INSANtek – Jurnal Inovasi dan Sains Teknik Elektro
Volume 2 No. 1 Mei 2021
E-ISSN: 2722-547X

Implementasi Web Filtering Menggunakan Router Fortigate FG300D

Sari Dewi [1], Adam Iqbal islami[2]

[1,]Universitas Bina Sarana Informatika, Sistem Informasi PSDKU Pontianak
e-mail: sari.sre@bsi.ac.id

[2] Universitas Bina Sarana Informatika, Teknologi Komputer
e-mail: adamiqbal070798@gmail.com

Abstrak - Perkembangan teknologi saat ini sejalan dengan kemajuan teknologi jaringan internet yang menghubungkan user ke seluruh dunia. Untuk Lokal Area Networking (LAN) atau sistem jaringan komputer lokal saat ini sudah menjadi sistem yang wajib dibangun oleh perkantoran modern untuk membantu kelancaran tugas-tugas komputerisasi dan komuikasi.Penggunaan dan pemanfaata teknologi informasi berbasis internet bagi perusahan merupakan salah satu implementasi produk teknologi yang dijadikan tulang punggung sekaligus urat nadi dalam meningkatkan kinerja perusahaan. Masih terdapatnya akses ke dalam laman web atau situs tertentu seperti, media sosial dan web streaming video yang tidak ada kaitannya dengan pekerjaan . Sehingga hal ini sering kali di salah gunakan oleh karyawan yang dapat mengganggu kinerja mereka dengan diterapkannya konfigurasi web filter melalui aplikasi berbasis web Fortinet, yang ada di router Fortigate 300D. Dimana pemblokiran laman web situs dan aplikasi tersebut berguna agar user tidak dapat mengakses situs yang tidak sesuai pekerjaan.

Kata Kunci: Jaringan Komputer, Lokal Area Network (LAN), Web Filter, Router, Fortinet, Fortigate FG300D

PENDAHULUAN

Di jaman modern saat ini kemajuan teknologi khususnya teknologi informasi berkembang dengan pesat. Perkembangan ini sejalan dengan kemajuan teknologi komputer dan jaringan komputer yang menghubungkan user ke seluruh dunia yang lebih dikenal saat ini sebagai sistem jaringan atau International networking yang disingkat Internet.

Untuk Lokal Area Networking atau sistem jaringan komputer lokal saat ini sudah menjadi sistem yang wajib dibangun oleh perkantoran modern untuk membantu kelancaran tugas-tugas komputerisasi dan komuikasi (Supriyanto, 2019).

Oleh karena itu keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang yang sudah pasti membutuhkan keseriusan dan dana tidak sedikit (Farly, Najoan, & Lumenta, 2017). Pastilah suatu perusahaan yang menjadikan TI sebagai strategi untuk bersaing didunia global ini membutuhkan solusi system keamanan ini. Maka kualitas sumber daya manusia dalam membangun suatu sistem jaringan menjadi sangat diperlukan.

Menurut (Dewi, Riyadi, Suwastitaratu, & Hikmah, 2020) Dengan memanfaatkan internet,Selain mudah dan cepat, penggunaan internet dapat menekan biaya operasional perusahaan. Tetapi dengan segala kelebihannya, internet juga memiliki kelemahan. Internet yang dapat diakses oleh semua orang membuatnya menjadi tidak aman untuk mengirimkan informasi yang sifatnya rahasia. Apalagi sudah banyak bermunculan aplikasi-aplikasi yang bisa membobol pesan dengan sangat mudah, yang dilakukan oleh para hacker yang tidak beranggung jawab, Penggunaan dan pemanfaatan teknologi informasi berbasis internet bagi PT. Karlin Mastrindo merupakan salah satu implementasi produk teknologi yang dijadikan tulang punggung sekaligus urat nadi dalam meningkatkan kinerja perusahaan.

