Jurnal Informatika Terpadu

https://journal.nurulfikri.ac.id/index.php/JIT
ISSN ONLINE : 2460-8998

IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE *SECURITY PROFILES* MENGGUNAKAN FORTIGATE PADA KOMISI APARATUR SIPIL NEGARA

Fauzi Rizki Arbie[1], Mugi Raharjo[2]

[1,2] Program Studi Informatika, Universitas Nusa Mandiri
Jakarta Selatan, DKI Jakarta, Indonesia 12540
fauzi.arbie@gmail.com, mugi.mou@nusamandiri.ac.id

Abstract

Current technological advances mean that all work carried out cannot be separated from the use of the internet network, both for accessing website pages to search for information and using applications as a medium for work. After conducting in-depth research, it was found that the network management and security used at the Pancoran State Civil Service Commission still uses default settings, causing less efficient use of the internet during work time, and is also vulnerable to attacks from outside. Network security is very important to protect data connected to the network both from the user and from the server side. Apart from that, administrators find it difficult to control access rights to web and applications that are not related to the needs of the organization or agency. To make it easier for administrators to control and improve network security, optimizing the use of the Fortigate 500E firewall is very necessary. By implementing the security profiles method on the Fortigate device, it will be easier to manage network traffic at preset hours and increase network security against irresponsible external attacks. By implementing the security profiles method, websites and applications that are not accordance with the organization's objectives can be blocked automatically according to the preset time and network security at KASN Pancoran will be maintained. With this implementation, internet use at the State Civil Service Commission can be more stable by determining access priority for frequently used applications.

Keywords: *Firewall Fortigate 500E, KASN, Network Security, Optimalization, and Security Profiles*

Abstrak

Kemajuan teknologi saat ini membuat semua pekerjaan yang dilakukan tidak lepas dari penggunaan jaringan internet, baik untuk mengakses halaman situs untuk mencari informasi maupun penggunaan aplikasi sebagai media untuk bekerja. Setelah dilakukan penelitian mendalam, ditemukan bahwa manajemen dan keamanan jaringan yang digunakan pada Komisi Aparatur Sipil Negara Pancoran masih menggunakan pengaturan *default*, menyebabkan penggunaan internet yang kurang efisien ketika waktu kerja, juga rentan terhadap serangan dari luar. Keamanan jaringan sangat penting untuk melindungi data yang terkoneksi dalam jaringan baik dari sisi pengguna maupun dari *server*. Selain itu administrator kesulitan untuk mengontrol hak akses terhadap *web* dan aplikasi yang tidak berkaitan dengan kebutuhan organisasi atau instansi. Untuk memudahkan administrator mengontrol serta meningkatkan keamanan jaringan, maka optimalisasi penggunaan *firewall* fortigate 500E sangat diperlukan. Dengan mengimplementasikan metode *security profiles* pada perangkat fortigate tersebut, maka akan memudahkan untuk mengatur lalu lintas jaringan pada jam – jam yang sudah diatur serta meningkatkan keamanan jaringan terhadap serangan dari luar yang tidak bertanggung jawab. Dengan implementasi metode *security profiles* tersebut, web dan aplikasi yang tidak sesuai dengan tujuan organisasi dapat di blok secara otomatis sesuai waktu yang sudah diatur dan keamanan jaringan pada Komisi Aparatur Sipil Negara Pancoran akan terjaga. Dengan implementasi ini penggunaan internet di Komisi Aparatur Sipil Negara dapat lebih stabil dengan menentukan *priority* akses terhadap aplikasi yang sering digunakan.

Kata kunci: *Firewall* Fortigate 500E, KASN, Keamanan Jaringan, Optimalisasi, dan *Security Profiles*

1. PENDAHULUAN

Kemajuan teknologi telah membawa pengaruh besar bagi kehidupan manusia secara global untuk mendapatkan informasi juga berkomunikasi secara cepat dan akurat. Hal itu terjadi juga pada cara kerja di instansi Komisi Aparatur Sipil Negara (KASN) yang terletak di daerah Pancoran, Jakarta. Namun, seiring dengan kemajuan tersebut, muncul

Diterima 04 Januari 2024, Direvisi 26 Februari 2024, Diterima untuk publikasi 20 Maret 2024

pula permasalahan serius, terutama terkait dengan kejahatan siber yang dapat berasal dari dalam atau luar sistem jaringan komputer, memberikan dampak negatif yang signifikan [1]. Adanya serangan virus dari luar yang disebabkan pengguna jaringan tidak teliti saat mengunjungi sebuah *website* saat akan mengunggah *file.* Munculnya perangkat lunak baru yang mendukung aktivitas di berbagai bidang, seperti jejaring sosial, bisnis, dan kegiatan akademis yang beroperasi di atas *platform* berbasis jaringan. Hal itu menyebabkan tugas yang diemban oleh jaringan komputer akan menjadi semakin kompleks, karena jumlah aplikasi berbasis jaringan atau aplikasi terdistribusi yang berada di lokasi yang berbeda semakin meningkat dan dapat diakses dari berbagai tempat [2], oleh sebab itu perlu dilakukan konfigurasi lebih lanjut terhadap perangkat jaringan yang di terapkan di KASN yang saat ini hanya menggunakan konfigurasi *default.* Selain guna meningkatkan efisiensi penggunaan *bandwidth*, juga dapat meningkatkan keamanan bagi pengguna dalam jaringan KASN.

Evolusi ini sesuai dengan kemajuan teknologi komputer dan jaringan komputer yang menghubungkan pengguna ke seluruh dunia, yang dikenal saat ini sebagai sistem jaringan atau *International networking*, yang umumnya disingkat sebagai Internet [3]. Dengan menerapkan pemfilteran situs web dan manajemen *bandwidth*, dapat memanfaatkan internet secara positif dan sehat, serta menjaga keamanan dan kinerja jaringan [4]. Untuk mengatur dan menjaga jaringan komputer atau internet di KASN Pancoran maka diperlukan perangkat *firewall*, dalam hal ini KASN Pancoran sudah menggunakan perangkat *firewall* fortigate, namun pengaturan yang digunakan belum maksimal guna menunjang kinerja pada waktu jam kerja, di mana lalu lintas jaringan padat.

