jaringan internal yang dibuat ke zona SD-WAN terlebih dahulu (LAN dan WAN) [5]. Ketika *policy* sudah berhasil dibuat, maka dari sisi *interface* LAN akan bisa berkomunikasi ke *interface* WAN dan begitu pula sebaliknya.

2.3. SD-WAN *Rules*

SD-WAN *Rules* digunakan untuk mengontrol pemilihan jalur lalu lintas tertentu agar proses pengiriman datanya dapat dilakukan secara dinamis ke tautan yang diinginkan [6], dimana dalam penelitian ini akan dipilih mode '*manual*'. Mode ini dipilih untuk memungkinkan peneliti dalam memilih jalur trafik yang diinginkan sesuai dengan link ISP yang tersedia.

2.4. *Routing*

Perutean adalah sebuah mekanisme untuk mengarahkan serta menentukan jalur yang akan dilalui oleh sebuah paket data dari device satu ke device yang lain dalam sebuah jaringan. Konsep dasar routing sendiri berada dilapisan jaringan TCP/IP dimana pada lapisan ini terjadi proses pemberian alamat pada setiap *user* atau perangkat. Pada umumnya semua router, termasuk perangkat FortiGate telah diatur menggunakan *default routes* 0.0.0.0/0.0.0.0 (*ip destination*/netmask). Ini dilakukan agar proses mengatur operasional jaringan bisa menjadi lebih cepat terutama bagi *beginner administrator* (administrator pemula) kecuali terdapat case selama pembuatan jaringan yang memerlukan konfigurasi-konfigurasi lain [8].

http://dx.doi.org/10.31963/elekterika.v6i2.3478

2.5. *Traffic Steering*

Traffic Steering adalah teknik tambahan yang diterapkan pada lalu lintas jaringan terutama ketika suatu filtering, modifikasi atau optimasi dibutuhkan [9]. Teknik ini diterapkan agar penggunaan *traffic* dari sebuah link dapat diarahkan sesuai dengan kebutuhan client sehingga dapat lebih mengoptimalkan penggunaan fungsional dari link itu sendiri. Fortinet menawarkan konsep *Traffic Steering* yang cerdas, mampu mengarahkan aplikasi tertentu, protokol dan lalu lintas pelanggan untuk memastikan bahwa hanya link yang diinginkan saja yang digunakan sehingga secara signifikan meminimalkan jumlah node layanan dan sumber daya jaringan lain yang akan meningkatkan fungsional dari sebuah link.

2.6. *Internet Service Provider* (ISP)

ISP atau *Internet Service Provider* adalah produsen atau lembaga yang memberikan pelayanan kepada konsumen agar bisa mengakses internet dan berbagai media online. Terdapat 2 kategori koneksi internet yang banyak digunakan yaitu *internet broadband* dan *internet dedicated*. Secara garis besar, *internet broadband* merupakan jenis layanan yang biasanya digunakan untuk koneksi internet rumahan berbagai perangkat seperti *smartphone* dimana dari segi kecepatan maupun performansi nya akan terbagi ke setiap pengguna, berbeda dengan layanan *internet dedicated*. Koneksi yang disediakan oleh layanan *internet dedicated* dipusatkan penggunaannya secara privat sehingga performansi dan kecepatan koneksi nya bisa digunakan oleh 1 *user* secara penuh, itu sebabnya jenis layanan ini lebih sering digunakan untuk kepentingan bisnis seperti kantor perusahaan atau *co-working space*. Dalam penelitian ini akan digunakan 2 link yaitu link ISP Lintasarta (jenis *internet dedicated*) dan link ISP MNC (jenis *internet broadband*).

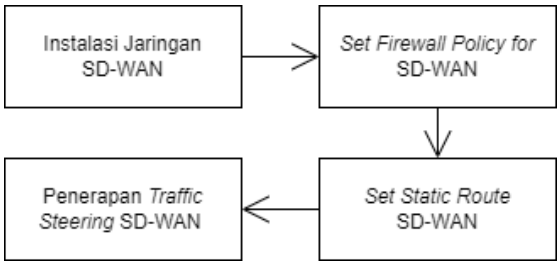
III. METODE PENELITIAN

Penelitian ini dilakukan di PT. Media Telekomunikasi Mandiri (MTM), bertempat di ITS Tower 9th Floor – Jl. Raya Pasar Minggu No.18, Jakarta Selatan, Indonesia. Adapun alat dan bahan yang digunakan selama penelitian berlangsung ditunjukkan pada Tabel 1 berikut :