Fortigate sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai gateway dan router bagi jaringan LAN (Local Area Network) sehingga tidak dibutuhkan lagi router ataupun perangkat tambahan load balancing bila ada lebih dari satu koneksi WAN (Wide Area Network) (Faizan, Hegde, & Yaligar, 2019). Satu perbedaan yang utama, konten FortiASIC yang di custom sendiri serta prosesor jaringan fortinet memungkinkan sistem fortigate mendeteksi dan mengeliminir secara real time ancaman yang terintegrasi, bahkan dalam skala kompleks, tanpa menurunkan kinerja jaringan, sementara serangkaian proses manajemen, analisa, database dan solusi perlindungan endpoint bekerja meningkatkan penyebaran fleksibilitas dan memberikan dampak yang nyata dalam mengurangi biaya operasional manajemen keamanan jaringan (Sistem, Agustina, & Rifqi, 2021)

METODE PENELITIAN

Pada Metode penelitian ini Penulis melakukan pengamatan-pengamatan langsung terhadap kegiatan yang berhubungan dengan masalah yang diambil. Hasil dari pengamatan tersebut langsung dicatat oleh penulis dan dari kegiatan observasi ini dapat diketahui kesalahannya atau proses dan kegiatan tersebut di Gedung Dipo Business Centre (Dipo Tower), Lantai 12, PT. Karlin Mastrindo. Jl. Jend. Gatot Subroto No.Kav 50-52, RW.7, Petamburan, Tanah Abang, Kota Jakarta Pusat, DKI Jakarta. Selain melakukan kegiatan tersebut diatas penulis juga melakukan studi kepustakaan melalui literatur-literatur mengenai.

HASIL DAN PEMBAHASAN

Pada PT. Karlin Mastrindo menggunakan Internet Service Provider (ISP) First Media dengan cara berlangganan bulanan. Menjalankan kegiatan sehari-hari dua jaringan yaitu jaringan kabel UTP dan jaringan wifi. Jaringan komputer LAN digunakan oleh PT. Karlin Mastrindo, terutama pada gedung mempunyai sistem jaringan komputer yang terdiri dari dua buah switch dan terinstal pada ruang data center dan ruang finance dan yang lainnya saling terkoneksi (terhubung).

Kebutuhan akan jaringan komputer PT. Karlin Mastrindo digunakan untuk berbagai fungsi diantaranya adalah :

1. Untuk pertukaran informasi
2. Pemakaian secara bersama sumber daya komputer.
3. Akses bersama ke Internet
4. Mempermudah pengawasan terhadap pemakaian komputer karyawan/karyawati.

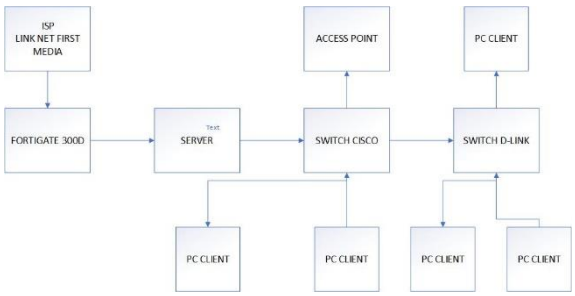
Maka untuk menghubungkan jaringan antara komputer pada PT. Karlin Mastrindo, khususnya jaringan yang terpasang pada ruang data center menggunakan switch, dan telah membentuk suatu jaringan komputer LAN.

Switch yang dipakai untuk jaringan komputer LAN pada PT. Karlin Mastrindo merupakan komponen jaringan komputer yang memiliki banyak port yang akan menjadi penghubung bagi banyak titik jaringan atau node sehingga akan membentuk jaringan komputer LAN pada topologi bus.

Untuk lebih jelasnya, di bawah ini penulis mendeskripsikan secara umum analisa yang telah penulis lakukan pada PT. Karlin Mastrindo adalah sebagai berikut:

1. ISP (Internet Service Provider) yang digunakan yaitu Link Net First Media dengan cara berlangganan bulanan.
2. Terdapat 1 unit switch Cisco 2960 48 port dan 5 switch D-Link 1024A masing-masing 24 port yang digunakan sebagai alat untuk menghubungkan jaringan LAN di PT. Karlin Mastrindo.
3. Terdapat 1 unit access point pada ruang staff.
4. Menggunakan kabel cat 5e dan konektor RJ45 yang digunakan sebagai media penghubung antar perangkat jaringan.