Maka dari itu pengaturan lebih lanjut pada jaringan kantor KASN di Pancoran sangat diperlukan guna memaksimalkan keamanan bagi pengguna jaringan internet di dalam KASN Pancoran, serta manajemen penggunaan internet dan *bandwidth* yang sesuai dan demi mendukung fungsi dan tugas dari organisasi tersebut. Dengan mengimplementasikan metode *security profiles* pada perangkat *fortigate* tersebut, maka akan memudahkan untuk mengatur lalu lintas jaringan pada jam yang sudah diatur serta meningkatkan keamanan jaringan terhadap serangan dari luar yang tidak bertanggung jawab. Dengan implementasi metode *security profiles* tersebut, web dan aplikasi yang termasuk kategori kurang baik serta tidak ada hubungan dengan tujuan organisasi dapat di blok secara otomatis sesuai waktu yang sudah diatur dan keamanan jaringan pada KASN Pancoran akan terjaga.

Konsep Dasar Jaringan

Jaringan komputer adalah himpunan perangkat, termasuk komputer, printer, *switch*, dan perangkat lain yang saling terkoneksi menggunakan media kabel atau gelombang radio. Melalui koneksi ini, terjadi komunikasi dan pertukaran data antara perangkat – perangkat dalam jaringan [2]. Pada penelitian lainnya ada yang menyebutkan juga bahwa jaringan komputer adalah kumpulan komputer yang saling terhubung dan mandiri. Setiap komputer yang tergabung dalam jaringan komputer memiliki dan mengendalikan sistem operasinya sendiri, beroperasi secara mandiri [5].

Manajemen jaringan merupakan hal utama yang harus dilakukan seorang administrator jaringan guna mengatur dan mengawasi penggunaan jaringan internet dari jaringan lokal. Manajemen Jaringan Komputer melibatkan keterampilan dalam menerapkan metode tertentu untuk memantau, mengendalikan, serta merencanakan sumber daya dan komponen sistem jaringan komputer dan komunikasi yang digunakan. Pada manajemen jaringan selain pengaturan *bandwidth* yang digunakan agar penggunaannya yang tidak ada hubungannya dengan pekerjaan tidak berlebihan, serta melakukan pengecekan rutin, memonitor juga melakukan *maintenance* agar tidak terjadi masalah pada jaringan [6].

Topologi Jaringan

Merupakan suatu metode yang digunakan untuk menghubungkan dua komputer atau lebih, dengan menggunakan berbagai perangkat seperti Kabel *UTP*, Kabel Fiber Optik, *Straigh-Through*, *Cross-Over*, *Coaxial*, atau bahkan tanpa kabel (Nirkabel) sebagai media transmisi. Desain topologi jaringan ini secara pasti memberikan kemudahan kepada pengguna untuk berkomunikasi dengan pengguna lainnya, bahkan jika mereka berada di tempat atau lantai yang berbeda [7].

Alamat IP

Lebih dikenal sebagai *Internet Protocol Address* atau disingkat *IP Address,* merupakan sebuah protokol yang berfungsi memberikan alamat identifikasi pada setiap perangkat yang terhubung ke dalam jaringan. Disebutkan juga bahwa *IP Address* merupakan sebuah kode unik yang diibaratkan sebagai alamat rumah bagi setiap perangkat yang terhubung ke internet. Kode ini terdiri dari deretan angka (baik biner maupun desimal) dengan panjang 32 bit hingga 128 bit. Fungsinya adalah untuk mengidentifikasi dan menentukan lokasi perangkat tersebut dalam jaringan internet [8].

Konsep Penunjang Usulan

Dengan menggunakan *Fortigate* yang lebih dari sekadar perangkat keamanan jaringan biasa. Ia bertindak sebagai *gateway* dan *router* yang andal untuk *LAN (Local Area Network)*, sehingga Anda tidak memerlukan *router* atau perangkat *load balancing* tambahan, bahkan dengan koneksi WAN (*Wide Area Network*) ganda [9]. Implementasi keamanan jaringan menggunakan metode *security profiles* yang dilakukan pada perangkat *firewall* fortigate di KASN Pancoran dilakukan dengan

mengusulkan skema jaringan serta manajemen *traffic network schedules*, *web filtering* dan *application control* yang ada pada perangkat fortigate.

Firewall

Merupakan bentuk teknologi keamanan jaringan yang berfungsi mengatur paket data yang masuk ke dalam jaringan dan menentukan paket data yang akan diblokir. Selain itu, *firewall* digunakan untuk melindungi, membatasi, dan menolak koneksi antara jaringan pribadi dengan jaringan luar yang dianggap berpotensi membahayakan [10]. Dikatakan juga bahwa *firewall* merupakan alat perantara yang terletak di antara *web client* dan *web server*. Perangkat ini melakukan analisis terhadap pesan pada lapisan OSI Layer-7 ketika terjadi pelanggaran terhadap kebijakan keamanan yang telah ditetapkan [11]. *Firewall* diartikan juga sebagai sistem atau perangkat yang bertindak sebagai penjaga gerbang antara jaringan lokal Anda dan internet. Ia memfilter lalu lintas data yang masuk dan keluar, mengizinkan komunikasi yang aman, dan mencegah akses yang tidak sah [12]. Ada juga yang menyebutkan bahwa *Firewall* bagaikan penjaga keamanan siber yang cerdas, ia menggunakan teknik filter untuk menganalisis setiap paket data yang masuk dan keluar dari jaringan Anda. Ia bertindak layaknya detektif yang teliti, meneliti paket utama, sumber, dan tujuan data tersebut.

Fortigate

Fortigate adalah perangkat jaringan dengan sistem keamanan yang dirilis oleh perusahaan Fortinet. Fortinet merupakan sebuah perusahaan dan penyedia layanan yang beroperasi di seluruh dunia, termasuk di antara mayoritas perusahaan Fortune Global 100 pada tahun 2009. Fortinet memimpin pasar dalam hal *unified threat management* (UTM). Fortigate, sebagai perangkat, bertanggung jawab untuk menjamin keamanan jaringan secara menyeluruh, dan berperan sebagai *gateway* serta *router* untuk jaringan LAN, sehingga tidak memerlukan *router* tambahan atau perangkat penyeimbang beban jika terdapat lebih dari satu koneksi WAN [13]. Fortigate digunakan karena merupakan perangkat telah menyediakan fitur-fitur keamanan jaringan yang penting tanpa perlu membeli perangkat tambahan secara terpisah. Fortigate dapat diandalkan untuk menangani kompleksitas jaringan perusahaan menengah hingga besar. Penggunaan Fortigate juga dianggap sebagai investasi perusahaan dalam keamanan untuk melindungi data perusahaan [14].

