Peningkatan Keamanan Dan Efisiensi Branch Office Dengan Cisco Software-Defined WAN (SD-WAN)

(Studi Kasus : Bank XYZ)

[1]Febryo Ponco Sulistyo

Fakultas Ilmu Komputer, Universitas Mercu Buana[1]

febryo.ponco@mercubuana.ac.id

***Abstract* - Digital transformation has ushered in a new era of long-lasting IT infrastructure changes. These changes have resulted in new challenges for the network and security teams, such as securing the distributed and hybrid workforce and delivering secure access to business-critical applications across a multicloud environment. In addition, the internet is rapidly becoming the preferred method of connectivity due to cost and availability. Still, it does not provide the security, consistency, visibility, or quality of traditional technologies such as Multiprotocol Label Switching (MPLS) links. IT needs to rearchitect its WAN edge to deliver consistent and predictable digital experiences in a multicloud world.Cisco® SD-WAN is a cloud-delivered WAN solution that connects any user to any application, with integrated capabilities such as multicloud, security, enhanced visibility, and analytics building toward a Secure Access Service Edge (SASE)-enabled architecture. Software Defined WAN or better known as SD-WAN has now become a technology that is hype and has a lot of interest, in addition to simplifying SD-WAN operations, it can also reduce operational costs, especially links. Researchers will make it within the scope of the PoC Lab (Proof of Concept) so that later the results from this PoC can show the expected results, namely being able to improve the security of connections between branches and the results achieved by devices between branches whose connections are successful using SD-WAN with traffic and data that already encrypted with IPSEC and also other features by the Cisco SD-WAN**

Keyword:Cisco SD-WAN, Network Security, Multi-Branch, Eficiency

***Abstrak* – Transformasi digital telah mengantarkan era baru perubahan infrastruktur TI yang tahan lama. Perubahan ini menghasilkan tantangan baru bagi tim jaringan dan keamanan, seperti mengamankan tenaga kerja hybrid dan terdistribusi serta memberikan akses yang aman ke aplikasi bisnis penting di lingkungan multicloud. Selain itu, internet dengan cepat menjadi metode konektivitas yang disukai karena biaya dan ketersediaan. Namun, itu tidak memberikan keamanan, konsistensi, visibilitas, atau kualitas teknologi tradisional seperti tautan Multiprotocol Label Switching (MPLS). TI perlu merancang ulang keunggulan WAN-nya untuk menghadirkan pengalaman digital yang konsisten dan dapat diprediksi di dunia multicloud. Cisco® SD-WAN adalah solusi WAN yang dihadirkan cloud yang menghubungkan setiap pengguna ke aplikasi apa pun, dengan kemampuan terintegrasi seperti multicloud, keamanan, visibilitas yang ditingkatkan , dan pembangunan analitik menuju arsitektur yang mendukung Secure Access Service Edge (SASE). Software Defined WAN atau yang lebih dikenal dengan SD-WAN kini telah menjadi teknologi yang sedang hype dan banyak peminatnya, selain dapat mempermudah operasional SD-WAN juga dapat menekan biaya operasional khususnya link. Peneliti akan membuatnya dalam ruang lingkup Lab PoC (Proof of Concept) sehingga nantinya hasil dari PoC ini dapat menunjukkan hasil yang diharapkan yaitu mampu meningkatkan keamanan koneksi antar cabang dan hasil yang dicapai oleh perangkat antar cabang yang koneksi berhasil menggunakan SD-WAN dengan lalu lintas dan data yang sudah dienkripsi dengan IPSEC dan juga fitur lain oleh Cisco SD-WAN**

