ZONAsi Jurnal Sistem Informasi
ZONAsi VOL. 7 NO. 2 Mei 2025
Page: 611 - 623
ISSN: 2656-7407 (Online)
2656-7393 (Print)

ANALISIS PENERAPAN SISTEM KEAMANAN *SOFTWARE DEFINED WIDE AREA NETWORKING* (SD-WAN) PADA KANTOR DIREKTORAT JENDERAL PAJAK

Hasan Ramdani[1], Thomas Budiman[2], Anton Zulkarnain Sianipar [3], Ito Riris[4], Rumadi Hartawan[5], Ifan Junaedi[6]
[123]Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Jayakarta, Indonesia
Jl. Salemba I No. 8-10, Jakarta Pusat, (021) 3906060
[1]22577003@stmik.jayakarta.ac.id, [2]thomas @stmik.jayakarta.ac.id, [3]antonz@stmik.jayakarta.ac.id
[4]itoriris@stmik.jayakarta.ac.id, [5]rumadi_hartawan@stmik.jayakarta.ac.id, [6]ifanjuanedi8@gmail.com

Abstrak

Pada artikel jurnal ini membahas tentang analisis penerapan sistem keamanan Software-Defined Wide Area Networking yang ada di Kantor Pusat Direktorat Jenderal Pajak. Saat ini, Direktorat Jenderal Pajak (DJP) masih mengandalkan jaringan tradisional untuk menghubungkan Data Center dan Disaster Recovery Center ke kantor-kantor vertikalnya. Namun, dengan pertumbuhan aktivitas dan volume data yang terus meningkat, jaringan tradisional menghadapi tantangan dari sisi manajemen, efisiensi, dan terutama keamanan. Teknologi Software-Defined Wide Area Network hadir sebagai solusi inovatif untuk mengatasi berbagai kelemahan yang ada pada WAN tradisional. SD-WAN mampu menyederhanakan manajemen jaringan dengan memisahkan perangkat keras dari kontrolnya, serta menyediakan koneksi yang lebih fleksibel, aman, dan mudah dikelola. SD-WAN tidak hanya mengoptimalkan kinerja jaringan, tetapi juga memberikan kemudahan dan kecepatan tanpa harus melibatkan tenaga IT di lokasi

Kata kunci: *Jaringan Komputer, SD-WAN, VPN, Internet, WAN*

Abstract

Abstract prepared well, allowing the reader to identify the basic content of a document quickly This research discusses the analysis of the implementation of the Software-Defined Wide Area Networking security system at the Headquarters of the Directorate General of Taxes. Currently, the Direktorat Jenderal Pajak (DJP) still relies on the traditional network to connect the Data Center and Disaster Recovery Center to its vertical offices. However, with the growth of activity and the ever-increasing volume of data, traditional networks face challenges in terms of management, efficiency, and especially security. SD-WAN (Software-Defined Wide Area Network) technology is present as an innovative solution to overcome various weaknesses that exist in traditional WAN. SD-WAN simplifies network management by separating hardware from its control, as well as providing more flexible, secure, and manageable connections. SD-WAN not only optimizes network performance, but also provides convenience and speed without having to involve IT personnel on site.

Keywords: *Computer Network, SD-WAN, VPN, Internet, WAN*

1. PENDAHULUAN

Seiring dengan perkembangan teknologi dan kebutuhan yang semakin kompleks, jaringan komunikasi pada sebuah organisasi menjadi hal yang sangat krusial. Saat ini, Direktorat Jenderal Pajak (DJP) masih mengandalkan jaringan tradisional untuk menghubungkan *Data Center* dan *Disaster Recovery Center* ke kantor-kantor vertikalnya. Namun, dengan pertumbuhan aktivitas dan volume data yang terus meningkat, jaringan tradisional menghadapi tantangan dari sisi manajemen, efisiensi, dan terutama keamanan.

Teknologi SD-WAN (*Software-Defined Wide Area Network*) hadir sebagai solusi inovatif untuk mengatasi berbagai kelemahan yang ada pada WAN tradisional. SD-WAN mampu menyederhanakan manajemen jaringan dengan memisahkan perangkat keras dari kontrolnya, serta menyediakan koneksi yang lebih fleksibel, aman, dan mudah dikelola. SD-WAN tidak hanya mengoptimalkan kinerja

jaringan, tetapi juga memberikan kemampuan enkripsi end-to-end, segmentasi jaringan, serta *deployment* yang lebih mudah dan cepat tanpa harus melibatkan tenaga IT di lokasi.

Dengan meningkatnya ancaman keamanan siber, aspek keamanan menjadi salah satu fokus utama dalam pengadopsian SD-WAN. Teknologi ini menawarkan berbagai fitur keamanan canggih seperti *enkripsi, firewall*, dan segmentasi jaringan yang memastikan data sensitif terlindungi dengan baik.

Pada penelitian sebelumnya yang dilakukan oleh [1] mengenai Peningkatan Keamanan dan Efisiensi Branch Office Dengan Software-Defined WAN (SD-WAN), dalam jurnal ini fokus pada keamanan di kantor cabang oleh karena itu saya mengembangkan dari sisi keamanan Kantor Pusat agar pengaturan pada sistem keamanan lebih terpustt dan terkontrol satu titik di kantor pusat tanpa tim IT terjun langsung ke site untuk visit ke kantor cabang.

Dalam hal ini penulis melakukan identifikasi masalah yang ada di Kantor Direktorat Jenderal Pajak antara lain keterbatasan keamanan pada jaringan WAN tradisional di DJP memerlukan *software* untuk mengamankan jaringan tersebut, tingkat keamanan jaringan di kantor vertikal DJP saat ini belum optimal dan proses manajemen dan pemeliharaan jaringan yang rumit dan lambat dapat menurunkan kinerja operasional.

Penelitian ini bertujuan untuk mencapai hal-hal sebagai berikut menyusun kebutuhan sistem keamanan *software defined wide area networking* di DJP, kemudahan dalam memantau dan mengatur semua perangkat dan koneksi di unit vertikal, kemudahan dalam kegiatan management perangkat jaringan WAN di unit vertikal. Manfaat yang dapat diperoleh dari penelitian ini antara lain memperluas wawasan dan ilmu pengetahuan bagi penulis tentang penggunaan SD-WAN khususnya di pengelolaan jaringan layanan intranet dan internet, memberikan gambaran atas solusi SD-WAN yang dapat membantu proses operasional tata kelola jaringan layanan jaringan komunikasi data intranet maupun internet di Kantor Direktorat Jenderal Pajak Kementerian Keuangan Republik Indonesia dan menyajikan informasi mengenai tentang pentingnya memiliki teknologi SD-WAN.