Security Profiles

Merupakan komponen penting fitur *Unified Threat Management* (UTM) merupakan sebuah solusi yang disediakan pada konfigurasi *firewall* dengan biaya yang rendah untuk menghalau ancaman atau serangan dari luar berupa virus atau spam [2]. Itu semua terletak pada salah satu fitur yang disediakan perangkat fortigate dengan nama *security profile* [5].

Network Schedules

Lalu lintas data dalam jaringan dapat disesuaikan oleh administrator, mengonfigurasi waktu yang sudah ditentukan penggunaannya untuk menunjang kebutuhan pengguna.

Web Filtering

Salah satu metode layanan keamanan web yang disediakan oleh Fortinet, yang memiliki beberapa fungsi utama, seperti menghentikan konten yang tidak diinginkan atau berbahaya [15] juga tidak ada hubungannya dengan kebutuhan organisasi.

Application Control

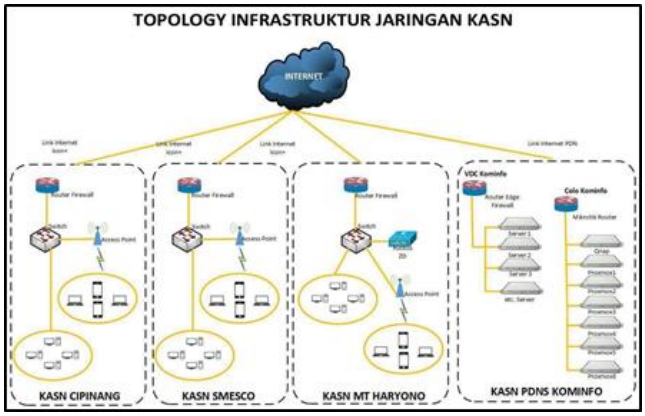
Merupakan pengaturan untuk menentukan tindakan apa yang harus dilakukan terhadap lalu lintas data aplikasi tersebut dalam jaringan.

2. METODE PENELITIAN

2.1. Metode Pengumpulan Data

2.1.1. Wawancara

Dalam penyusunan penelitian ini untuk mendapatkan informasi dengan selengkap – lengkapnya terkait permasalahan jaringan yang ada di KASN Pancoran, maka penulis melakukan tanya jawab dengan Kepala Bagian Data dan Pengawasan Internal yang memiliki tanggung jawab terhadap infrastruktur jaringan dan sumber daya Teknologi Informasi yang ada. Juga penulis melakukan tanya jawab dengan staf terkait yang memiliki tanggung jawab sebagai administrator jaringan. Salah satu yang penulis dapatkan dari hasil dari wawancara kepada staf terkait yaitu berupa topologi jaringan yang digunakan oleh instansi KASN yang akan ditampilkan pada Gambar 1 di bawah ini.

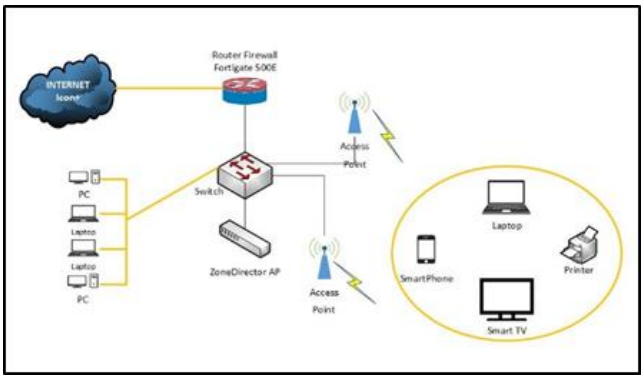


Gambar 1. Topologi Jaringan seluruh KASN

2.1.2. Observasi

Penulis melakukan pengamatan secara langsung guna melihat teknologi dan perangkat jaringan yang digunakan oleh KASN Pancoran. Metode ini dilakukan untuk mengumpulkan data yang benar serta akurat untuk digunakan sebagai bahan penelitian oleh penulis. Dari hasil observasi yang penulis lakukan, maka didapatkan data

skema jaringan yang digunakan di KASN Pancoran seperti Gambar 2 berikut ini:



Gambar 2. Skema jaringan KASN Pancoran

2.1.3. Studi Pustaka

Metode studi pustaka juga digunakan penulis untuk melengkapi data dalam penyusunan penelitian, memperkuat landasan teori mengenai keamanan serta manajemen jaringan. Penulis juga mencari referensi dengan mempelajari penelitian terdahulu yang memiliki latar belakang permasalahan yang tidak jauh berbeda dengan penelitian yang dilakukan saat ini sebagai tambahan referensi.

2.2. Tahapan penelitian

2.1.1. Analisis Kebutuhan

Dalam penelitian ini, setelah mengumpulkan informasi dengan cara observasi serta wawancara, keadaan jaringan yang terdapat pada KASN Pancoran maka diperlukan pengaturan tambahan pengaturan jaringan lebih optimal pada saat waktu kerja dan lebih aman bagi para pengguna.

2.1.2. Desain

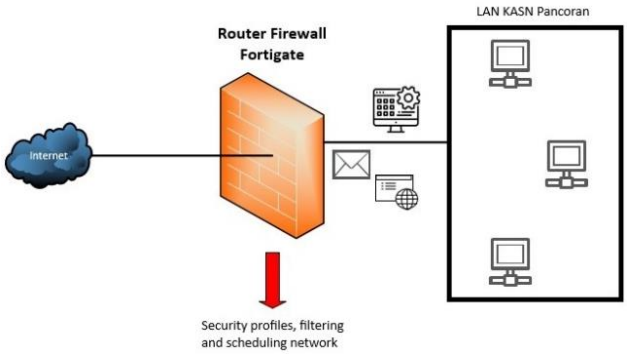
Penulis juga melakukan perancangan skema jaringan yang digunakan dengan menerapkan metode *security profile* guna menunjang pengaturan jaringan pada perangkat fortigate.

2.1.3. *Testing* dan Implementasi

Proses *testing* dilakukan terhadap beberapa pengguna saja yang nantinya akan dilakukan implementasi terhadap keseluruhan grup pengguna jaringan di KASN Pancoran.