1. Blok Jaringan

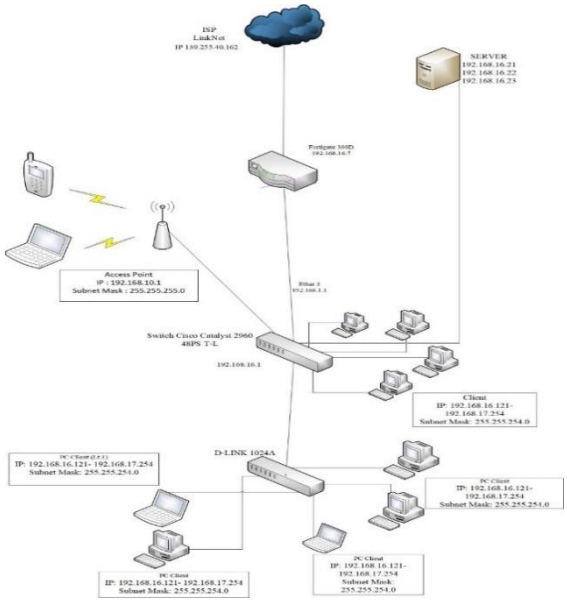


Gambar 1. Blok Jaringan PT. Karlin Mastrindo

Keterangan dari gambar blok diagram pada jaringan PT. Karlin Mastrindo adalah sebagai berikut :

1. ISP (Internet Service Provider) yang digunakan yaitu menggunakan Link Net First Media di hubungkan ke Fortigate.
2. Access Point menggunakan TP-LINK Auranet EAP110 merupakan pilihan yang tepat karena fiturnya yang Multi-SSID membagi beberapa jaringan nirkabel untuk pengguna yang berbeda.
3. Terdapat 1 switch Cisco Catalyst 2960-X Series yang langsung terhubung ke Fortigate. Lalu dari switch Cisco 2960 Catalyst 2960-X Series terhubung ke switch D-LINK 1024A beruntun.
4. Topologi yang digunakan adalah bus.

2. Skema Jaringan



Gambar 2. Skema jaringan PT. Karlin Mastrindo

Dilihat dari skema jaringan yang terdapat pada PT. Karlin Mastrindo Jakarta dapat diketahui bahwa :

1. Internet Service Provider (ISP) pada PT. Karlin Mastrindo Jakarta menggunakan Link Net First Media dengan media transfer berupa kabel serat optik, dengan Bandwidth 50 Mbps.
2. PT. Karlin Mastrindo Jakarta menggunakan Switch Cisco Catalyst 2960 48 port sebagai switch pusat yang terhubung dari router Fortigate 300D dan disambung ke komputer client (karyawan). Tedapat juga switch D-Link 1024A 24 port.
3. Komputer yang terdapat pada PT. Karlin Mastrindo Jakarta berbeda di setiap ruangan , jumlah komputer diruang Finance berjumlah 5 unit, ruang Accounting berjumlah 5 unit dan ruang karyawan 40 unit.
4. Kabel yang digunakan pada PT. Karlin Mastrindo Jakarta adalah kabel Unshielded Twisted Pair berjenis Category 5 dan RJ-45 sebagai konektor.

3. Keamanan Jaringan Komputer

Sistem keamanan jaringan di PT. Karlin Mastrindo terdapat hotspot tertutup dengan sistem keamanan WPA2/PSK yang terpasang pada access point. Sehingga yang dapat mengakses masuk jaringan wifi di PT. Karlin Mastrindo hanya karyawan yang mengetahui password dari access point nya saja. Keamanan jaringan PT. Karlin Mastrindo menggunakan firewall Fortigate untuk melindungi jaringan lokal dari serangan luar ataupun serangan dari dalam.

4. Perangkat Fortigate

Fortigate merupakan sebuah perangkat yang digunakan untuk melindungi sebuah jaringan dari berbagai macam serangan seperti virus dan hacking, dari hasil informasi yang penulis dapatkan fortigate memiliki beberapa keunggulan seperti antivirus, web filtering dan kontorling aplikasi (Ipsec, 2021), namun disini penulis hanya akan membahas masalah web filtering, web filtering sendiri merupakan sebuah metode keamanan web service yang diberikan oleh fortinet, dengan berbagai fungsi utama yaitu memblokir sebuah kontent yang tidak pantas, dan terdapat fungsi lain selain memblokir yaitu memisahkan malware yang tersimpan pada iklan yang terdapat pada sebuah web, dari beberapa sumber mengatakan bahwa terdapat beberapa kategori dari kontent yang terdapat pada web filter diantaranya : 76 kategori, 40 juta domain, lebih dari 1 milyar web page, dan kontent yang update otomatis (Of & Xx, 2011).

Sumber : https://www.fortinet.com/demo-center.html
Gambar 3. Proses Filter Fortigate

Gambar diatas menunjukkan bahwa fortigate digunakan sebagai media untuk mengamankan jaringan internet dari beberapa gangguan virus maupun hacker yang memasukan virus kedalam beberapa content yang terdapat pada sebuah situs, fortigate dapat memf ilter sebuah situs jika terdeteksi memiliki beberapa virus didalamnya, karena fortigate memiliki sistem antivirus untuk mengamankan jaringan dari virus.