Keyword: Cisco SD-WAN, Network Security, Multi-Branch, Efisiensi

I. PENDAHULUAN

Bank XYZ adalah salah satu dari Bank Buku III di Indonesia sehingga menjadikan Bank ini adalah Bank yang memiliki asset yang sangat besar dan juga nasabah yang banyak maka dari itu penting bagi Bank XYZ untuk meningkatkan pelayanan dan juga menjaga kepercayaan dari nasabh-nasabahnya. Serta Bank XYZ ini juga memiliki lebih dari 100 cabang termasuk cabang pembantu dan juga kantor fungsional dan memiliki lebih dari 100 ATM di yang tersebar di seluruh Indonesia. Maka dari itu, dibutuhkan sebuah solusi yang dapat meningkatkan keamanan dan juga mengefisiensi kan biaya serta mempercepat performance untuk network antar cabang sehingga dapat tercapai layanan yang reliable, cepat, hemat dan aman.[1]

Software Defined WAN atau lebih dikenal dengan SD-WAN adalah salah satu penerapan teknologi SDN untuk mengkontrol WAN [2] dan sangat berguna apabila kamu memiliki ratusan hingga ribuan cabang Sebenarnya penerapan teknologi SDN sudah lama diterapkan salah satunya pada implementasi WLAN dimana WLC mengkontrol banyak AP .

Secara teknis SD-WAN memiliki perbedaan yang sangat signifikan dibandingkan dengan tradisional WAN, ketika kamu menjalankan konsep tradisional WAN kamu perlu melakukan remote ke masing-masing perangkat WAN di cabang ketika melakukan instalasi, perubahan konfigurasi, upgrade dan lain sebagainya [3]. Sedangkan dengan menggunakan SD-WAN maka semuanya akan dilakukan dari single atau centralized dashboard dan amat sangat membantu bagi sebuah organisasi yang memiliki ratusan hingga ribuan outlet.

Lalu apa saja manfaat menggunakan SD-WAN ketimbang menggunakan Tradisional WAN[4]

1. Meningkatkan Performance

Salah satu manfaat menggunakan SD-WAN adalah meningkatnya performance link yang amat signifikan, hampir seluruh platform SD-WAN menyediakan fitur traffic engineering yang mampu melakukan hal ini contohnya seperti application pinning, application aware routing, dan lain sebagainya. Proses failover ketika salah satu link WAN mati juga amat cepat rata-rata 1-3 detik RTO lebih cepat daripada teknologi tradisional. [5]

2. Operasional Lebih Mudah dan Cepat

Centralized dashboard membantu tim operasional untuk melakukan konfigurasi dan monitoring yang lebih mudah dan dapat kamu bayangkan betapa terbantunya tim operasional yang menghandel banyak outlet atau cabang dengan metode ini, aktivitas perubahan konfigurasi, upgrade, dan monitoring semuanya dilakukan dari single dashboard saja. Selain itu hampir semua platform SD-WAN juga menyediakan teknologi zero-touch-provisioning yang memungkinkan kamu hanya membawa router saja ke cabang/outlet ketika proses instalasi awal dan konfigurasi akan otomatis terinstall di router tersebut, hal ini sangat membantu time-to-market apabila kamu diharuskan dengan cepat melakukan perubahan dan ekspansi bisnis.[6]

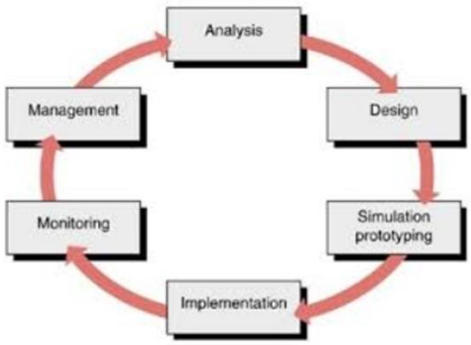
3. Lebih Menghemat Biaya Operasional

Salah satu manfaat SD-WAN adalah menekan biaya operasional, hampir sebagian besar use-case dan success story SD-WAN adalah beban operasional untuk membayar link ke provider yang sangat besar sebelum menggunakan SD-WAN, rata-rata mereka menggunakan 2 link private (MPLS/Metro-E) sebagai link kearah HO. Salah satu rahasia SD-WAN adalah teknik traffic engineering yang sangat mudah sehingga dapat meutilisasi link internet yang lebih murah sebagai link WAN dengan mudah dan aman. Hal ini berdampak besar tidak hanya terhadap biaya operasional melainkan juga performance link itu sendiri dimana biasanya link internet memiliki kapasistas yang lebih besar ketimbang private link (MPLS/Metro-E).[7]

Untuk penelitian kali ini, peneliti akan mengukur dan memberikan hasil menggunakan Cissco SD-WAN pada ruang lingkup Proof of Concept (PoC) yang akan dijadikan acuan dalam penerapan security antar cabang dengan menggunakan Cisco SD-WAN.