3. HASIL DAN PEMBAHASAN

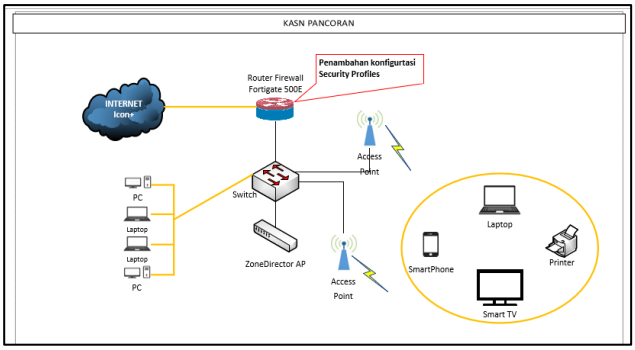
3.1. Skema Jaringan Usulan



Gambar 3. Usulan Skema Jaringan

Pada Gambar 3 penulis memberikan usulan berupa skema jaringan yang diusulkan akan ditambahkan pengaturan *security profiles* yang di dalamnya terdapat *filtering web* yang akan membatasi hak akses terhadap web yang dapat diakses, kemudian *application control* yang mengatur aplikasi mana saja yang diperkenankan diakses. semua itu akan dikombinasikan dengan *network schedule* yang mana setiap pengaturan akan berfungsi sesuai dengan waktu – waktu yang sudah ditentukan dan semua akan tercatat dalam *log* fortigate agar dapat membantu administrator memantau aktivitas pengguna jaringan serta menambah keamanan terhadap jaringan tersebut.

3.2. Topologi Jaringan Usulan



Gambar 4. Usulan Topologi Jaringan

Pada Gambar 4 di atas penulis menjelaskan lebih rinci mengenai usulan topologi yang akan digunakan dengan menggunakan perangkat fortigate sebagai *router* dan *firewall* yang kemudian akan dihubungkan ke *switch* untuk menghubungkan jaringan lokal, untuk jaringan nirkabel. Penggunaan perangkat *Zone Director* untuk mengatur seluruh *access point*.

Tabel 1. Kebutuhan *hardware* yang digunakan

No	*Hardware*
1	Fortigate FG-500E
2	Aruba Switch 48 Port
3	Ruckus ZoneDirector ZD 1200
4	Ruckus Access Point R510
5	PC / Laptop

Dalam Tabel 1 penulis menerangkan mengenai daftar perangkat keras yang akan digunakan untuk menjalankan usulan topologi dan skema jaringan pada instansi KASN Pancoran.

Tabel 2. Kebutuhan *software* yang digunakan

No	*Software*
1	OS Windows
2	MacOS
3	Browser Chrome/Edge/Safari

Pada Tabel 2 merupakan daftar perangkat lunak yang dipakai untuk menunjang implementasi dan pengetesan pada jaringan pada instansi KASN Pancoran.

3.3. Keamanan Jaringan

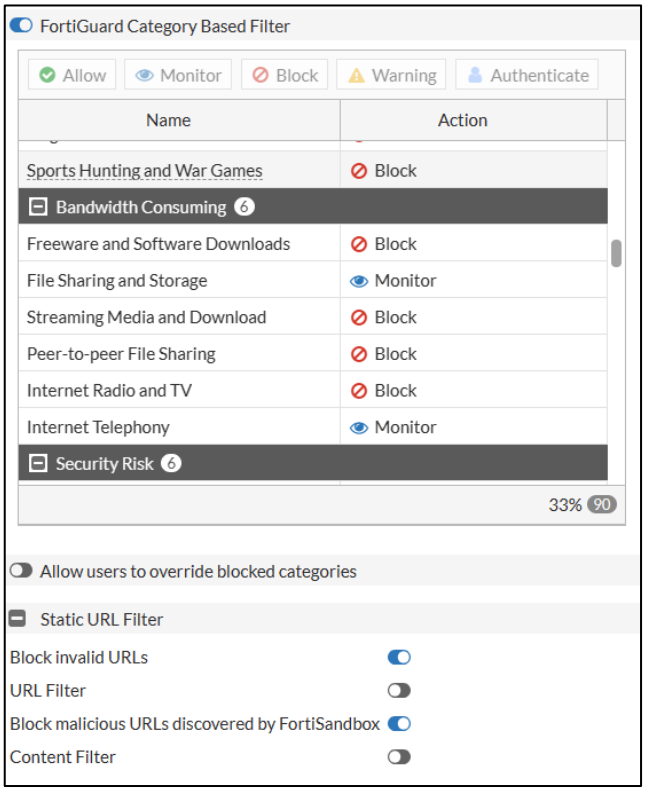
Pada keamanan jaringan instansi KASN Pancoran penulis mengusulkan untuk menerapkan pengaturan hak akses *web*, hak akses aplikasi serta pembagian waktu hak akses agar lebih aman dan mengoptimalkan penggunaan jaringan internet pada saat pengguna beraktivitas untuk kepentingan instansi.

3.4. Rancangan Aplikasi Jaringan

Pada rancangan ini penulis akan mengonfigurasi untuk implementasi metode *security profiles* dengan sejumlah fitur di dalamnya. Fitur yang akan penulis konfigurasi pada fortigate akan ditambahkan melalui aplikasi forti berbasis web aplikasi.

3.4.1. *Web Filtering*

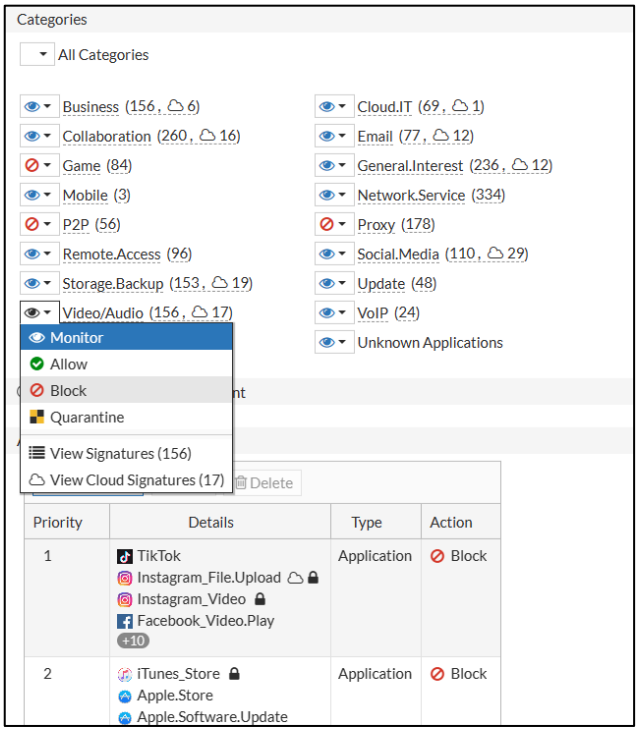
Pada Gambar 5 di bawah, merupakan bagian konfigurasi web *filtering* yang mana penulis akan melakukan konfigurasi mengenai kategori *website* apa saja yang diizinkan dan tidak diizinkan untuk diakses oleh pengguna jaringan, beri aksi blok untuk yang tidak diizinkan dan aksi monitor untuk akses yang diizinkan.