Tabel 1. Alat Dan Bahan

Nama Alat Dan Bahan	Jumlah
Laptop atau PC	1 Buah
Perangkat FortiGate 50e	1 Buah
Kabel UTP	3 Buah
Link *Internet Service Provider*	2 Link
Command Prompt	1 Buah

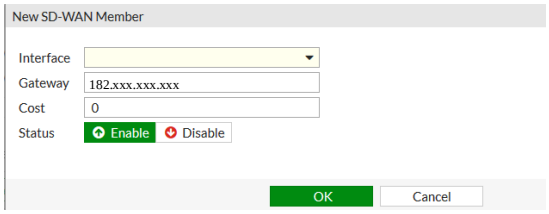
Pada penelitian ini akan dilakukan perancangan melalui sebuah simulasi menggunakan perangkat FortiGate 50e. Tujuan simulasi ini adalah untuk mendapatkan gambaran mengenai konfigurasi apa saja yang perlu dilakukan dalam pembuatan jaringan SD-WAN – *Traffic Steering*. Mulai dari penginstalan jaringan SD-WAN itu sendiri, penyetingan *policy* SD-WAN dan *static routing*, hingga penerapan SD-WAN *Rules* seperti pada Gambar 1.



Gambar 1. *Blok Diagram Tahapan Perancangan*

3.1. Instalasi Jaringan SD-WAN

Instalasi jaringan SD-WAN akan dilakukan melalui GUI yang tersedia pada perangkat FortiGate.. Hal yang perlu diperhatikan adalah perangkat FortiGate yang akan diakses melalui GUI ini harus dalam keadaan Aktif/menyala dan memiliki IP yang sudah dapat diakses secara online [3]. Perancangan dilakukan dengan penambahan SD-WAN member untuk interface WAN1 (Link Lintasarta) dan WAN2 (Link MNC), mengatur '*Gateway*' WAN1 dan WAN2 sesuai dengan IP masing-masing dari Link Lintasarta dan MNC, dan nilai *cost* sebesar 0 [10].



Gambar 2. *Perancangan Jaringan SD-WAN*

http://dx.doi.org/10.31963/elekterika.v6i2.3478

3.2. *Set Firewall Policy for* SD-WAN

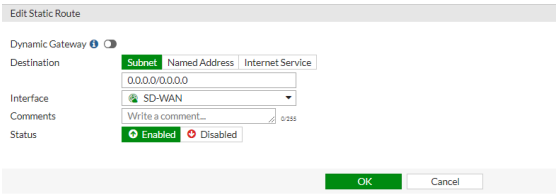
Pada langkah ini akan dilakukan penambahan 2 *policy* untuk memungkinkan WAN dan LAN dalam jaringan dapat saling terhubung dengan pengaturan parameter seperti yang ditunjukkan pada Tabel 2. Selain itu hal yang perlu diperhatikan juga adalah untuk *reordering* (mengubah urutan) *policy* yang telah dibuat sesuai dengan prioritasnya, dimana dalam hal ini adalah LAN TO WAN → WAN TO LAN.

Tabel 2. *Setting Paramater Policy* SD-WAN

Name	LAN TO WAN	WAN TO LAN
Incoming Interface	LAN-OFFICE	SD-WAN
Outgoing Interface	SD-WAN	LAN-OFFICE
Source, Destination, Schedule, Service, Action	All, All, Always, All, Accept	All, All, Always, All, Accept
NAT	Enable	Disable

3.3. *Set Static Route* SD-WAN

Static route yang akan diterapkan adalah *default routing* dengan 0.0.0.0/0.0.0.0 sebagai IP destinasi dan netmask nya [8].



Gambar 3. *Setting Static Route* pada SD-WAN

3.4. Penerapan *Traffic Steering* SD-WAN

Penerapan *traffic steering* dapat dilakukan dengan menambahkan parameter SD-WAN *Rules* ke dalam jaringan SD-WAN yang telah di konfigurasi sebelumnya, ini dilakukan agar kita dapat mengontrol pemilihan jalur *traffic* sesuai dengan link yang diinginkan [3]. Untuk memungkinkan dilakukannya *Traffic Steering* pada jaringan, maka mode/metode SD-WAN *Rules* yang harus digunakan adalah mode *manual*. Strategi ini diterapkan agar kita dapat mengatur secara manual jenis *Interface* mana yang akan melalui link yang diinginkan [3]. Dalam penelitian ini terdapat 2 jenis *Interface* yang kemudian nantinya akan di arahkan ke 2 link yang berbeda, Link Lintasarta (WAN1) ditujukan sebagai *traffic Interface* LAN_OFFICE dimana *setting*-an ini akan mengarahkan semua permintaan user terhadap data perusahaan hanya melalui Link Lintasarta saja . Sedangkan untuk Link MNC (WAN2) ditujukan sebagai *traffic Interface* Sosial Media, sehingga ketika user meminta akses ke sebuah sosial media akan secara otomatis diarahkan melalui link MNC, sehingga diperlukan 2 SD-WAN *rules* yaitu TRAFFIK-STEERING_APK-OFFICE (untuk WAN1) dan TRAFFIK-STEERING_APK-SOSMED (untuk WAN2) dengan *setting* parameter seperti yang ditunjukkan pada Tabel 3. Dan sama hal nya dengan pengaturan *policy* SD-WAN sebelumnya, perlu dilakukan *reordering* SD-WAN *rules* yaitu dengan urutan TRAFFIK-STEERING_APK-OFFICE → TRAFFIK-STEERING_APK-SOSMED