Menurut analisa penulis terdapat permasalahan di PT. Karlin Mastrindo sebagai berikut :

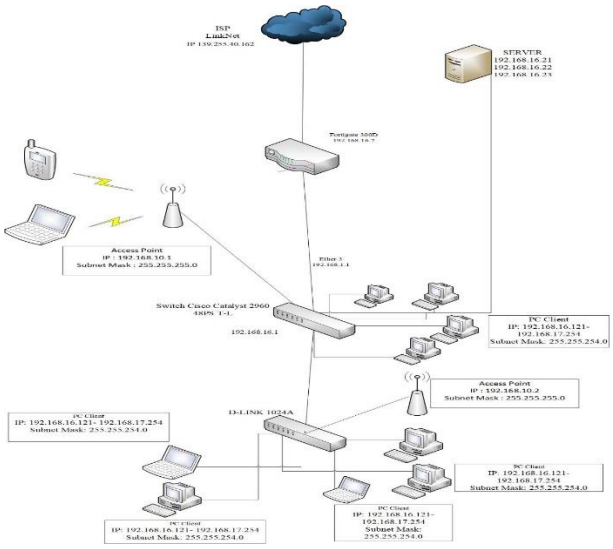
Masih terdapatnya akses ke dalam laman web atau situs tertentu seperti, media sosial (Facebook, Instagram, Twitter) dan web streaming video (youtube, netflix) yang tidak ada kaitannya dengan pekerjaan di PT. Karlin Mastrindo. Sehingga hal ini sering kali di salah gunakan, baik untuk karyawan maupun peserta sertifikasi yang dapat mengganggu kinerja mereka. Kurang adanya Hotspot/Wifi, sehingga akses internet belum sepenuhnya berjalan dengan baik dan masih terdapat perangkat client (karyawan) seperti laptop yang terhubung langsung dengan kabel LAN. Sehingga hal itupun menyulitkan aktivitas pekerjaan client (karyawan), dikarenakan sering melakukan cabut dan pasang ketika laptop client tersebut harus dibawa ke ruangan atau ke tempat lain.

5.Pemecahan Masalah

Beberapa kendala atau kekurangan pada jaringan internet yang telah dijelaskan pada bagian permasalahan pokok tersebut menunjukan adanya keterbatasan yang bisa menyebabkan kinerja jaringan maupun kinerja karyawan pada PT. Karlin Mastrindo menjadi tidak maksimal. Dari masalah-masalah pokok yang penulis temukan selama melakukan riset di PT. Karlin Mastrindo penulis memiliki beberapa solusi untuk menyelesaikan permasalahan tersebut, yaitu :

Penulis memberikan solusi untuk melakukan pemblokiran situs (Facebook, Instagram, Twitter, Youtube) dengan cara mengkonfigurasi web filter melalui aplikasi berbasis web Fortinet, yang ada di Fortigate 300D. Dimana pemblokiran laman web situs dan aplikasi tersebut berguna agar user (karyawan) tidak dapat mengakses situs yang tidak sesuai pekerjaan. Penambahan 1 access point Linksys Ea8500, dimana access point ini digunakan sebagai pemancar jaringan ke perangkat client (karyawan) seperti smartphone dan laptop. Access point tersebut dikoneksikan secara langsung pada jaringan wireless yang ada, sehingga perangkat client

itupun tidak lagi harus melakukan cabut atau pasang kabel LAN yang dinilai kurang efisien.

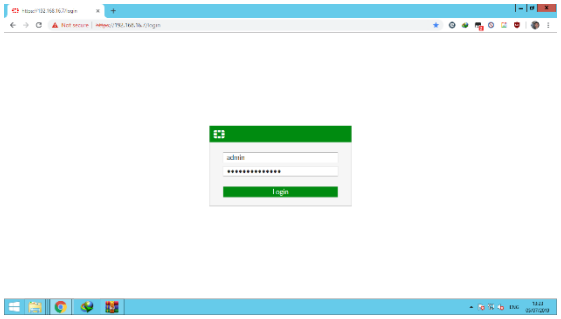


Gambar 4. Skema jaringan usulan PT. Karlin Mastrindo.