Gambar 5. *Web Filtering*

3.4.2. *Aplication Control*

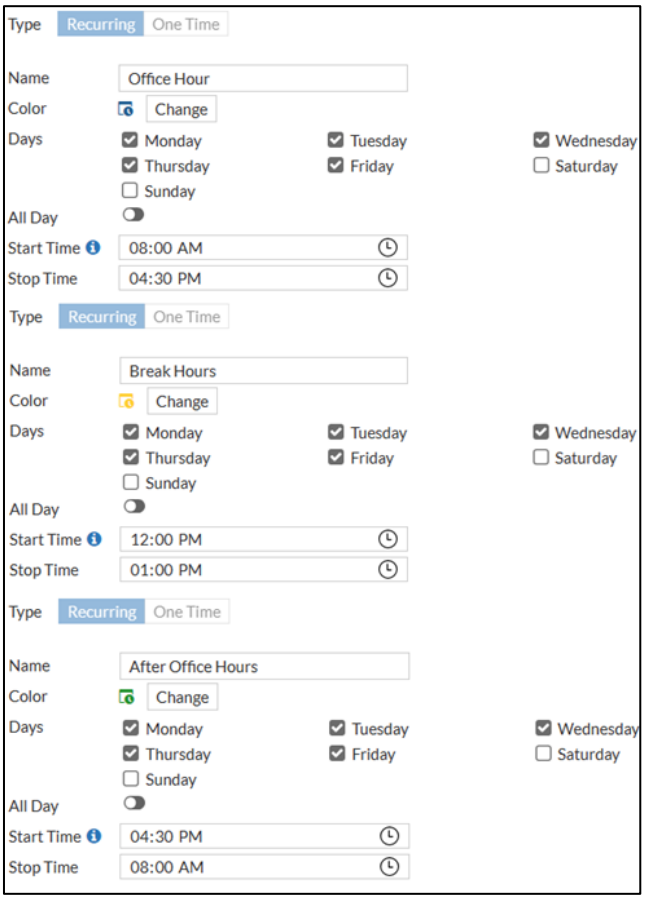
Pada *application control* penulis akan melakukan konfigurasi mengenai kategori aplikasi apa saja yang diizinkan dan tidak diizinkan untuk diakses oleh pengguna jaringan. Isi aksi blok untuk yang tidak diizinkan dan aksi monitor untuk akses yang diizinkan, seperti dengan yang ditampilkan pada Gambar 6 di bawah ini.



Gambar 6. *Application Control*

3.4.3. *Network Schedules*

Pada Gambar 7, ditampilkan fitur pembagian jadwal untuk menjalankan *policy* yang akan dibuat nantinya. Penulis akan membagi waktu menjadi 3, yaitu *Office hours, Break hours dan After Office Hours.* Di mana konfigurasi mengenai hak akses aplikasi dan web lebih ditekankan pada saat jam kerja untuk meningkatkan efektivitas dan keamanan saat bekerja. Pembatasan media sosial dan platform *streaming* selama jam kerja dengan *Rule Schedule* pada Fortinet dapat meningkatkan kinerja karyawan secara signifikan [12].

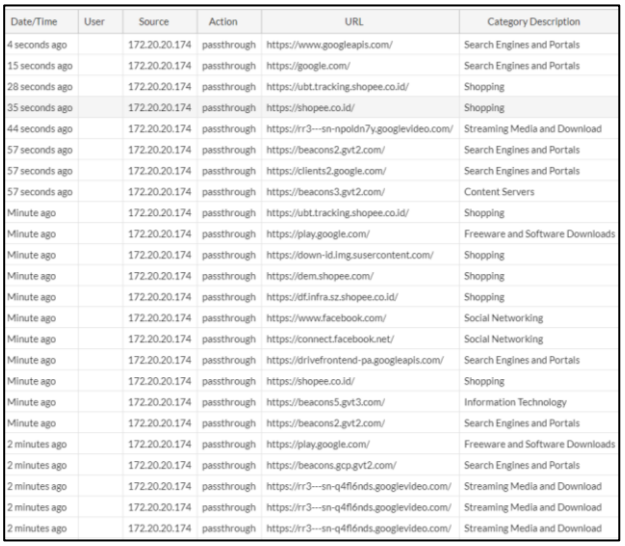


Gambar 7. *Network Schedules*

3.5. Pengujian Aplikasi Jaringan

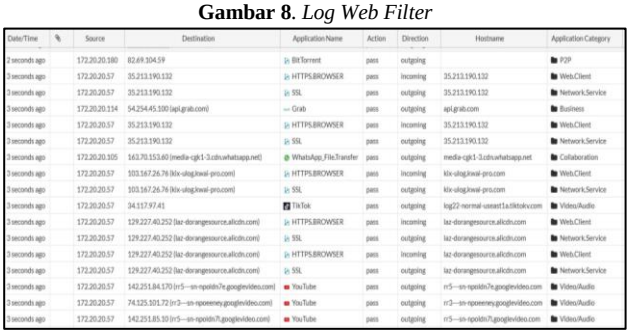
3.5.1. Pengujian Awal

Pada pengujian awal, penulis akan melakukan tes dengan melihat pada *log web filter dan log aplication control* , di mana *web* dengan kategori yang tidak ada kepentingannya dengan pekerjaan instansi KASN Pancoran masih bisa diakses, dan beberapa kategori tidak terdapat di log karena aksi pada pengaturan di fortigate masih standar. Itu semua akan dijelaskan dalam Gambar 8, Gambar 9 dan Gambar 10 di bawah ini untuk membuktikannya, dan sebagai acuan perbandingan sebelum dan setelah dilakukan konfigurasi.