II. METODE PENELITIAN

Pengembangan Jaringan untuk implementasi dalam penelitian ini menggunakan metode Network Developmpment Life Cycle (NDLC) merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data.[8] Jika pengimplementasian teknologi jaringan dilaksanakan dengan efektif, maka akan memberikan sistem informasi yang akan memenuhi tujuan bisnis strategis, kemudian pendekatan top-down dapat diambil

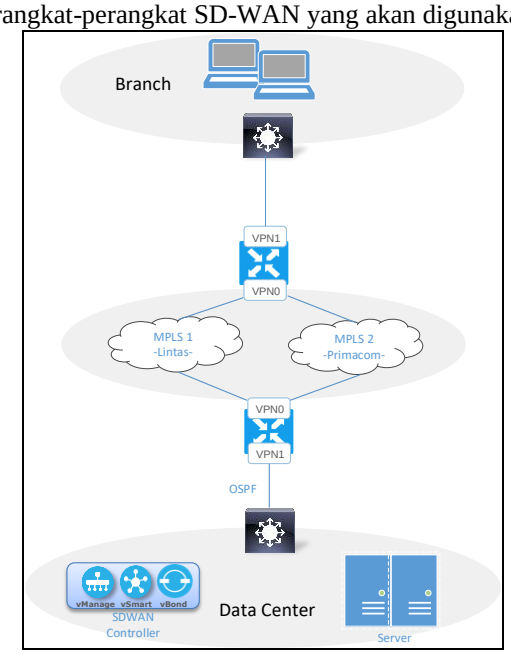


Gambar 1. Network Development Life Cycle (NDLC)

III. PROOF OF CONCEPT (POC)

Proof of Concept adalah pembuatan sebuah simulasi system atau topology dimana yang bertujuan untuk membuktikan kepada customer bahwa fitur fitur yang ditawarkan dapat sesuai dengan requirement (kebutuhan) dari customer sehingga dapat meyakinkan customer untuk dapat menggunakan teknologi dan jasa yang kami tawarkan

Secara Garis besar Perancangan Sistem ini digambarkan dengan menggunakan High Level Design Topology agar dapat memahami langkah-langkah dari sistem yang peneliti buat ini Dalam tahap perancangan perangkat keras ini, akan dilakukan perancangan fisik dari perangkat-perangkat SD-WAN yang akan digunakan dalam Proof of Concept ini.



Gambar 2. PoC Topology Scenario

PoC SD-WAN dilakukan dengan menempatkan 1 Unit SD-WAN Edge (ISR 4321) pada DC Bank XYZ di MT 1 dan 1 Unit SD-WAN Edge (VEDGE-100B) pada kantor cabang Citra. Controller SD-WAN menggunakan On-Prem device (1 buah server) dengan menginstall 3 komponen Controller (VSmart, VManage, & VBond) pada VMWare.

Terdapat 2 link yang menghubungkan Cabang Citra dengan Data Center/HO yaitu MPLS Lintasarta & Primacom. Tujuan pengetesan pada PoC kali ini bahwa kita ingin memisahkan traffic menuju Antivirus Server/WSUS & Pengetesan copy file dengan traffic Bank yang critical (Core Banking, dll). Dimana diharapkan traffic user menuju Antivirus Server/WSUS & Pengetesan copy file tidak mengganggu traffic critical lain nya.