Adapun landasan teori yang mendukung dalam penulisan ini antara lain sebagai berikut:

a) Menurut Wicaksono (2016) LAN adalah singkatan dari local Area Network suatu jaringan komputer yang masi berada di gedung atau ruangan. Dalam membuat jaringan LAN, minimal kita harus menyediakan dua buah komputer yang masing-masing memiliki kartu jaringan atau LAN Card.[2]
b) Menurut Ahmaddul Hadi (2016) router adalah sebuah perangkat jaringan yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. [3]
c) Menurut Bitar (2021), system adalah sekumpulan objek, unsur – unsur atau bagian – bagian yang mempunyai arti berbeda – beda yang saling berhubungan, saling bekerjasama serta saling mempengaruhi satu sama lain dan memiliki keterkaitan pada sebuah rencana yang sama dalam mencapai suatu tujuan tertentu pada lingkungan yang kompleks. [4].
d) DoS adalah metode serangan di mana penyerang mengirimkan permintaan secara berulang guna memberatkan beban server hingga menyebabkannya rusak bahkan tidak berfungsi. Selanjutnya, penyerang dapat leluasa mengakses hingga merusak data dalam jaringan tersebut [5].
e) Terdapat 2 jenis IP address yaitu IPv4 dan IPv6. [6]
f) Menurut Bullock (2009), *data center* sebenarnya adalah server atau ruang komputer tempat berkumpulnya beberapa server perusahaan. Data center ini yang paling banyak digunakan lembaga atau perusahaan yang bertujuan untuk peningkatan layanan dan daya saing dengan lembaga atau perusahaan lain dalam melayani stakeholdersnya. Ujungnya adalah peningkatan efektivitas pada proses bisnis masing- masing lembaga atau perusahaan tersebut. [7]
g) *Disaster Recovery Center (DRC)* adalah kemampuan sebuah infrastruktur untuk melakukan kembali operasi secepatnya pada saat terjadi gangguan yang signifikan seperti bencana besar yang tidak dapat diduga sebelumnya. Fungsi dari adanya DRC adalah untuk meminimalkan kerugian finansial dan non-finansial dalam menghadapi kekacauan bisnis atau bencana alam yang meliputi fisik dan informasi berupa data penting perusahaan, serta meningkatkan rasa aman di antara personel, supplier, investor, dan customer [8]
h) Unified Threat Management (UTM) adalah suatu sistem aplikasi yang mengintegrasikan berbagai fitur keamanan menjadi suatu platform hardware tunggal. UTM mampu mendeteksi dan mengurangi ancaman atau gangguan yang mempengaruhi performansi jaringan serta dapat mengatur alokasi trafik berdasarkan aplikasi, protokol atau interface pada jaringan. Kelebihan

menggunakan UTM dibandingkan dengan menggunakan perangkat secara terpisah yang merupakan bagian dari UTM seperti Intrusion Detection System (IDS), Firewall, Antivirus dan Proxy Server secara bersamaan ialah dari segi cost dan manajemennya yang dimana lebih efisien dan memiliki kompleksitas yang rendah dalam konfigurasinya.[9]

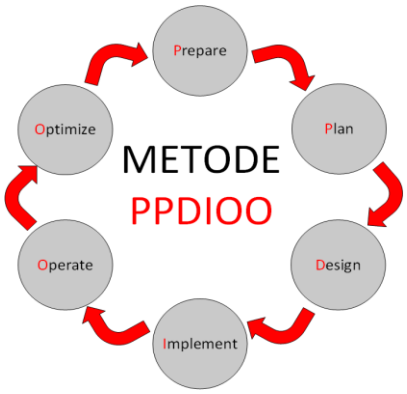
i) Dengan menggunakan IPSec, data yang dikirim melalui jaringan dapat diamankan dari ancaman yang mungkin terjadi di atas layer network. [10]
j) Berikut merupakan beberapa jenis topologi logis yang umum digunakan hingga saat ini. [11] yaitu topologi jaringang bus, topologi jaringan ring dan topologi jaringan mesh.
k) Pada perangkat jaringan merujuk pada semua komputer, perangkat tambahan, kartu antarmuka, dan periferal yang saling terhubung dalam suatu jaringan komputer untuk memungkinkan transfer data (Madcoms, 2010)
l) Sedangkan DoS adalah metode serangan di mana penyerang mengirimkan permintaan secara berulang guna memberatkan beban server hingga menyebabkannya rusak bahkan tidak berfungsi. Selanjutnya, penyerang dapat leluasa mengakses hingga merusak data dalam jaringan tersebut [5].
m) Dengan adanya protokol-protokol tersebut di setiap lapisan, model OSI memungkinkan komunikasi yang terstandarisasi dan efisien dalam jaringan komputer. Setiap lapisan memiliki peran khusus dalam memproses data dan menyediakan layanan yang dibutuhkan oleh aplikasi dan pengguna [12].
n) Menurut Prof. Dr. Ir. Hapzi Ali, MM (2016) software adalah perangkat lunak komputer seperti, operating sistem (Windows, Linux), program aplikasi perbankan dan program aplikasi lainnya dan menurut Purnama et al. (2021) Software berfungsi sebagai sistem operasi atau sistem pendukung yang berfungsi untuk mengatur atau mengontrol dan Software ini juga berfungsi sebagai penerjemah dari setiap instruksi - instruksi ke dalam bahasa mesin sehingga dapat di terima oleh Hardware. [13]
o) Ada dua jenis bandwidth diantaranya bandwidth analog dan digital. Biasanya, lebih dikenal dengan istilah bandwidth digital. Sementara itu, penyedia layanan internet seperti Internet Service Provider (ISP) sering menggunakan istilah *bandwidth* analog untuk menggambarkan kecepatan koneksi internet yang mereka tawarkan [14].

2. METODE PENELITIAN

Metodologi penelitian merupakan cara atau proses yang digunakan oleh seorang peneliti untuk mendapatkan data atau informasi yang diperlukan dalam penelitian. Penelitian yaitu suatu penyelidikan yang dilakukan secara sistematis untuk meningkatkan pengetahuan tentang suatu topik. Dengan melibatkan upaya yang terorganisasi dan terstruktur untuk menyelidiki masalah tertentu yang memerlukan jawaban. Motivasi dasar untuk melakukan penelitian yaitu keinginan untuk memperoleh dan mengembangkan pengetahuan, yang merupakan kebutuhan umum bagi manusia [15]sehingga menjadi perancangan untuk melakukan implementasi SD-WAN

2.1. Metode PPDIOO

Penulis menggunakan metode PPDIOO (*Prepare*, *Plan*, *Design*, *Implement*, *Operate*, *Optimize*) dalam penelitian ini. Metode ini dikenalkan oleh perusahaan berasal Negara Amerika yang tepatnya berada di San Francisco California [16]. Metode ini memiliki 6 tahapan, yaitu:



***Gambar 1** Metode PPDIOO*

1. *Prepare*

Pada tahap ini melakukan penetapan kebutuhan yang akan mendukung dalam penelitian penulis seperti alat dan bahan penelitian.

2. *Plan*

Pada tahap ini melakukan identifikasi bagaimana rencana dalam melakukan penelitian, seperti pengumpulan data hingga mendapatkan kesimpulan dan saran.