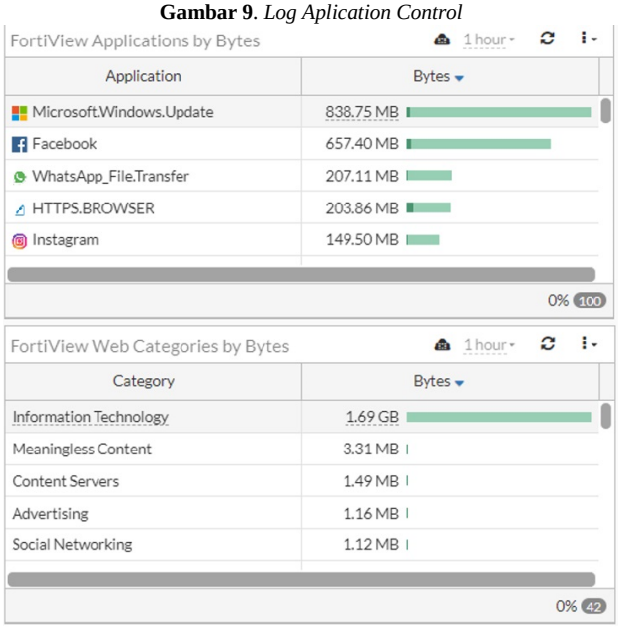
Date/Time	User	Source	Action	URL	Category Description
4 seconds ago		172.20.20.174	passthrough	https://www.googleapis.com/	Search Engines and Portals
15 seconds ago		172.20.20.174	passthrough	https://google.com/	Search Engines and Portals
28 seconds ago		172.20.20.174	passthrough	https://ubt.tracking.shopee.co.id/	Shopping
35 seconds ago		172.20.20.174	passthrough	https://shopee.co.id/	Shopping
44 seconds ago		172.20.20.174	passthrough	https://rr3---sn-npoidn7y.googlevideo.com/	Streaming Media and Download
57 seconds ago		172.20.20.174	passthrough	https://beacons2.gvt2.com/	Search Engines and Portals
57 seconds ago		172.20.20.174	passthrough	https://clients2.google.com/	Search Engines and Portals
57 seconds ago		172.20.20.174	passthrough	https://beacons3.gvt2.com/	Content Servers
Minute ago		172.20.20.174	passthrough	https://ubt.tracking.shopee.co.id/	Shopping
Minute ago		172.20.20.174	passthrough	https://play.google.com/	Freeware and Software Downloads
Minute ago		172.20.20.174	passthrough	https://down-id.img.susercontent.com/	Shopping
Minute ago		172.20.20.174	passthrough	https://dem.shopee.com/	Shopping
Minute ago		172.20.20.174	passthrough	https://df.infra.sz.shopee.co.id/	Shopping
Minute ago		172.20.20.174	passthrough	https://www.facebook.com/	Social Networking
Minute ago		172.20.20.174	passthrough	https://connect.facebook.net/	Social Networking
Minute ago		172.20.20.174	passthrough	https://drivefrontend-pa.googleapis.com/	Search Engines and Portals
Minute ago		172.20.20.174	passthrough	https://shopee.co.id/	Shopping
Minute ago		172.20.20.174	passthrough	https://beacons5.gvt3.com/	Information Technology
Minute ago		172.20.20.174	passthrough	https://beacons2.gvt2.com/	Search Engines and Portals
2 minutes ago		172.20.20.174	passthrough	https://play.google.com/	Freeware and Software Downloads
2 minutes ago		172.20.20.174	passthrough	https://beacons.gcp.gvt2.com/	Search Engines and Portals
2 minutes ago		172.20.20.174	passthrough	https://rr3---sn-q4fl6nds.googlevideo.com/	Streaming Media and Download
2 minutes ago		172.20.20.174	passthrough	https://rr3---sn-q4fl6nds.googlevideo.com/	Streaming Media and Download
2 minutes ago		172.20.20.174	passthrough	https://rr3---sn-q4fl6nds.googlevideo.com/	Streaming Media and Download

Gambar 8. *Log Web Filter*



Date/Time	Source	Destination	Application Name	Action	Direction	Hostname	Application Category
2 seconds ago	172.20.20.180	82.69.104.59	BitTorrent	pass	outgoing		P2P
3 seconds ago	172.20.20.57	35.213.190.132	HTTPS.BROWSER	pass	incoming	35.213.190.132	Web.Client
3 seconds ago	172.20.20.57	35.213.190.132	SSL	pass	outgoing	35.213.190.132	Network.Service
3 seconds ago	172.20.20.114	54.254.45.100 (api.grab.com)	Grab	pass	outgoing	api.grab.com	Business
3 seconds ago	172.20.20.57	35.213.190.132	HTTPS.BROWSER	pass	incoming	35.213.190.132	Web.Client
3 seconds ago	172.20.20.57	35.213.190.132	SSL	pass	outgoing	35.213.190.132	Network.Service
3 seconds ago	172.20.20.105	163.70.153.60 (media-cgk1-3.cdn.whatsapp.net)	WhatsApp_File.Transfer	pass	outgoing	media-cgk1-3.cdn.whatsapp.net	Collaboration
3 seconds ago	172.20.20.57	103.167.26.76 (klx-ulog.kiwai-pro.com)	HTTPS.BROWSER	pass	incoming	klx-ulog.kiwai-pro.com	Web.Client
3 seconds ago	172.20.20.57	103.167.26.76 (klx-ulog.kiwai-pro.com)	SSL	pass	outgoing	klx-ulog.kiwai-pro.com	Network.Service
3 seconds ago	172.20.20.57	34.117.97.41	TikTok	pass	outgoing	log22-normal-useast1a.tiktokv.com	Video/Audio
3 seconds ago	172.20.20.57	129.227.40.252 (laz-dorangesource.alicdn.com)	HTTPS.BROWSER	pass	incoming	laz-dorangesource.alicdn.com	Web.Client
3 seconds ago	172.20.20.57	129.227.40.252 (laz-dorangesource.alicdn.com)	SSL	pass	outgoing	laz-dorangesource.alicdn.com	Network.Service
3 seconds ago	172.20.20.57	129.227.40.252 (laz-dorangesource.alicdn.com)	HTTPS.BROWSER	pass	incoming	laz-dorangesource.alicdn.com	Web.Client
3 seconds ago	172.20.20.57	129.227.40.252 (laz-dorangesource.alicdn.com)	SSL	pass	outgoing	laz-dorangesource.alicdn.com	Network.Service
3 seconds ago	172.20.20.57	142.251.84.170 (rr5---sn-npoidn7e.googlevideo.com)	YouTube	pass	outgoing	rr5---sn-npoidn7e.googlevideo.com	Video/Audio
3 seconds ago	172.20.20.57	74.125.101.72 (rr3---sn-npoeenez.googlevideo.com)	YouTube	pass	outgoing	rr3---sn-npoeenez.googlevideo.com	Video/Audio
3 seconds ago	172.20.20.57	142.251.85.10 (rr5---sn-npoidn7f.googlevideo.com)	YouTube	pass	outgoing	rr5---sn-npoidn7f.googlevideo.com	Video/Audio