Tabel 3. *Create* SD-WAN *Rules*

TRAFFIC-STEERING_ APK-OFFICE	TRAFFIC-STEERING_ APK-SOSMED
Source Address > LAN_OFFICE	*Source Address* > ALL
Destination Internet Service dan *Application* > pilih semua jenis aplikasi office yang kiranya akan diakses dalam jaringan. seperti Email, Microsoft Office 365, dsb.	*Destination Address* > ALL
Outgoing Interface Strategy > Manual	*Outgoing Interface Strategy* > Manual
Interface Preferences > WAN1	Interface Preferences > WAN2

3.5. Teknik Pengolahan dan Analisis Data

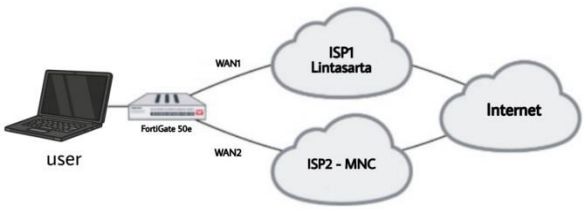
Pengolahan data dilakukan dengan cara mengumpulkan semua hasil-hasil data yang telah didapatkan melalui sebuah simulasi perancangan jaringan sehingga dapat dianalisis Selain itu, dilakukan uji keberhasilan dari jaringan yang sudah dirancang tersebut. Proses uji keberhasilan jaringan akan dilakukan dengan men-*tracking* apakah pemilihan jalur lalu lintas suatu link sudah sesuai dengan yang kita inginkan atau tidak, sehingga proses pengiriman data dapat dilakukan secara dinamis ke tautan yang terbaik. Hasil dari simulasi dan uji keberhasilan jaringan yang dilakukan ini kemudian dianalisis sehingga dapat mencapai sebuah pemahaman dan kesimpulan akhir mengenai proses pengumpulan dan pengolahan data.

http://dx.doi.org/10.31963/elekterika.v6i2.3478

IV. HASIL DAN PEMBAHASAN

Hasil penelitian ini dibagi menjadi tiga yaitu hasil penerapan jaringan SD-WAN pada FortiGate, penerapan konsep *traffic steering* pada jaringan SD-WAN, dan performa jaringan setelah penerapan konsep *traffic steering* dalam jaringan SD-WAN FortiGate. Masing-masing hasil dapat dijabarkan sebagai berikut:

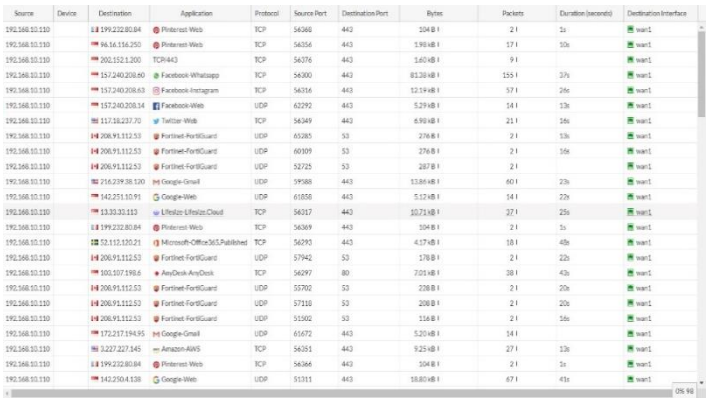
4.1. Penerapan Jaringan SD-WAN pada FortiGate