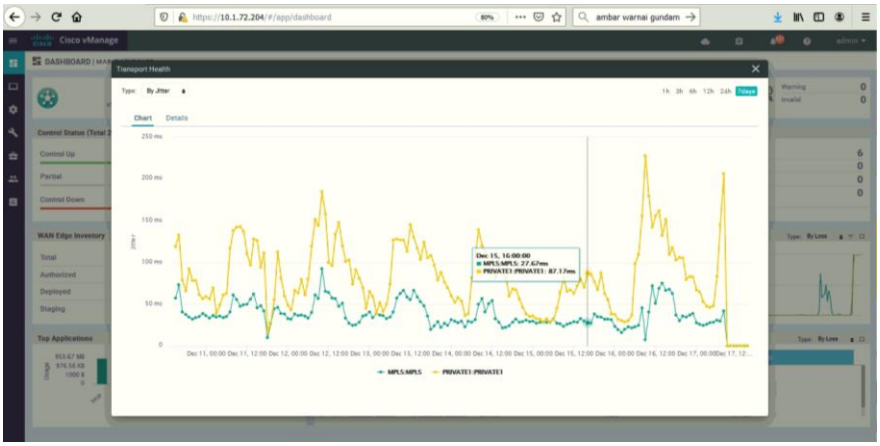
IV. HASIL PENELITIAN

Gambar 3. Dashboard Cisco SD-WAN

Terdapat 2 WAN Edge (DC & Cabang Citra)

1 VSmart, 1 VBond, & 1 VManage

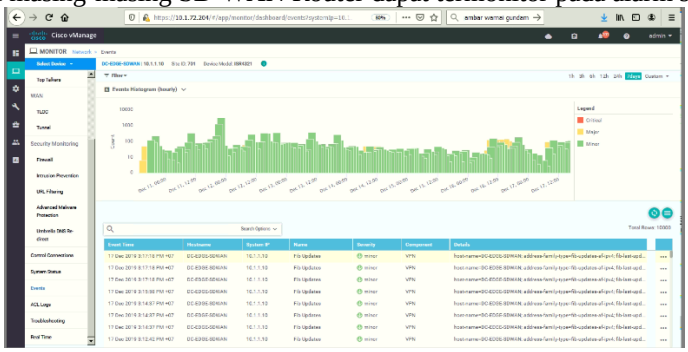
Transport Health
Terdapat 2 tunnel ipsec active antar 2 site (DC – Cabang Citra). 2 Tunnel tersebut masing-masing menggunakan link MPLS dari Primacom & Lintasarta.
Pembagian Link dibedakan menjadi 2 : Color MPLS = Link Lintasarta Color Private1 = Link Primacom



Gambar 4. Tunnel Health

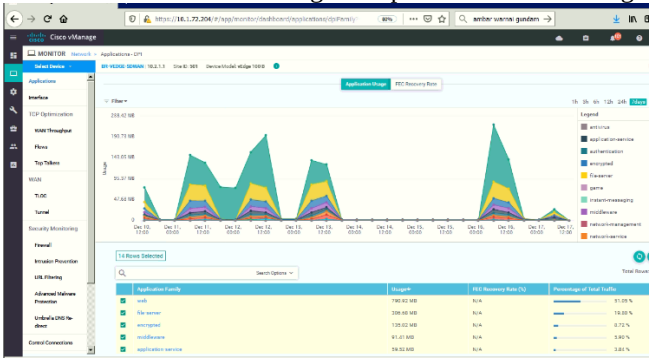
Penjelasan Dari grafik transport health yang di tampilkan pada SD-WAN, diketahui kualitas link Lintasarta lebih bagus di banding primacom. Link Lintasarta memiliki rata-rata latency 20-30 m/s sedangkan Link Primacom 600-800 m/s. Link Lintasarta lebih sering mengalami RTO/Putus, dibanding Link Primacom.

Alarm
Setiap alert yang berasal dari masing-masing SD-WAN Router dapat termonitor pada alarm system SD-WAN.