Gambar 9. *Log Aplication Control*

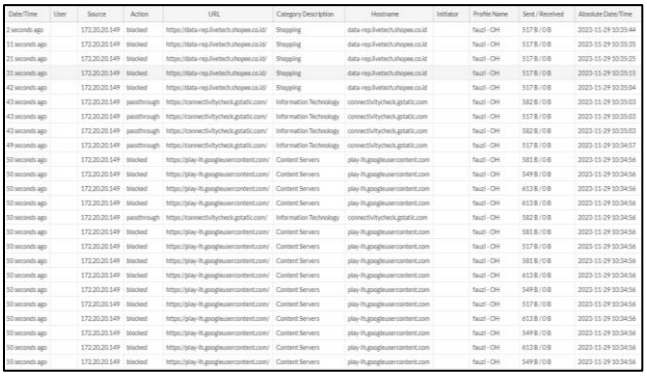


Gambar 10. Peringkat web dan aplikasi

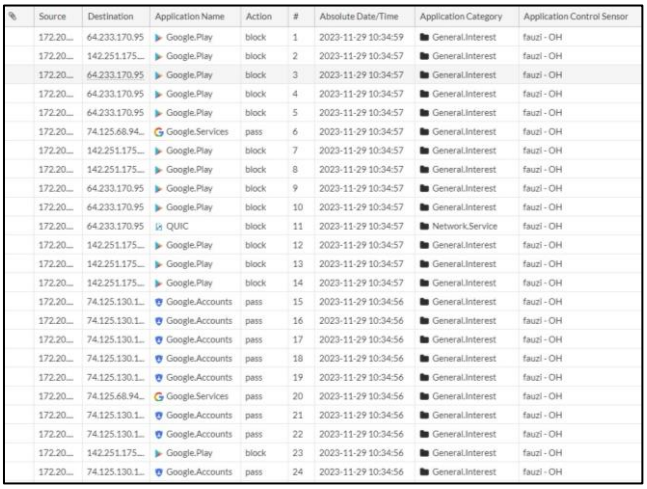
3.5.2. Pengujian Akhir

Pada pengujian akhir seperti yang ditampilkan pada Gambar 11 dan Gambar 12 berupa tangkapan layar dari *log web filter* dan *log application control*, dilakukan pengujian terhadap konfigurasi yang sebelumnya sudah dijalankan. Beberapa kategori sudah diberikan aksi monitor dan blok. Hasilnya web dan aplikasi yang kategorinya sudah ditentukan aksinya tidak dapat diakses pada saat jam kerja dan beberapa kategori dapat diakses saat jam kerja sudah berakhir. Serta

dari Gambar 13 merupakan tampilan dari sisi pengguna menggunakan *browser* ketika mengakses situs yang kategorinya sudah diberikan pembatasan hak akses.

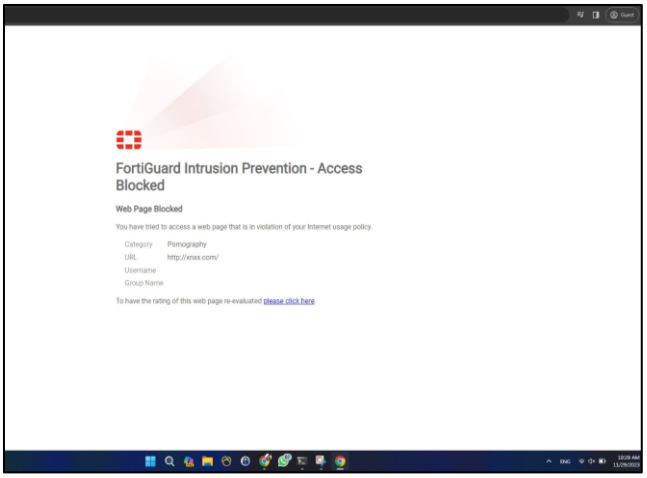


Gambar 11. *Log Block Web Filter*



Source	Destination	Application Name	Action	#	Absolute Date/Time	Application Category	Application Control Sensor
172.20....	64.233.170.95	Google.Play	block	1	2023-11-29 10:34:59	General.Interest	fauzi - OH
172.20....	142.251.175....	Google.Play	block	2	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	64.233.170.95	Google.Play	block	3	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	64.233.170.95	Google.Play	block	4	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	64.233.170.95	Google.Play	block	5	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	74.125.68.94...	Google.Services	pass	6	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	142.251.175....	Google.Play	block	7	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	142.251.175....	Google.Play	block	8	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	64.233.170.95	Google.Play	block	9	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	64.233.170.95	Google.Play	block	10	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	64.233.170.95	QUIC	block	11	2023-11-29 10:34:57	Network.Service	fauzi - OH
172.20....	142.251.175....	Google.Play	block	12	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	142.251.175....	Google.Play	block	13	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	142.251.175....	Google.Play	block	14	2023-11-29 10:34:57	General.Interest	fauzi - OH
172.20....	74.125.130.1...	Google.Accounts	pass	15	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	74.125.130.1...	Google.Accounts	pass	16	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	74.125.130.1...	Google.Accounts	pass	17	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	74.125.130.1...	Google.Accounts	pass	18	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	74.125.130.1...	Google.Accounts	pass	19	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	74.125.68.94...	Google.Services	pass	20	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	74.125.130.1...	Google.Accounts	pass	21	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	74.125.130.1...	Google.Accounts	pass	22	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	142.251.175....	Google.Play	block	23	2023-11-29 10:34:56	General.Interest	fauzi - OH
172.20....	74.125.130.1...	Google.Accounts	pass	24	2023-11-29 10:34:56	General.Interest	fauzi - OH