Gambar 4. Topologi Jaringan SD-WAN

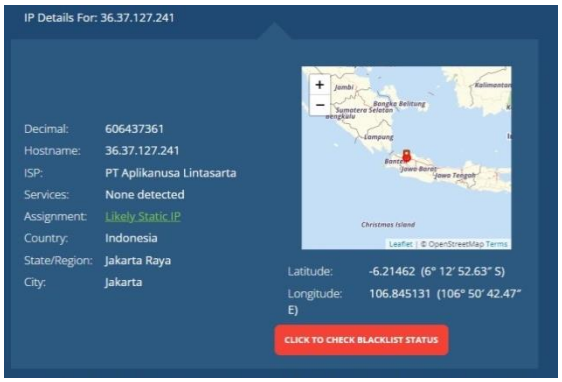
Konfigurasi yang dilakukan akan membentuk jaringan SD-WAN dengan 2 akses link ISP. Perancangan ini memungkinkan perangkat untuk mengakses data-data melalui trafik dari link yang tersedia tersebut. Namun apabila pengaturan penggunaan tiap link ISP tidak dilakukan, maka permintaan setiap akses yang dilakukan user hanya akan dilewatkan melalui salah satu trafik link saja yang dalam kasus ini adalah WAN1-Lintasarta. akibatnya pemanfaatan link yang ada hanya akan terpusat pada salah satu ISP saja dimana hal ini mengakibatkan tidak optimalnya penggunaan link-link yang terdapat pada suatu perusahaan. Hal ini dapat dibuktikan dengan melakukan pengambilan data terhadap alur trafik selama proses penelitian berlangsung. Gambar 5 menunjukkan bahwa semua permintaan akses yang dilakukan oleh user diarahkan melalui satu link saja yaitu WAN1. baik itu akses yang dilakukan untuk keperluan *official* kantor maupun akses menuju aplikasi sosial media seperti *Instagram*, *Facebook, Twitter* dan lain sebagainya. Selain melakukan pengetesan langsung pada perangkat FortiGate, pengamatan alur trafik juga dapat dilakukan menggunakan *Command Prompt* yaitu dengan melakukan tes *ping* dan *tracert route. Ping* dilakukan untuk melihat keberhasilan koneksi dalam jaringan dengan mengirimkan 4 paket ICMP ke salah satu layanan sosial media yaitu *Instagram.com* (157.240.208.174), hasil tes ping yang dilakukan menunjukkan pengiriman semua paket ICMP berstatus *Reply* dengan presentasi 0% *packet loss*, ini membuktikan koneksi internet melalui Link ISP telah berjalan dengan baik. Sedangkan *tracert route* dilakukan untuk melihat lompatan alur trafik yang dilalui mulai dari user hingga sampai ke tujuan permintaan akses yang diinginkan, dan melalui lompatan tersebut IP *public* dari link ISP yang digunakan saat itu dapat terlihat. Gambar 6 menunjukkan bahwa semua permintaan akses yang dilakukan oleh user saat ini masih diarahkan melalui trafik link WAN1 saja, ini dibuktikan dengan terdeteksinya IP publik dari link WAN1-Lintasarta (36.37.127.241) ketika *tracert route* dilakukan.

Penerapan Teknologi SD-WAN dilakukan dengan memberikan beberapa konfigurasi langsung pada perangkat FortiGate 50e yaitu dengan melakukan perancangan jaringan SD-WAN dan penambahan link WAN1 dan WAN2 sesuai dengan IP masing-masing ISP (Lintasarta dan MNC), kemudian melakukan *setting static route* dan *firewall policy* untuk memungkinkan terjadinya koneksi pada jaringan SD-WAN. Gambaran setelah penerapan teknologi SD-WAN pada FortiGate ditunjukkan pada Gambar 4 di bawah ini:



Gambar 5. Pengamatan Alur Trafik sebelum penerapan *traffic steering*

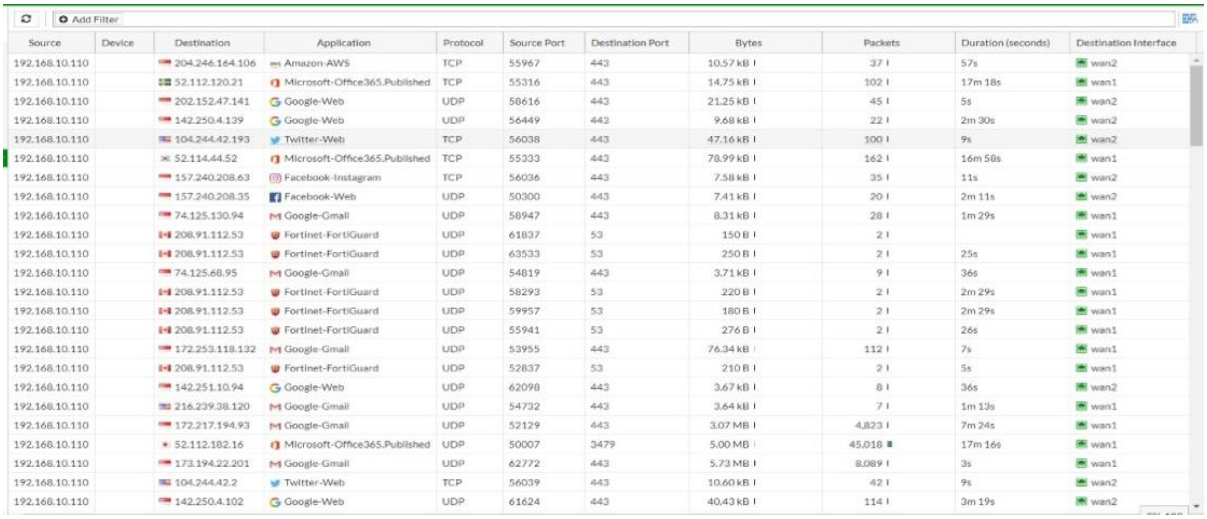
http://dx.doi.org/10.31963/elekterika.v6i2.3478