Gambar 5. Alarm Dashboard SD-WAN

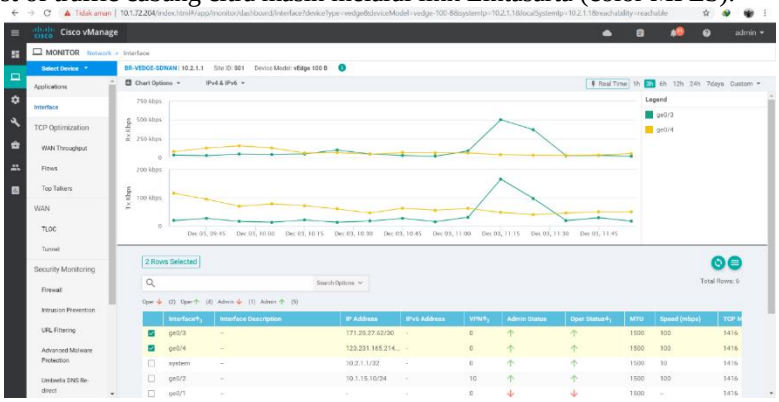
Specific Monitor – Branch Site
Application Traffic
Berikut adalah capture application traffic dari DC ke Cabang Citra pada 7 hari monitoring.



Gambar 6. SD-WAN Traffic Monitoring

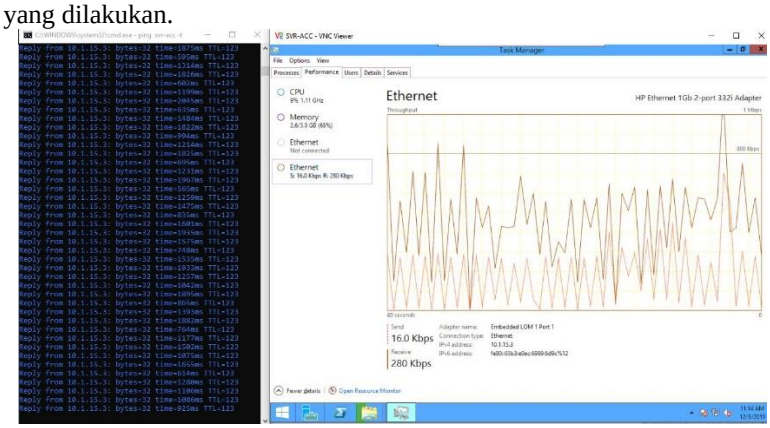
Interface Traffic

Pada saat PoC dilakukan pengetesan copy file dari DC ke Cabang Citra yang diarahkan melalui link Primacom (Color Private1), sementara most of traffic cabang citra masih melalui link Lintasarta (color MPLS).



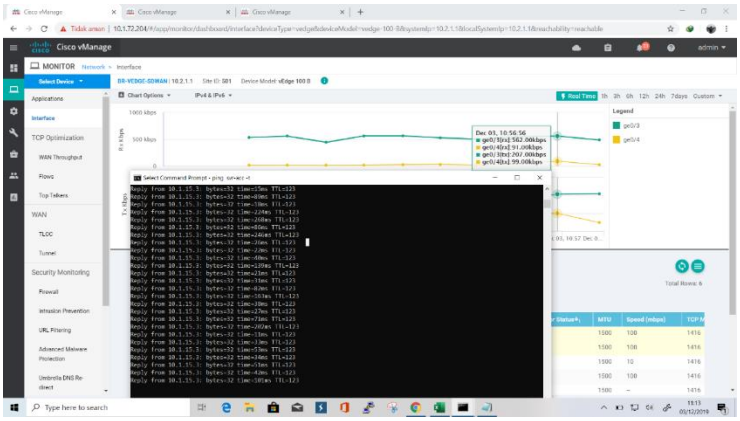
Gambar 7. SD-WAN Interface Traffic

Berikut proses copy file yang dilakukan.