Gambar 12. *Log Aplication Control*



Gambar 13. Pengujian *user*

4. KESIMPULAN

Dari hasil pembahasan dan penelitian yang telah diuraikan, maka yang dapat disimpulkan di antaranya:

a. Fitur *security profiles* pada fortigate firewall menggabungkan berbagai fitur keamanan, seperti antivirus, *web filtering*, dan *application control*, untuk memberikan perlindungan terpadu terhadap ancaman jaringan.
b. Setelah dilakukan *web filtering*, *web* yang dirasa kurang aman akan di blok secara otomatis.
c. Dengan kemampuan *Application Control*, perusahaan dapat mengelola dan mengontrol aplikasi yang diizinkan atau diblokir, memberikan kontrol yang lebih baik terhadap penggunaan sumber daya jaringan yang dimiliki.
d. Penambahan Fitur *schedule network* memungkinkan perusahaan mengatur waktu akses tertentu, meningkatkan kontrol dan keamanan dengan membatasi akses ke sumber daya tertentu selama jam-jam tertentu sesuai dengan kebijakan internal.
e. Penggunaan internet di KASN Pancoran yang sebelumnya banyak digunakan untuk kepentingan di luar kebutuhan pekerjaan dapat diminimalisir dengan diimplementasikannya metode *security profiles* yang terdapat pada *firewall* fortigate, sehingga diharapkan dapat meningkatkan produktivitas pegawai.

Dengan kesimpulan ini, implementasi *Security Profiles* pada Fortigate *Firewall* selain memberikan fleksibilitas dan kontrol oleh administrator terhadap pengguna jaringan internet, juga memberikan keamanan jaringan internet. Hal tersebut sangat dibutuhkan untuk mendukung operasional perusahaan secara keseluruhan.

Ucapan Terima Kasih

Terima kasih kami ucapkan kepada Jurnal Informatika Terpadu atas kesempatannya dalam mempublikasikan tulisan ini, dan juga terima kasih kepada Komisi Aparatur Sipil Negara (KASN) Pancoran yang telah memberikan kesempatan dalam melakukan observasi. Kepada dosen pembimbing serta pihak kampus kami yang telah mendukung tiada henti dalam penyusunan jurnal ini.

DAFTAR PUSTAKA

[1] A. Riduan and N. Sadikin, “Perancangan Firewall Menggunakan Fortigate Di PT Swadharma Duta Data,” *J. Maklumatika*, vol. 8, no. 1, pp. 90–98, 2021, [Online]. Available: https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/122

[2] A. Wijaya, T. Dali Purwanto, J. Jenderal Ahmad Yani No, K. I. Seberang Ulu, K. Palembang, and S. Selatan, “JEPIN (Jurnal Edukasi dan Penelitian Informatika) Implementasi Metode Rekayasa Sistem Jaringan Komputer untuk Pengembangan Jaringan Komputer,” *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 3, pp. 294–300, 2019.

[3] S. Dewi and A. I. Islami, “Implementasi Web Filtering Menggunakan Router Fortigate FG300D,” *INSANtek*, vol. 2, no. 1, pp. 22–27, 2021, doi: 10.31294/instk.v2i1.424.

[4] A. Dzulfiqri and A. Hidayat, “Implementasi Manajemen Bandwidth Dan Filtering Content Dengan Router Mikrotik Pada Smp Muhammadiyah 3 Metro,” *J. Mhs. Ilmu Komput.*, vol. 3, no. 2, pp. 324–331, 2022.

[5] M. Ikhsan, "Optimalisasi Keamanan Jaringan dan Internet dengan Fitur Unified Threat Management pada Perangkat Firewall," *SENTINEL*, vol. 1, no. 1, pp. 21–36, 2018, doi: 10.56622/sentineljournal.v1i1.4.

[6] S. Faizah, E. Pudjiarti, and A. Saryoko, "Perancangan Jaringan Dengan Menggunakan Static Routing Dan VPN PPTP Pada SMK Bina Putra," *Bina Insa. Ict J.*, vol. 9, no. 1, p. 53, 2022, doi: 10.51211/biict.v9i1.1728.

[7] Meilinaeka, "Mengenal Macam Macam Topologi pada Jaringan Komputer," Universitas Telkom. Accessed: Dec. 28, 2023. [Online]. Available: https://it.telkomuniversity.ac.id/mengenal-macam-macam-topologi-jaringan/

[8] E. Dwi Setiawan and M. Raharjo, "Jurnal Informatika Terpadu," *J. Inform. Terpadu*, vol. 9, no. 1, pp. 34–39, 2023, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[9] N. Bayu and A. Susila, "Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan VPN Berbasis SSL-VPN (Studi Kasus: Kementerian PANRB)," *Log. J. Ilmu Komput. dan …*, vol. 2, no. 1, pp. 153–159, 2023, [Online]. Available: https://journal.mediapublikasi.id/index.php/logic/article/view/2899%0Ahttps://journal.mediapublikasi.id/index.php/logic/article/download/2899/2214

[10] D. Wicaksono, "Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.v9i2.2103.

[11] G. H. A. Kusuma, "Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19," *J. Informatics Adv. …*, vol. 2, no. 2, pp. 1–4, 2021, [Online]. Available: http://journal.univpancasila.ac.id/index.php/jiac/article/view/3259

[12] B. A. Prasetia, D. A. Ramadhany, G. Guniawan, and I. G. Waluyo, "Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia Analisa Perangkat Fortinet Sebagai Firewall Untuk Memblokir Aplikasi Sosial Media Dan Platform Streaming Saat Jam Kerja (Studi Kasus : PT. Aplikanusa Lintasarta)," *Biner J. Ilmu Komput. , Tek. dan Multimed.*, vol. 1, no. 3, pp. 496–504, 2023, [Online]. Available: https://journal.mediapublikasi.id/index.php/Biner

[13] A. Fitriadi and H. A. Tawakal, "Jurnal Informatika Terpadu," *J. Inform. Terpadu*, vol. 7, no. 2, pp. 62–69, 2021, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[14] H. Suryantoro, A. Sopian, and D. Dartono, "Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan Vpn-Ip Berbasis Ipsec," *Jeis J. Elektro Dan Inform. Swadharma*, vol. 1, no. 1, pp. 1–7, 2021, doi: 10.56486/jeis.vol1no1.64.

[15] B. Prasetyo, A. Puspitasari, and R. Nasution, "IMPLEMENTASI MANAJEMEN BANDWIDTH DAN FILTERING WEB ACCESS CONTROL MENGGUNAKAN METODE ADDRESS LIST," *JIKA (Jurnal Inform.*, vol. 3, no. 2, 2019, doi: 10.31000/jika.v3i2.2192.