Gambar 6. Detail IP Public WAN1-Lintasarta

4.2. Penerapan Konsep *Traffic Steering* pada Jaringan SD-WAN

Setelah perancangan jaringan SD-WAN telah berhasil dilakukan, langkah selanjutnya adalah dengan menerapkan konsep *Traffic Steering* kedalam jaringan SD-WAN. yaitu dengan melakukan konfigurasi SD-WAN *Rules*. Langkah konfigurasi yang dilakukan berupa penambahan 2 *rules* baru yaitu TRAFFIC-STEERING_APK-OFFICE yang ditujukan untuk mengatur penggunaan link WAN1-Lintasarta dan *rules* TRAFFIC-STEERING_APK-SOSMED untuk mengatur penggunaan pada link WAN2-MNC. Konsep *Traffic Steering* berfungsi untuk mengatur arah trafik dari permintaan akses user terhadap sebuah data tertentu, dimana dalam hal ini data yang dimaksudkan adalah pada kegunaan data *official* kantor (*Microsoft Office*, *Dropbox*, *Email*, dsb) dan *non-official* kantor atau lebih tepatnya sosial media seperti *Instagram*, *Facebook*, *Twitter* dan lain sebagainya. Sebelum penerapan *Traffic Steering* dilakukan semua permintaan data tersebut masih diarahkan melalui satu link saja yaitu WAN1, namun setelah settingan SD-WAN *Rules* diberikan akses data *official* kantor hanya akan diarahkan menggunakan layanan link dari ISP Lintasarta (WAN1) saja sedangkan untuk akses data sosial media akan menggunakan layanan ISP MNC (WAN2). Dari hasil pengambilan data yang ditunjukkan pada Gambar 7 dapat diketahui bahwa setelah penerapan konsep *Traffic Steering* dilakukan pada jaringan SD-WAN, alur trafik yang awalnya hanya diarahkan melalui WAN1 telah berubah sesuai dengan settingan SD-WAN *Rules* yang telah diberikan. Dapat dilihat bahwa semua aplikasi *official* kantor seperti *Microsoft Office*, *Google-Gmail* dan lain sebagainya hanya diarahkan melalui link WAN1-Lintasarta. Sedangkan untuk trafik pada link WAN2-MNC hanya dilalui oleh akses terhadap data-data sosial media seperti *Instagram*, *Twitter*, *Facebook*, dan sebagainya. Hal ini juga bisa dibuktikan melalui tes *ping* dan *tracert route*. hasil ping yang telah dilakukan terhadap IP yang juga sama dengan sebelumnya yaitu 157.240.208.174 (*Instagram.com*) menunjukkan pengiriman 4 paket ICMP berstatus *Reply* dengan presentasi 0% *Packet Loss*.