3. *Design*

Pada tahap ini, penulis melakukan desain jaringan atau biasa disebut dengan topologi jaringan pada implementasi SD-WAN.

4. *Implement*

Pada tahap ini, peralatan yang sudah disiapkan sebelumnya untuk dilakukan konfigurasi layanan jaringan menggunakan teknologi SD-WAN.

5. *Operate*

Setelah konfigurasi SD-WAN selesai dan berhasil *running*, pada tahap ini dilakukan pengujian untuk mengetahui sistem keamanan pada perangkat SD-WAN berjalan aktif.

6. *Optimize*

Lalu pada tahap terakhir, setelah mendapatkan hasil pengujian analisa keamanan akan didapatkan kesimpulan dan saran untuk memperbaiki kendala yang didapatkan.

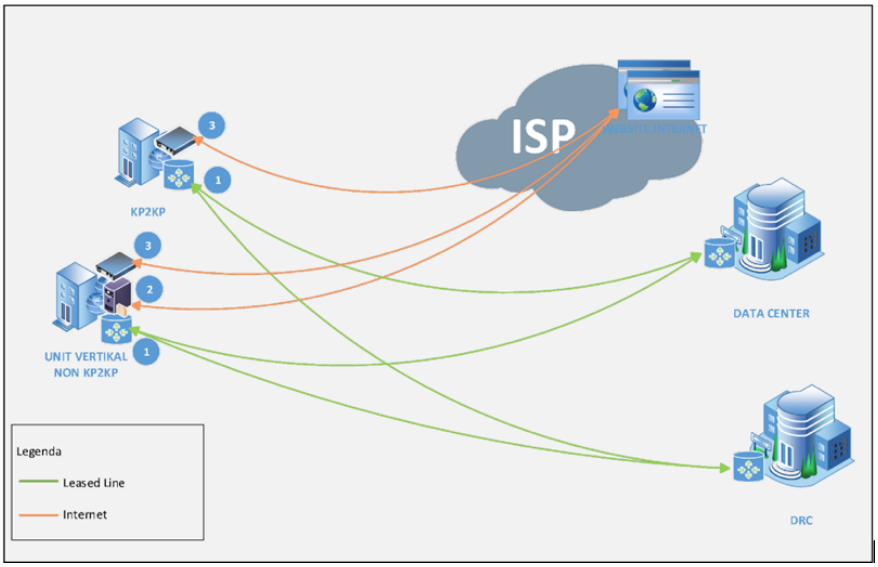
2.2. Metode Analisis

Pendekatan analisis *SWOT* (*Strengths, Weaknesses, Opportunities, Threats*) digunakan untuk menganalisis permasalahan dan kelemahan sistem dalam implementasi SD-WAN di Kantor Pusat DJP RI. Metode SWOT merupakan sebuah alat untuk mengidentifikasi berbagai faktor secara sistematis, yang selanjutnya digunakan untuk merumuskan strategi perusahaan. Logika yang mendasari analisis ini bertujuan untuk memaksimalkan potensi kekuatan dan peluang, sambil mengurangi dampak dari kelemahan dan ancaman yang ada. Secara singkat, analisis SWOT diterapkan dengan cara mengidentifikasi dan memilah faktor-faktor yang mempengaruhi keempat aspek tersebut untuk meningkatkan efektivitas implementasi SD-WAN di Kantor Pusat DJP RI.

3. Hasil dan Pembahasan

3.1 Hasil

Dari hasil yang didapatkan, terkait usulan implementasi jaringan SD-WAN yang efektif dan efisien. Analisis Desain Topologi yang Sedang Berjalan.



***Gambar 2** Desain Topologi yang sedang berjalan*

Pada Gambar diatas menunjukkan topologi jaringan WAN unit kerja vertikal. Pada unit kerja vertikal DJP terdapat beberapa perangkat dan fungsi sebagai berikut:

1. Router, perangkat router digunakan sebagai *gateway user* menuju DC DJP dan DRC Kemenkeu untuk melakukan akses aplikasi-aplikasis di intranet. Perangkat ini terkoneksi dengan jaringan leased line dari provider/penyedia jaringan intranet.
2. UTM, perangkat UTM digunakan sebagai *gateway user* menuju jaringan internet untuk melakukan akses aplikasi-aplikasi yang ada di internet. Perangkat ini terkoneksi dengan jaringan internet dedicated dari provider/penyedia jaringan internet. Perangkat UTM bekerja dengan cara menjadi sebuah proxy server yang akan meneruskan akses user menuju internet.
3. Modem Internet Broadband, perangkat ini ada di beberapa unit kerja yang melakukan sewa internet broadband secara mandiri. Perangkat ini tidak terhubung dengan LAN unit kerja, sehingga hanya digunakan untuk keperluan perangkat komputer yang tidak terkoneksi dengan LAN.

Seluruh unit vertikal dan unit pelaksana teknis Ditjen Pajak (DJP) diberikan koneksi leased line untuk mengakses aplikasi internal DJP dan koneksi internet untuk mengakses website-website di jaringan internet. Selain untuk mengakses website internet, user juga dapat menggunakan koneksi internet untuk mengakses aplikasi internal menggunakan SSL VPN. Pada topologi tersebut, terdapat beberapa kelemahan yang menjadi kendala bagi user di unit kerja, pengelola jaringan dan pengelola keamanan di Direktorat TIK antara lain:

1. Koneksi leased line dan internet di unit kerja memiliki fungsi yang berbeda. Koneksi leased line digunakan untuk akses aplikasi internal baik di DC DJP maupun DRC Kemenkeu. Koneksi leased line diatur menggunakan perangkat router yang menjadi gateway unit kerja untuk menuju WAN intranet. Sedangkan koneksi internet diatur menggunakan sebuah perangkat UTM yang berfungsi sebagai proxy server dan alat pengamanan (security) untuk akses ke jaringan internet. Kedua koneksi ini berkerja masing-masing dan tidak menjadi backup yang secara otomatis bekerja ketika salah satu koneksi mengalami gangguan. Ketika koneksi leased line pada suatu unit kerja mengalami gangguan, user harus melakukan tindakan untuk menggunakan SSL VPN melalui koneksi internet untuk tetap dapat mengakses aplikasi internal.
2. Pada topologi jaringan existing tidak memungkinkan untuk dilakukan pengaturan *Quality of Service* (QoS). Hal ini dikarenakan pada koneksi leased line tanpa suatu "overlay" mengakibatkan bentrok parameter QoS dengan yang ditetapkan oleh penyedia (provider) jaringan leased line.
3. Kegiatan operasional seperti pemantauan dan pengaturan akses intranet dan internet tidak dapat dilakukan pada satu alat manajemen yang terintegrasi. Perangkat router dan UTM yang ada pada unit kerja bekerja dengan fungsi yang berbeda dan diatur menggunakan perangkat manajemen yang berbeda pula. Kegiatan provisioning perangkat baik diawal implementasi maupun pada saat penggantian perangkat rusak, diperlukan campur tangan admin untuk melakukan konfigurasi perangkat terlebih dahulu sebelum dapat dipasang di unit kerja untuk dapat beroperasi. Hal ini akan menambahkan durasi (waktu) dan membutuhkan SDM dengan pengetahuan yang cukup untuk mengerjakannya.
4. Secara *logic*, koneksi unit kerja memiliki dua pintu keluar (gateway) yaitu router sebagai gateway menuju intranet dan UTM sebagai gateway menuju internet. Akses dari user menuju intranet dan menuju internet melewati dua perangkat yang berbeda. Apabila terdapat gangguan pada satu koneksi, user akan langsung merasakan dampak gangguan ini. Hal ini dikarenakan aliran data dari user menuju intranet dan internet tidak dapat diatur untuk secara otomatis berpindah antar dua koneksi tersebut.