Gambar 8. Proses Testing Copy File

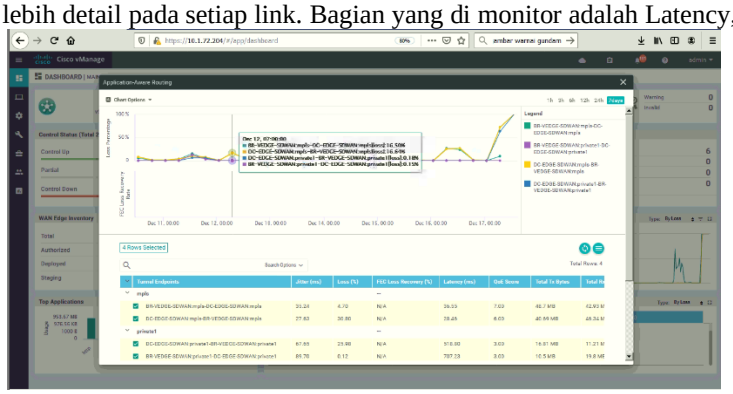
Pada saat proses copy file terdeteksi traffic interface Primacom (Color Private1) tinggi/naik. Hal ini membuktikan bahwa policy SD-WAN berjalan sesuai.



Gambar 9. Bukti saat Copy File di SD-WAN Dashboard

Tunnel Health

Pada bagian Tunnel Health pada dasarnya hampir sama dengan Transport Health sebelumnya. Bedanya pada bagian ini kita dapat melihat kualitas link lebih detail pada setiap link. Bagian yang di monitor adalah Latency, Loss & Jitter.

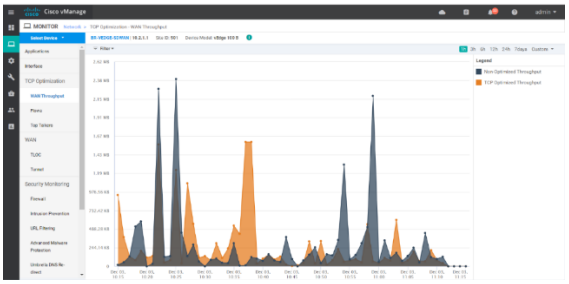


Gambar 10. Tunnel Health

TCP Optimization

Pada VEDGE 100B Cabang Citra kita telah aktifkan pula fitur WAN Opti agar dapat mengoptimalkan serta mengefisienkan transmisi packet data.

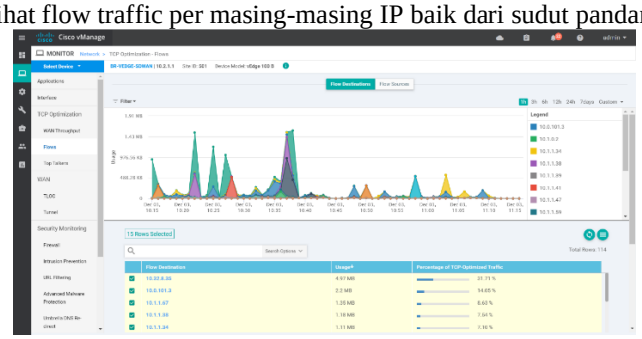
WAN Throughput



Gambar 11. WAN Throughput

Flow (Destination)

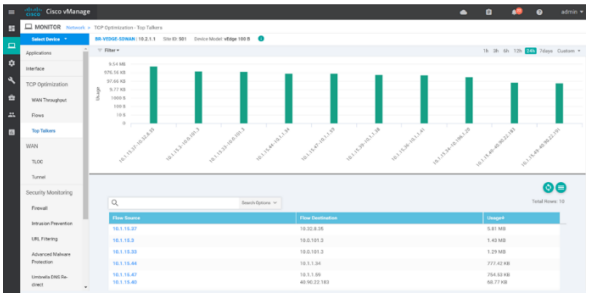
Pada bagian ini kita dapat melihat flow traffic per masing-masing IP baik dari sudut pandang source maupun destination.



Gambar 12. Flow and Destination Graphic

Top Talker

Pada bagian ini kita dapat memonitor top traffic yang melewati tunnel SD-WAN kita.