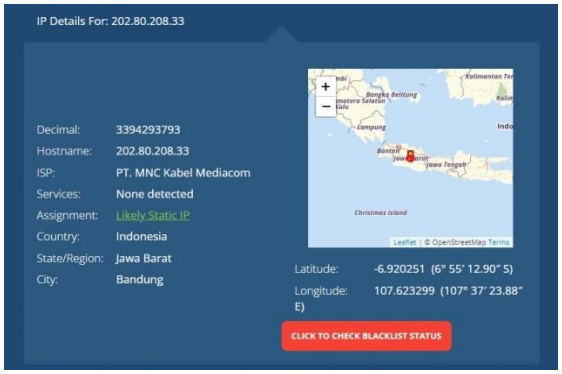


Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	Packets	Duration (seconds)	Destination Interface
192.168.10.110		204.246.164.106	Amazon-AWS	TCP	55967	443	10.57 kB	37	57s	wan2
192.168.10.110		52.112.120.21	Microsoft-Office365.Published	TCP	55316	443	14.75 kB	102	17m 18s	wan1
192.168.10.110		202.152.47.141	Google-Web	UDP	58616	443	21.25 kB	45	5s	wan2
192.168.10.110		142.250.4.139	Google-Web	UDP	56449	443	9.68 kB	22	2m 30s	wan2
192.168.10.110		104.244.42.193	Twitter-Web	TCP	56038	443	47.16 kB	100	9s	wan2
192.168.10.110		52.114.44.52	Microsoft-Office365.Published	TCP	55333	443	78.99 kB	162	16m 58s	wan1
192.168.10.110		157.240.208.63	Facebook-Instagram	TCP	56036	443	7.58 kB	35	11s	wan2
192.168.10.110		157.240.208.35	Facebook-Web	UDP	50300	443	7.41 kB	20	2m 11s	wan2
192.168.10.110		74.125.130.94	Google-Gmail	UDP	58947	443	8.31 kB	28	1m 29s	wan1
192.168.10.110		208.91.112.53	Fortinet-FortiGuard	UDP	61837	53	150 B	2		wan1
192.168.10.110		208.91.112.53	Fortinet-FortiGuard	UDP	63533	53	250 B	2	25s	wan1
192.168.10.110		74.125.68.95	Google-Gmail	UDP	54819	443	3.71 kB	9	36s	wan1
192.168.10.110		208.91.112.53	Fortinet-FortiGuard	UDP	58293	53	220 B	2	2m 29s	wan1
192.168.10.110		208.91.112.53	Fortinet-FortiGuard	UDP	59957	53	180 B	2	2m 29s	wan1
192.168.10.110		208.91.112.53	Fortinet-FortiGuard	UDP	55941	53	276 B	2	26s	wan1
192.168.10.110		172.253.118.132	Google-Gmail	UDP	53955	443	76.34 kB	112	7s	wan1
192.168.10.110		208.91.112.53	Fortinet-FortiGuard	UDP	52837	53	210 B	2	5s	wan1
192.168.10.110		142.251.10.94	Google-Web	UDP	62098	443	3.67 kB	8	36s	wan2
192.168.10.110		216.239.38.120	Google-Gmail	UDP	54732	443	3.64 kB	7	1m 13s	wan1
192.168.10.110		172.217.194.93	Google-Gmail	UDP	52129	443	3.07 MB	4,823	7m 24s	wan1
192.168.10.110		52.112.182.16	Microsoft-Office365.Published	UDP	50007	3479	5.00 MB	45,018	17m 16s	wan1
192.168.10.110		173.194.22.201	Google-Gmail	UDP	62772	443	5.73 MB	8,089	3s	wan1
192.168.10.110		104.244.42.2	Twitter-Web	TCP	56039	443	10.60 kB	42	9s	wan2
192.168.10.110		142.250.4.102	Google-Web	UDP	61624	443	40.43 kB	114	3m 19s	wan2

Gambar 7. pengamatan Alur Trafik setelah penerapan *traffic steering*

http://dx.doi.org/10.31963/elekterika.v6i2.3478

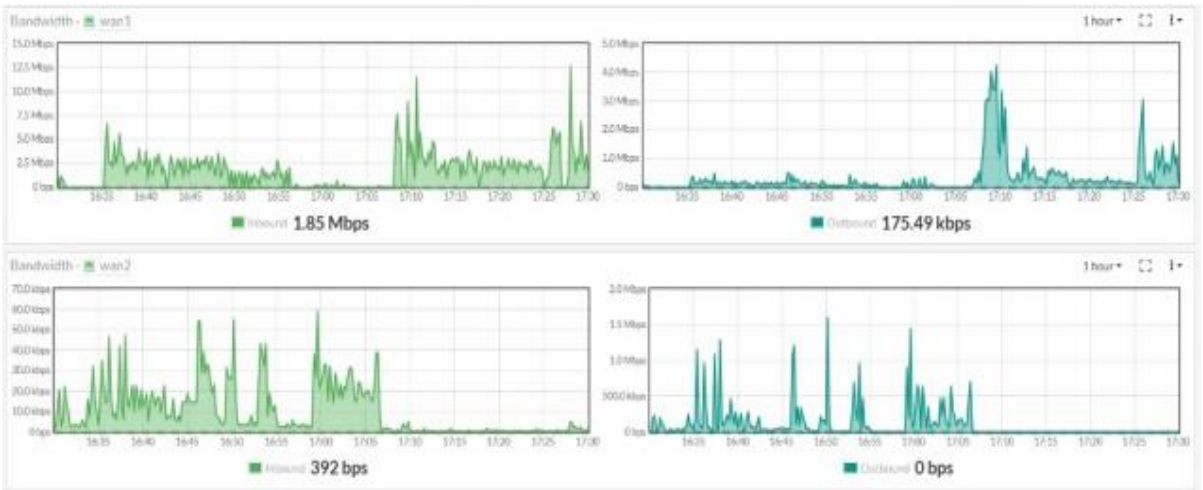
Sedangkan untuk hasil tes *tracert route* IP WAN1-Lintasarta tidak lagi terdeteksi seperrti sebelumnya, melainkan IP dari ISP WAN2-MNC yaitu 202.80.208.33 seperti yang ditunjukkan pada Gambar 8. Hal ini membuktikan bahwa permintaan akses terhadap data-data sosial media sudah berhasil diarahkan melalui link WAN2-MNC setelah penerapan konsep *Traffic Steering* dilakukan.