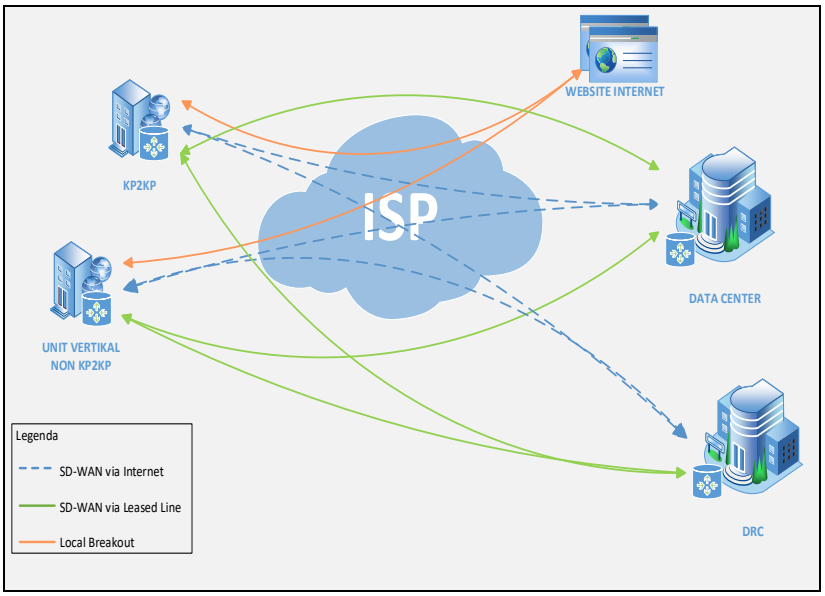
Berdasarkan analisis kondisi jaringan pada unit kantor vertikal saat ini, dibutuhkan penerapan teknologi SD-WAN untuk meningkatkan kinerja jaringan WAN yang dapat dimanfaatkan oleh user. Penerapan

teknologi SD-WAN ini dapat dilakukan dengan berpedoman pada kriteria-kriteria pada tabel dibawah ini.

Tabel 1 *Spesifikasi Kebutuhan Sistem Keamanan*

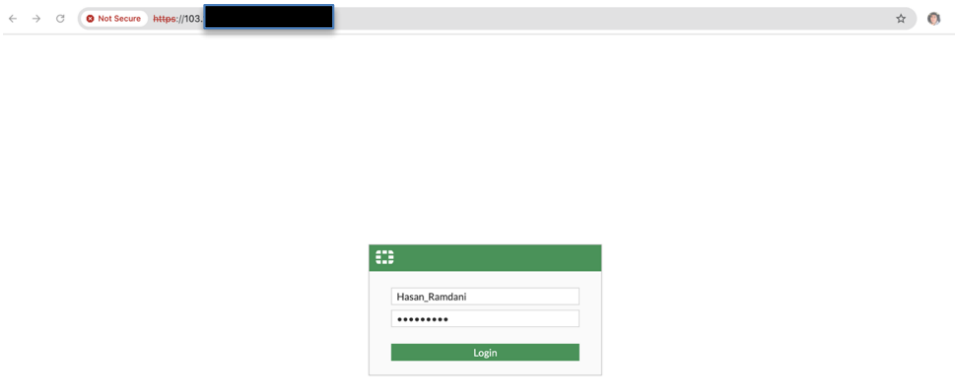
No.	Kriteria	Spesifikasi yang dibutuhkan
1	*Edge Connectivity Abstraction*	Dapat melakukan *Fail-Over* antara beberapa koneksi WAN dengan konfigurasi *active - active* dengan mendeteksi trafik berdasarkan Bandwidth dan Session;
		Dapat diimplementasikan menggunakan koneksi leased line, internet dedicated dan internet broadband serta variasi dari ketiganya;
		Dapat berfungsi sebagai gateway koneksi menuju jaringan internet;
2	WAN *Virtualization*	Dapat membuat koneksi *tunnel* yang dienkripsi dari unit kerja menuju DC DJP dan DRC Kemenkeu dan dari unit kerja menuju unit kerja yang lainnya;
3	*Policy-Driven, Centralized Management*	Memiliki sebuah manajemen terpusat (*centralize management*) untuk semua perangkat SD-WAN di unit kerja, dengan kemampuan minimal sebagai berikut:
		Memiliki *User Interface* berbasis *Graphical User Interface* (GUI);
		1. Dapat memonitor status perangkat dan koneksi pada semua unit kerja;
		2. Dapat melakukan *provisioning* secara *remote* (jarak jauh) dengan konsep *zero touch provisioning* (ZTP) atau *low touch;*
		3. Dapat melakukan perubahan konfigurasi perangkat SD-WAN pada semua unit kerja secara terpusat;
4	*Elastic Traffic Management*	Dapat melakukan *Application based QoS, security policy enforcement, application forwarding* dan WAN *path selection;*

Rancangan topologi untuk penerapan teknologi SD-WAN pada unit vertikal DJP dapat dilihat pada gambar dibawah ini.



***Gambar 3** Desain Topologi SD-WAN*

Fitur keamanan pada SD-WAN ini dapat kita buka melalui website dengan cara ketik https://103.[redacted] alamat website ini hanya dikhususkan untuk *view* demi keamanan yang ada di Kantor Pusat DJP dengan tampilan sebagai berikut:



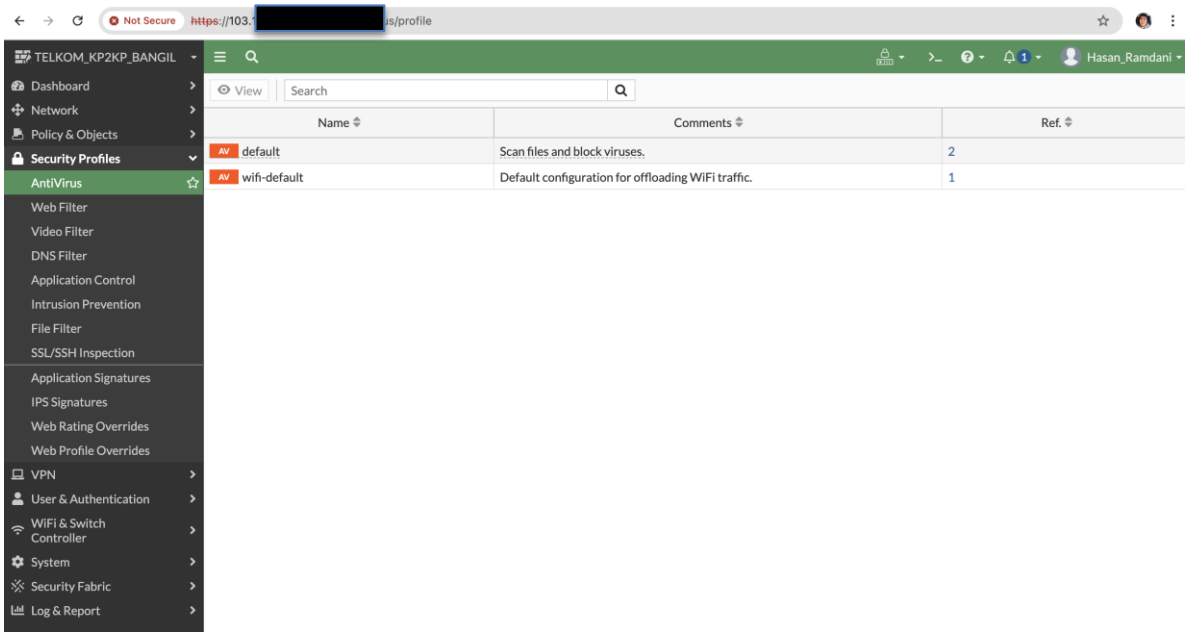
***Gambar 4** Dashboard Fortiget SD-WAN*

Pada gambar diatas merupakan tampilan awal dari *dashboard Fortigate* SD-WAN dimana kita memasukan data berupa *user name* dan *password* sebagai berikut:

User name : Hasan_Ramdani

Password : [redacted]

Untuk *setting* fitur keamanan KP2KP Bangil yang merupakan salah satu kantor vertikal yang ada di Kantor Pusat Direktorat Jenderal Pajak dapat kita lihat pada halaman sebagai berikut:

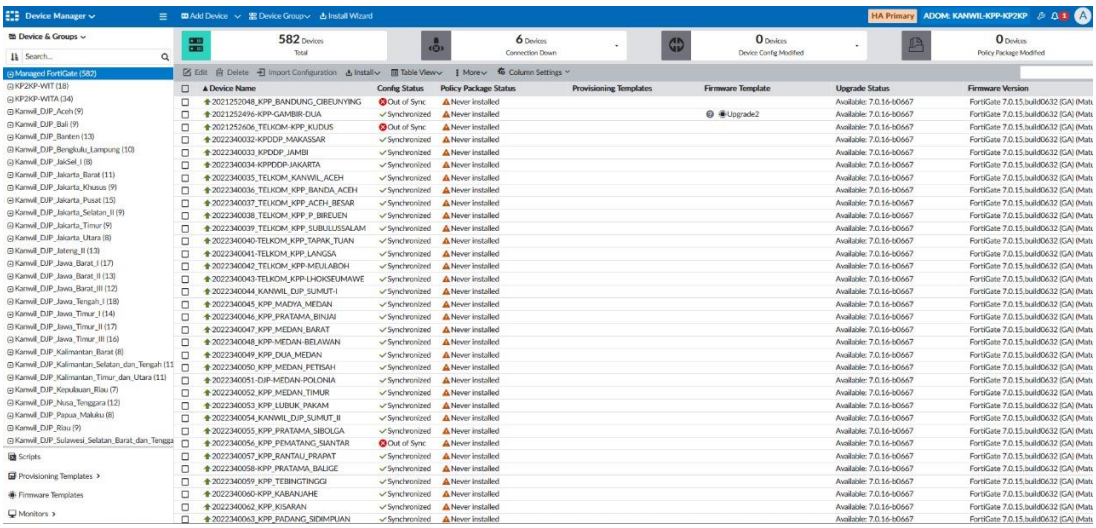


***Gambar 5** Dashboard Security Profiles*

Pada gambar diatas sistem keamanan dapat terlihat pada menu *security profiles* sebagai berikut :

1. *AntiVirus*
2. *Web Filter*
3. *Video Filter*
4. *DNS Filter*
5. *Application Control*
6. *Intrusion Prevention*
7. *File Filter*
8. *SSL/SSH Inspection*

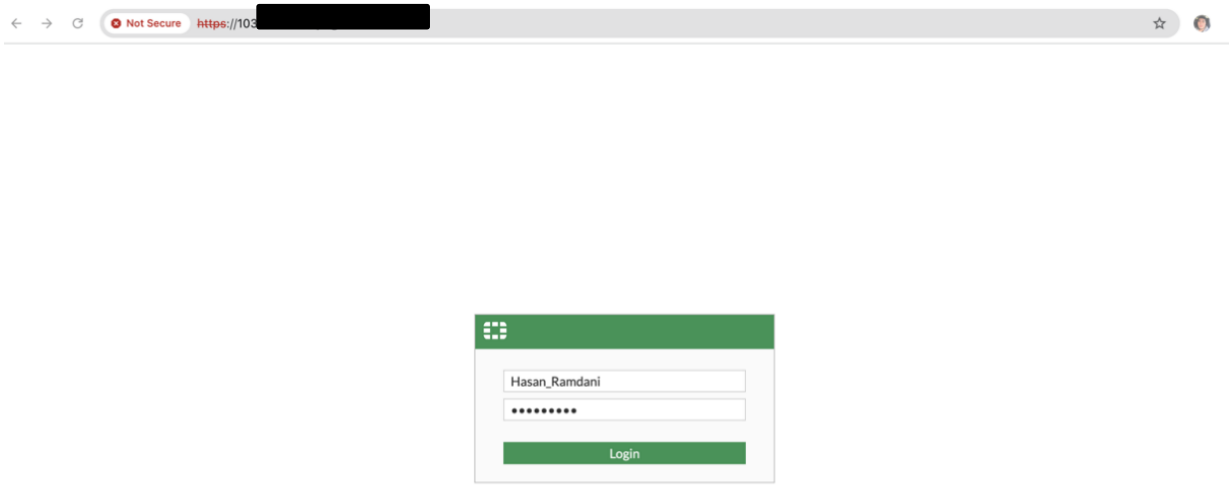
Dengan adanya fitur ini sistem keamanan di Kantor Direktorat Jenderal Pajak lebih optimal baik dari ancaman siber yang ada pada saat ini dimana data dari Wajib Pajak merupakan aset yang sangat besar terhadap target pencapaian pendapatan negara dalam sektor perpajakan yang berada di Indonesia.
Untuk mengontrol kantor vertikal di Kantor Direktorat Jenderal Pajak yang memiliki lebih dari 500 kantor vertikal yang harus diamankan dari segi keamanannya oleh sebab itu kehandalan dari software sistem keamanan SD-WAN yang ada pada *forti manager* menyediakan fitur yang lengkap yang dapat di monitor oleh kantor pusat sebagai berikut:



***Gambar 6** Dashboard Forti Manager*

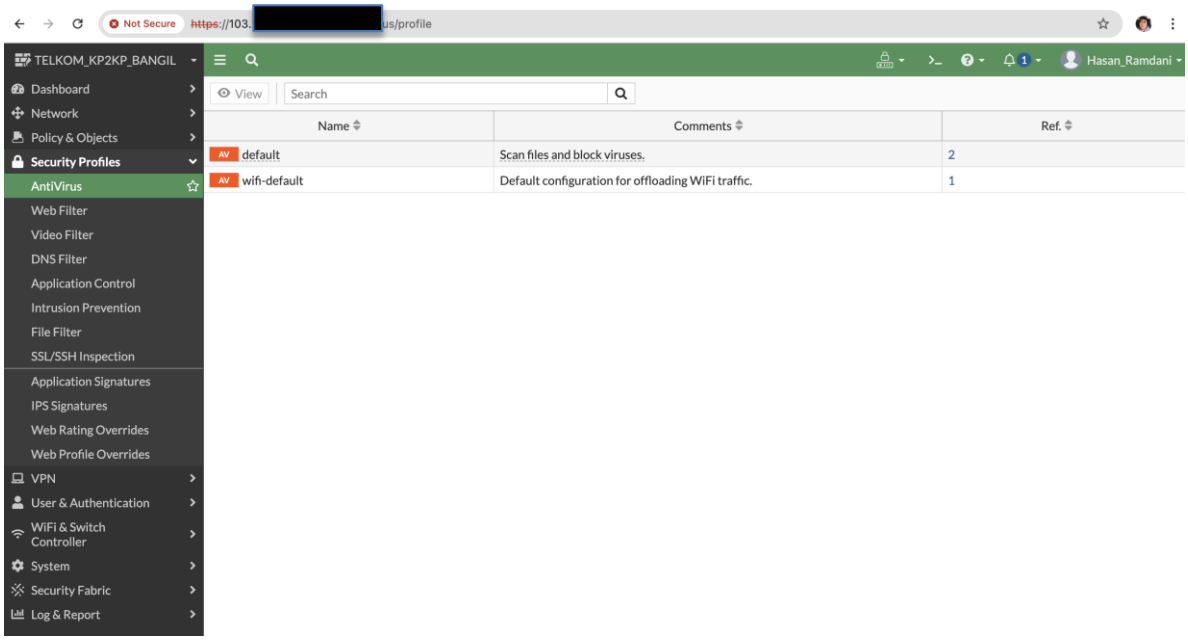
Pada gambar diatas memperlihatkan seluruh kantor vertikal yang ada di Kantor Direktorat Jenderal Pajak dapat dimonitor untuk kestabilan layanan jaringan serta keamanan sistem jaringan agar memperlancar kegiatan operasional pekerjaan harian di kantor pajak.

Simulasi Sistem Keamanan SD-WAN di KP2KP Bangil
Simulasi sistem keamanan SD-WAN ini peneliti mengambil disalah satu kantor vertikal yang ada di kantor pajak salah satunya di KP2KP Bangil. Untuk mengatur fitur keamanan pada SD-WAN ini dapat pertama kita buka melalui website dengan cara ketik https:/[redacted], alamat website ini hanya dikhususkan untuk *view* demi keamanan yang ada di Kantor Pusat DJP dengan tampilan sebagai berikut:

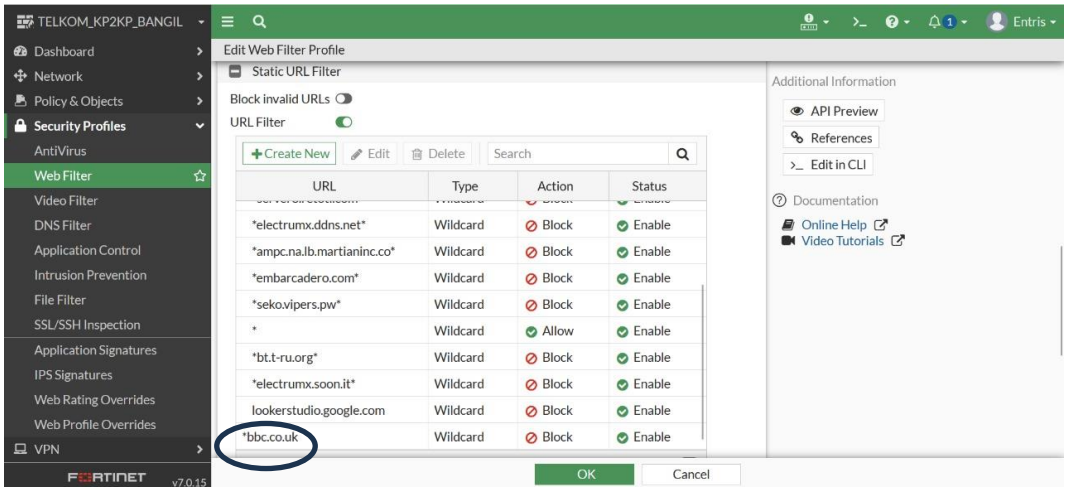


***Gambar 7** Dashboard Fortigate 60F*

Pada gambar diatas merupakan tampilan awal dari *dashboard Fortigate* SD-WAN dimana kita memasukan data berupa *user name* dan *password* sebagai berikut:
User name : Hasan_Ramdani
Password : [redacted]
Setelah melakukan otentikasi pada halaman login, kemudian dilanjutkan ke halaman pengaturan fitur keamanan. Pada halaman ini, terdapat beberapa menu pengaturan fitur keamanan sebagai berikut:

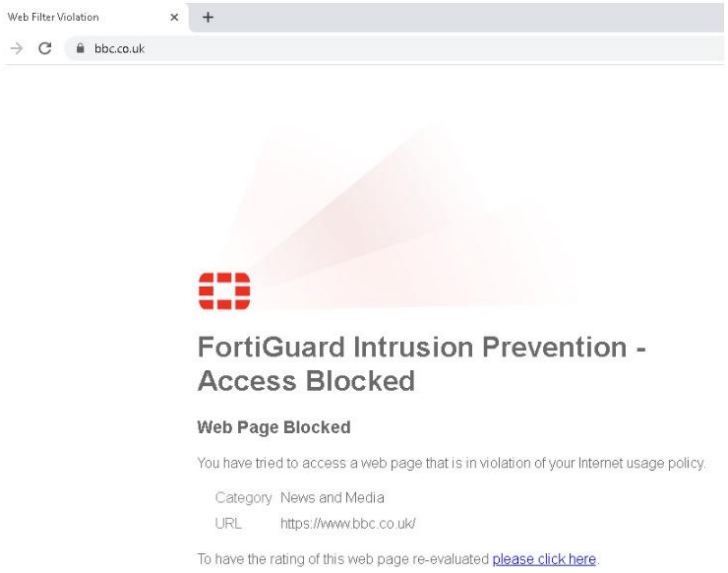


***Gambar 8** Dashboard Security Profiles*



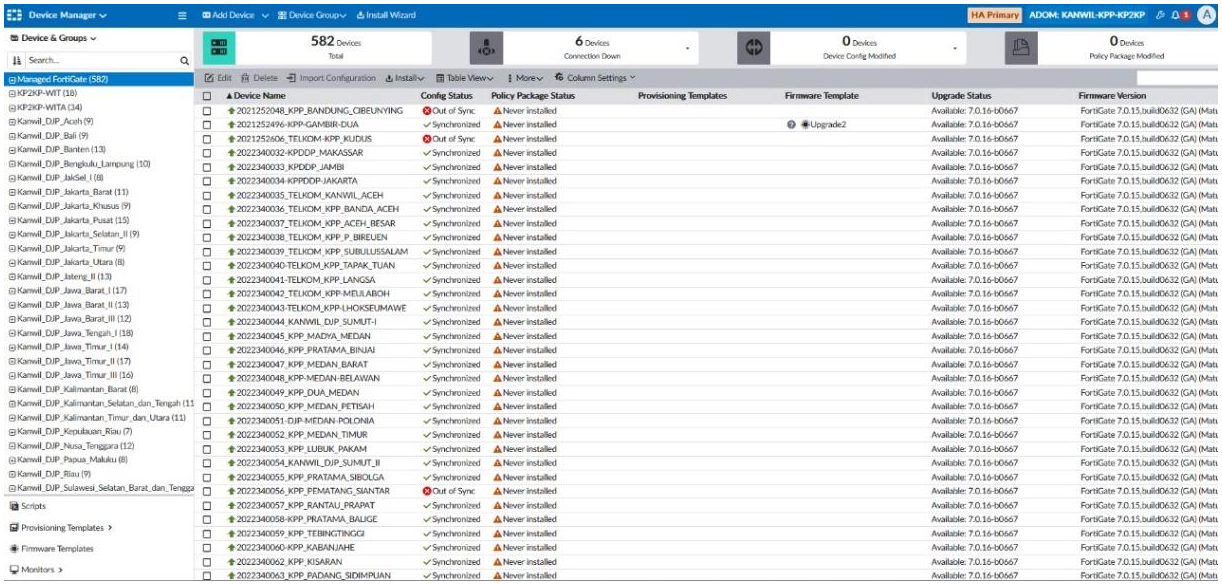
***Gambar 9** Pengaturan Web Fiter*

Pada gambar Pengaturan Web Filter diatas memperlihatkan untuk alamat www.bbc.co.uk kita block agar user yang mengakses alamat tersebut tidak bisa untuk membuka alamat ini, maka pada layar user di KP2KP Bangil akan tampil gambar dibawah ini:



Gambar 10 Sistem Keamanan SD-WAN pada Fortigate 60 F Aktif

Pada gambar sistem keamanan SD-WAN pada perangkat Fortigate 60 F di atas membuktikan bahwa sistem keamanan SD-WAN yang kita atur berhasil untuk ngeblock situs www.bbc.co.uk.
Semua fitur ini biasanya ditemukan dalam perangkat keamanan jaringan atau solusi seperti firewall canggih, UTM (Unified Threat Management), atau perangkat lunak keamanan untuk melindungi sistem dari ancaman siber dan memastikan keamanan data.
Dengan adanya fitur ini sistem keamanan di Kantor Direktorat Jenderal Pajak lebih optimal baik dari ancaman siber yang ada pada saat ini dimana data dari Wajib Pajak merupakan aset yang sangat besar terhadap target pencapaian pendapatan negara dalam sektor perpajakan yang berada di Indonesia.
Teknologi SDWAN akan memberikan kemudahan dalam pengaturan dan pengawasan kinerja jaringan WAN untuk seluruh unit kerja vertikal (UKV) DJP.
Direktorat Jenderal Pajak yang memiliki lebih dari 500 kantor vertikal yang harus dikelola aspek keamanannya, oleh sebab itu diperlukan teknologi yang dapat memudahkan pengaturan seluruh perangkat pada unit kantor vertikal.



Gambar 11 *Dashboard Forti Manager*

Pada gambar diatas memperlihatkan sebuah dasbor untuk memantau kinerja seluruh perangkat pada kantor vertikal DJP. Dasbor ini dapat digunakan oleh Direktorat TIK sebagai pusat pemantauan dan pengelolaan kinerja jaringan WAN seluruh kantor vertikal DJP.
Dengan adanya sebuah manajemen terpusat (*centralize management*) untuk semua perangkat SD-WAN di unit kerja, dengan kemampuan minimal sebagai berikut:

1. Memiliki *User Interface* berbasis *Graphical User Interface* (GUI);
2. Dapat memonitor status perangkat dan koneksi pada semua unit kerja;
3. Dapat melakukan *provisioning* secara *remote* (jarak jauh) dengan konsep *zero touch provisioning* (ZTP) atau *low touch;*
4. Dapat melakukan perubahan konfigurasi perangkat SD-WAN pada semua unit kerja secara terpusat.

3.2 Pembahasan

Pada penelitian sebelumnya yang dilakukan oleh (Sulistiyono, 2020) mengenai Peningkatan Keamanan dan Efisiensi Branch Office Dengan Software-Defined WAN (SD-WAN), dalam jurnal ini fokus pada keamanan di kantor cabang oleh karena itu saya mengembangkan dari sisi keamanan Kantor Pusat agar pengaturan pada sistem keamanan lebih terpusat dan terkontrol satu titik di kantor pusat tanpa tim IT terjun langsung ke site untuk visit ke kantor cabang.

Berdasarkan hasil diatas terdapat perbandingan model topologi WAN tradisional dengan yang dengan desain topologi SD-WAN yang diusulkan:

Tabel 2. Perbandingan Model Topologi yang di usulkan

No	Teknologi WAN Tradisional	Teknologi SD-WAN
1.	Menggunakan 3 perangkat yaitu Router seri 4321, UTM dan modem internet broadbang untuk menghubungkan 3 link pada setiap jaringan dari jasa penyedia layanan jaringan internet maupun intranet	Menggunakan 1 perangkat yaitu Fortigate seri 60 F untuk menghubungkan 3 link pada setiap jaringan dari jasa penyedia layanan jaringan internet maupun intranet

No	Teknologi WAN Tradisional	Teknologi SD-WAN
2	Koneksi leased line diatur menggunakan perangkat router yang menjadi gateway unit kerja untuk menuju WAN intranet	Koneksi leased line diatur menggunakan perangkat Fortigate yang menjadi gateway unit kerja untuk menuju WAN intranet
3	Tidak dapat melakukan pengaturan *Quality of Service* (QoS)	Dapat melakukan pengaturan *Quality of Service* (QoS)