Gambar 13. Top Traffic SD-WAN

V. KESIMPULAN DAN SARAN

Kesimpulan yang bisa kami dapatkan adalah sebagai berikut :

Cisco SD-WAN menawarkan solusi keamanan lokal dan cloud terintegrasi yang mencakup empat kategori keamanan: segmentasi jaringan, firewall perusahaan, gateway web aman, dan keamanan lapisan DNS. Setiap kategori keamanan itu sendiri mencakup kombinasi fitur keamanan yang berbeda. Enkripsi IPsec: Fabrik WAN yang mendasari untuk mengamankan akses WAN lokal dan akses internet langsung. Kontrol aplikasi: Praktik keamanan bawaan dalam setiap bagian tumpukan keamanan, yang mampu mengontrol 1400 aplikasi menggunakan firewall perusahaan di lokasi. Dekripsi SSL / TLS: Fitur keamanan dengan skala tidak terbatas untuk keamanan cloud atau keamanan di lokasi dengan sumber daya yang memadai. Keamanan DNS Layer .
Dari beberapa Fitur Keamanan tersebut, tentunya Cisco SD-WAN memiliki manfaat keamanan untuk Meningkatkan Keamanan Informasi / Data di Bank XYZ yakni diantaranya adalah untuk Perlindungan konstan terhadap semua ancaman internal dan eksternal dari cabang ke IaaS, Pengalaman pengguna yang ditingkatkan melalui internet langsung yang aman dan akses cloud, Visibilitas dan kontrol terpusat untuk semua lalu lintas internal, masuk dan keluar serta Mengurangi biaya dan kompleksitas menggunakan satu produk untuk jaringan, keamanan, dan cloud.

Serta Saran yang dapat Penulis berikan terkait dengan hal ini yakni Untuk pengembangan ke depannya mungkin bisa diujikan Bersama integrasi dengan Firewall on premise, Lalu bisa dikembangkan juga dengan teknologi SD-X lainnya seperti SDA (Software Defined Access) untuk area LAN dan juga SDN (Software Defined Network) untuk area Data Center Networkingnya dan Bisa dikembangkan dari sisi Business Analysis Cost yang membandingkan biaya dengan menggunakan SD-WAN ataupun tidak dengan menggunakan SD-WAN

REFERENSI

[1] M. Wood, “How to make SD-WAN secure,” *Netw. Secur.*, vol. 2017, no. 1, pp. 12–14, Jan. 2017, doi: 10.1016/S1353-4858(17)30006-5.

[2] P. Göransson, C. Black, and T. Culver, “SDN Futures,” *Softw. Defin. Networks*, pp. 353–374, Jan. 2017, doi: 10.1016/B978-0-12-804555-8.00015-6.

[3] N. Miloslavskaya, “Network Protection Tools for Network Security Intelligence Centers,” *Procedia Comput. Sci.*, vol. 190, pp. 597–603, Jan. 2021, doi: 10.1016/J.PROCS.2021.06.070.

[4] M. S. Tok and M. Demirci, “Security analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard,” *Comput. Secur.*, vol. 109, p. 102394, Oct. 2021, doi: 10.1016/J.COSE.2021.102394.

[5] J. Zhao, Z. Hu, B. Xiong, L. Yang, and K. Li, “Modeling and optimization of packet forwarding performance in software-defined WAN,” *Futur. Gener. Comput. Syst.*, vol. 106, pp. 412–425, May 2020, doi: 10.1016/J.FUTURE.2019.12.010.

[6] R. Joffe, “Network security in the new world of work,” *Netw. Secur.*, vol. 2021, no. 9, pp. 7–9, Sep. 2021, doi: 10.1016/S1353-4858(21)00102-1.

[7] S. Pamplin, “SD-WAN revolutionises IoT and edge security,” *Netw. Secur.*, vol. 2021, no. 8, pp. 14–15, Aug. 2021, doi: 10.1016/S1353-4858(21)00090-8.

[8] M. Sollars, “Love and marriage: why security and SD-WAN need to go together,” *Netw. Secur.*, vol. 2018, no. 10, pp. 10–12, Oct. 2018, doi: 10.1016/S1353-4858(18)30100-4.