Gambar 8. Detail IP Public WAN2-MNC

4.3. Performa Jaringan Dengan Penerapan Konsep *Traffic Steering* dalam Jaringan SD-WAN FortiGate

Salah satu cara untuk mengetahui bagaimana performa sebuah jaringan adalah dengan mengamati penggunaan *bandwidth* di dalam jaringan SD-WAN itu sendiri. Penggunaan *bandwidth* dalam jaringan SD-WAN dapat kita amati pada *dashboard* GUI FortiGate. Pada satu jam pertama akan dilakukan pengambilan data sebelum konsep *Traffic Steering* diterapkan, sedangkan untuk data setelah penarapan konsep *Traffic steering* akan dilakukan pada satu jam selanjutnya. Pengambilan data dilakukan dengan mengamati besar penggunaan *bandwidth* oleh perangkat *user* ketika sedang mengakses aplikasi maupun *website* baik itu untuk keperluan *official* kantor ataupun akses *user* terhadap sosial media dimana besar penggunaan *bandwidth* perangkat *user* pada jaringan akan ditunjukkan di *dashboard* GUI FortiGate yang ditampilkan dalam bentuk grafik dengan parameter waktu dan besar penggunaan *bandwidth* dari tiap link baik WAN1 dan WAN2. Dari hasil grafik pada Gambar 9 dapat diketahui bahwa penggunaan *bandwidth* pada link WAN1 sebelum penerapan konsep *Traffic Steering* memiliki rata-rata penggunaan sebesar 1.85 Mbps dengan nilai tertinggi ± sebesar 12.5 Mbps. Sedangkan untuk rata-rata penggunaan *bandwidth* pada link WAN2 hanya sebesar 392 bps dengan penggunaan tertinggi mencapai 60 Kbps saja, dimana nilai ini bisa dianggap tidak terpakai, sehingga dapat kita simpulkan bahwa sebelum penerapan konsep *Traffic Steering* dilakukan pemanfaatan layanan link ISP yang ada memang hanya diarahkan pada WAN1 sehingga dari segi penggunaan *bandwidth*-nya pun *juga* hanya dipusatkan pada link WAN1 saja. Dari hal ini dapat kita ketahui bahwa pemanfaatan layanan link dari ISP yang terdapat pada perusahaan bisa menjadi tidak optimal. Itu sebabnya diperlukan suatu penerapan konsep dalam jaringan yang mampu mengatur alur trafik dari penggunaan link tersebut yaitu *Traffic Steering*.



Gambar 9. Penggunaan *bandwidth* dalam jaringan sebelum penerapan *traffic steering*

http://dx.doi.org/10.31963/elekterika.v6i2.3478

Kemudian data penggunaan *bandwidth* setelah penerapan *traffic steering* dilakukan dapat dilihat pada Gambar 10 dan dari hasil grafik tersebut dapat diketahui bahwa penggunaan *bandwidth* baik pada WAN1 dan WAN2 sudah mulai berbeda. Untuk link WAN1-Linstasarta terpantau memiliki rata-rata penggunaan *bandwidth* sebesar 2.92 Mbps dengan penggunaan tertinggi mencapai 12 Mbps, sedangkan penggunaan *bandwidth* pada link WAN2-MNC memiliki nilai rata-rata sebesar 5.78 Mbps dengan penggunaan tertinggi yang terpantau sama yaitu kurang lebih 12 Mbps. Dengan kata lain, permintaan akses untuk data *non-official* yang dilakukan oleh *user* sudah berhasil dialihkan menuju link WAN2-MNC sehingga *bandwidth* dari link tersebut juga sudah mulai digunakan. Maka dapat disimpulkan bahwa kedua link dari layanan ISP yang terdapat pada perusahaan baik itu ISP Lintasarta maupun MNC sudah dapat digunakan dengan optimal dimana pemilihan alur trafik untuk masing-masing link tersebut juga sudah berhasil diterapkan sesuai dengan *setting* yang diinginkan.