Keberhasilan sistem keamanan dengan menggunakan teknologi SD-WAN sebagai berikut:

1. Gangguan pada link leased line akan dibackup oleh link internet sehingga layanan perpajakan di UKV tetap berjalan.
2. Security dapat diambil dengan log trafik serangan atau malware yg diblock oleh perangkat SD-WAN
3. Fitur keamanan yang digunakan sampain dengan layer 7 berupa aplikasi dapat melakukan proses IPS blocking, web filtering, antivirus, video filter, Aplication control.
4. Kegiatan operasional seperti pemantauan dan pengaturan akses intranet dan internet dapat dilakukan pada satu alat manajemen yang terintegrasi

4. KESIMPULAN

Dari hasil implementasi Penerapan Sistem Keamanan teknologi SD-WAN yang di lakukan di Kantor DJP sebagai berikut:

1. Topologi yang disampaikan ke Subdirektorat Pemantauan dan Pelayanan Sistem Informasi DJP dengan menggunakan teknologi SD-WAN dapat menyederhanakan desain jaringan sistem keamanan yang lebih optimal.
2. Perangkat Fortinet seri 60F yang telah disimulasikan di KP2KP Bangil memberikan dampak yang signifikan dari segi sistem keamanan, dimana semua layanan keamanan baik anti virus, web filter dan lain-lain sudah bisa di provide oleh perangkat SD-WAN.
3. Perangkat Forti Manager memberikan kemudahan untuk monitoring perangkat di seluruh kantor vertikal DJP.

Mengacu pada kesimpulan diatas, penulis memiliki beberapa saran untuk pengembangan ataupun penelitian lebih lanjut dalam implementasi SD-WAN ini, antara lain:

1. Adanya penelitian lebih lanjut pada sistem keamanan yang dilakukan pada Kantor Vertikal Direktorat Jenderal Pajak sebagai end user sekaligus penggguna layanan jaringan yang di sediakan oleh kantor pusat.
2. Kompleksitas teknologi SD-WAN salah satunya dalam penggunaan trafik penggunaan BW (Bandwidth) dimana disarankan untuk penelitian selanjutnya dapat mengambil topik terkait *Elastic Traffic Management*

Daftar Pustaka

[1] S. Sulistiyono, "Perancangan Jaringan Virtual Private Network Berbasis Ip Security Menggunakan Router Mikrotik," *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 7, no. 2, pp. 150–164, 2020, doi: 10.30656/prosisko.v7i2.2523.

[2] Junirma Buttu, "Analisis Kinerja Jaringan Wlan pada Sekolah Menengah Pertama Negeri 6 Palopo," *BANDWIDTH: Journal of Informatics and Computer Engineering*, vol. 1, no. 1, pp. 20–27, 2023, doi: 10.53769/bandwidth.v1i1.380.

[3] R. Chandra, "Virtualisasi Server Menggunakan Proxmox Untuk Mengoptimalkan Resource Server Pada SMK Bhakti Persada," vol. 1, no. 2, pp. 69–80, 2024.

[4] A. Z. Sianipar, P. Setiani, I. Junaedi, and V. Yasin, "Perancangan sistem informasi pelayanan penduduk berbasis website di rw 010 Kelurahan Keagungan Kecamatan Tamansari - Jakarta Barat," *Jurnal Manajamen Informatika Jayakarta*, vol. 1, no. 1, p. 20, 2021, doi: 10.52362/jmijayakarta.v1i1.414.

[5] K. Al Fikri and Djuniadi, "Keamanan Jaringan Menggunakan Switch Port Security," *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 5, no. 2, pp. 302–307, 2021.
[6] lmalik Muhammad Alviendra, Eko Setijadi, and Gatot Kusrahardjo, "Pengembangan dan Penerapan Sistem Virtual Private Network(VPN) pada Internet of Things(IOT) Menggunakan Simulasi," *Jurnal Teknik Its*, vol. 11, no. 1, 2022.
[7] A. Rosano and D. Sudrajat, "Perancangan Ruang Data Center Bank XYZ Menggunakan Standar ANSI/BICSI 002 dan Metode PPDIOO," *Jurnal Teknik Komputer AMIK BSI*, vol. 8, no. 2, pp. 174–180, 2022, doi: 10.31294/jtk.v4i2.
[8] R. Heryanto, I. Junaedi, and E. Kurniawan, "Perancangan Disaster Recovery Center (DRC) Pada PT. Samora Usaha Makmur," *Jurnal Sains dan Teknologi Widyaloka (JSTekWid)*, vol. 2, no. 2, pp. 169–178, 2023, doi: 10.54593/jstekwid.v2i2.182.
[9] M. R. Hidayat, R. Saragih, S. Basuki, A. Charisma, and A. D. Setiawan, "Implementasi Threat Mitigation Dan Traffic Policy Menggunakan UTM Pada Jaringan TCP/IP," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 2, pp. 437–446, 2024, doi: 10.25126/jtiik.20241127528.
[10] M. C. Shofwan and Y. Shalahuddin, "Study of QoS Comparison of UTP and Fiber Optic Cable Using the Wireshark Application," *JTECS : Jurnal Sistem Telekomunikasi Elektronika Sistem Kontrol Power Sistem dan Komputer*, vol. 3, no. 1, p. 1, 2023, doi: 10.32503/jtecs.v3i1.3335.
[11] M. D. S. Antariksa and A. Aranta, "Analisis Jaringan Komputer Local Area Network (LAN) Di Rumah Sakit UNRAM," *Jurnal Begawe Teknologi Informasi (JBegaTI)*, vol. 3, no. 2, pp. 201–212, 2022, doi: 10.29303/jbegati.v3i2.748.
[12] M. Hasibuan and C. E. Suharyanto, "IMPLEMENTASI DAN PERANCANGAN VOIP SERVER MENGGUNAKAN TRIXBOX OPENSOURCE DAN VPN SEBAGAI PENGAMANAN ANTAR CLIENT," *Jurnal Comasie*, vol. 4, no. 5, pp. 85–95, 2021.
[13] F. Nugroho and H. Ali, "Determinasi Simrs: Hardware, Software Dan Brainware (Literature Review Executive Support Sistem (Ess) for Business)," *Jurnal Manajemen Pendidikan Dan Ilmu Sosial*, vol. 3, no. 1, pp. 254–265, 2022, doi: 10.38035/jmpis.v3i1.871.
[14] S. Hadi and R. Wibowo, "IMPLEMENTASI MANAJEMEN BANDWIDTH MENGGUNAKAN QUEUE TREE PADA UNIVERSITAS SEMARANG," *Pengembangan Rekayasa dan Teknologi*, vol. 15, no. 2, pp. 112–117, Dec. 2019.
[15] Rahmadi, *PENGANTAR METODOLOGI PENELITIAN*, 1st ed., vol. 1. Banjarmasin: Antasari Press, 2011.
[16] Cisco, *Cisco Services for Carrier Ethernet*. Cisco System, 2008.