Gambar 10. Penggunaan *bandwidth* dalam jaringan setelah penerapan *traffic steering*

V. KESIMPULAN

Setelah melakukan proses perancangan, pengujian, serta analisis pada penerapan konsep teknologi *traffic steering* SD-WAN menggunakan perangkat FortiGate maka dapat disimpulkan bahwa :

1. Perancangan jaringan SD-WAN yang telah dilakukan pada perangkat FortiGate 50e mengarahkan semua alur trafik dari user hanya melalui link WAN1-Lintasarta saja baik itu permintaan akses terhadap data official kantor maupun data sosial media, sehingga penggunaan *bandwidth* hanya terpusat pada link ISP WAN1 saja. Hal ini dapat dibuktikan dengan hasil penggunaan *bandwidth* pada link WAN1 yang mencapai rata-rata 1.85 Mbps dengan penggunaan tertinggi mencapai ± 12.5 Mbps, sedangkan utuk WAN2-MNC hanya memiliki rata-rata sebesar 392 bps dengan penggunaan tertinggi mencapai 60 Kbps saja.
2. Penerapan konsep *traffic steering* ke dalam jaringan SD-WAN membuat alur trafik dari permintaan akses user berubah sesuai dengan pengaturan yang telah diberikan yaitu alur trafik link WAN1-Lintasarta hanya digunakan untuk akses data official kantor dan alur trafik link WAN2-MNC digunakan untuk akses data sosial media, sehingga *bandwidth* pada link ISP WAN2 juga sudah mulai aktif digunakan, ini dibuktikan dengan penggunaan bandwidth pada link WAN 1 yang terpantau memiliki rata-rata sebesar 2.92 Mbps dengan penggunaan tertinggi mencapai 12 Mbps dan untuk WAN 2 memiliki rata-rata penggunaan bandwidth sebesar 5.78 Mbps dengan nilai tertinggi mencapai 12 Mbps setelah penerapan *traffic steering* dilakukan.
3. Hasil pengiriman paket data ICMP melalui tes *ping* selama proses simulasi semuanya berhasil dilakukan dengan presentasi 0% *Packet loss*, hal ini menunjukkan bahwa konektivitas jaringan SD-WAN sudah berjalan dengan baik.
4. Hasil alur trafik dan penggunaan *bandwidth* pada jaringan SD-WAN FortiGate setelah penerapan konsep *traffic*

http://dx.doi.org/10.31963/elekterika.v6i2.3478

steering dilakukan menunjukkan bahwa pemanfaatan kedua link ISP yang terdapat pada perusahaan baik dalam segi konektivitas dan penggunaan *bandwidth*-nya sudah dapat dimanfaatkan secara optimal.

UCAPAN TERIMA KASIH

Penulis mengucapkan banyak terimakasih kepada Pihak PT. Media Telekomunikasi Mandiri (MTM) terutama Dept. *Integrated Operation Center* Divisi *Service Device Engineering* atas pemberian akses dan dukungan terhadap penelitian yang dilakukan.

REFERENSI

[1] Fortinet, *The Network Leader's Guide To Secure SD-WAN*, 372656-C-0-EN, 2021.
[2] Fortinet, *Analyst Day*, 2022.
[3] FortiOS, *Cookbook Version 6.2.9*, 01-629-538742-2021092, 2021.
[4] Sari, Dewi., A.I. Islami, "Implementasi Web Filtering Menggunakan Router Fortigate FG300D", Jurnal Inovasi dan Sains Teknik Elektro, Vol. 2, No, 2021.
[5] FortiOS 7.0.2, "Policies", Fortinet Document Library-Administration Guide, 2021.
[6] Fortinet Handbook, "Configuring SD-WAN Rules", Document Library-Administration Guide, 2021.
[7] Suminar, Pujowati., B.B Harianto, "Pengenalan Dasar Jaringan Komputer", Magelang: Pustaka Rumah C1nta, 2021.
[8] FortiOS 6.0.0, "Routing Concepts" Document Library-Administration Guide, 2021.
[9] Sandvine, *Traffic Steering/Diversion Intelligently Redirectly Traffic And Better Allocate Network Resources*, V20180703, 2018.
[10] Fortinet Cookbook, "Configuring the SD-WAN Interface Document Library-Administration Guide, 2021.

http://dx.doi.org/10.31963/elekterika.v6i2.3478