Dari skema jaringan usulan pada gambar III.6, penulis menambahkan 1 buah access point Linksys Ea8500. Bertujuan agar user mendapatkan sinyal yang lebih kuat dalam menggunakan jaringan wireless melalui access point**.**

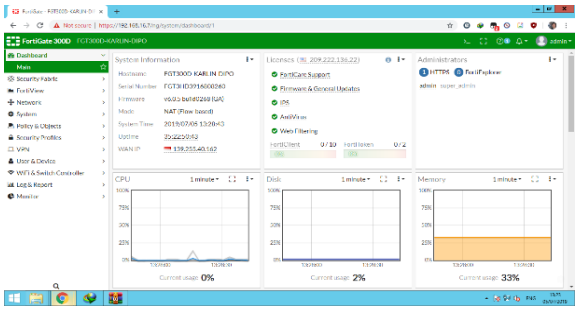
3.5.2. Konfigurasi Usulan

Peran Fortigate dalam pembatasan hak akses ini adalah untuk membatasi pengguna dalam mengakses website. Selanjutnya penuli akan menentukan website mana saja yang boleh diakses dan website mana yang tidak boleh diakses. Untuk mengkonfigurasi Fortigate dapat dilakukan dengan mengaksesnya melalui web admin. Yang artinya dalam proses konfigurasi selanjutnya akan dilakukan melalui web browser. Dalam implementasi ini Penulis menggunakan web browser Google Chrome. Sesuai dengan pembagian alamat IP yang sudah dilakukan di tahap sebelumnya, perangkat Fortigate dapat diakses di alamat https://192.168.16.7.



Gambar 5. Tampilan login admin pada web browser

Setelah login, menu awal muncul seperti ini：



Gambar 6. Tampilan awal setelah login admin pada web browser

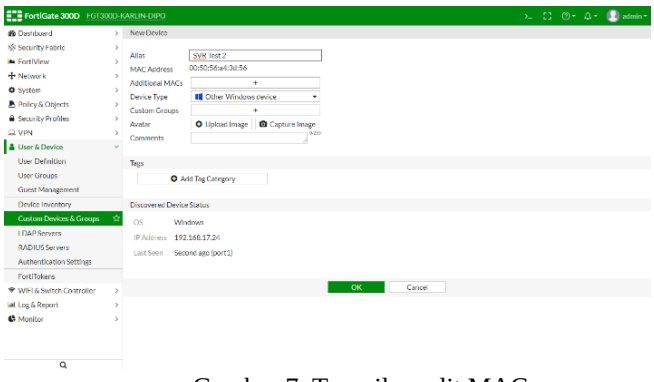
a. User & Device

Di dalam Fortigate perangkat yang terhubung pada jaringan semua ada di Device Inventory. Device tersebut didaftarkan berdasarkan MAC Address dan dimasukan ke grup yang telah ditentukan. Di dalam pembatasan dengan Fortigate akan digunakan taktik firewall yang sama yaitu “Ijinkan beberapa, dan Blok semua”. Jadi tidak semua device didaftarkan ke dalam Fortigate. Hanya device tertentu yang hanya memiliki kepentingan yang didaftarkan. Selain yang berkepentingan akan masuk ke akses default.

b. Device Inventory

Penulis sudah membuat contoh 2 server sistem operasi windows Virtual untuk didaftarkan ke dalam Fortigate, langkah-langkahnya adalah sebagai berikut.

1. Buka web admin Fortigate
2. Masuk ke menu User & Device > Device Inventory pada gambar 3.3 > Klik kolom Search dan masukan kedua MAC Address server yang inginkan



Gambar 7. Tampilan edit MAC Address kedua yang ingin didaftarkan

Selanjutnya klik Edit untuk didaftarkan dan masukan nama server masing-masing yang diinginkan di kolom Alias. Penulis memasukan nama SVR Test 1 dan SVR Test 2 pada gambar 6 dan gambar 7.

c. Custom Device & Group

Setiap device yang sudah didaftarkan selanjutnya akan dikelompokkan ke dalam sebuah Group.

Group ini akan berfungsi sebagai group akses. Penulis akan membuat masing-masing 2 contoh group akses untuk dikelompokkan kedua server virtual berdasarkan kategori website yang sering dipakai untuk pekerjaan. Jenis-jenis group aksesnya adalah sebagai berikut.

1. Group yang di Block
2. Group yang di Open

Untuk membuat group akses bisa Klik menu Custom Device & Group > klik Create New Device Group, Selanjutnya masukan nama group akses Group yang di Block, lalu klik tambah pada kolom Members dan pilih device SVR Test 1 atau pilih device yang lainnya untuk dibatasi aksesnya. Device yang ada di group ini akan dibatasi hak akses jaringannya.

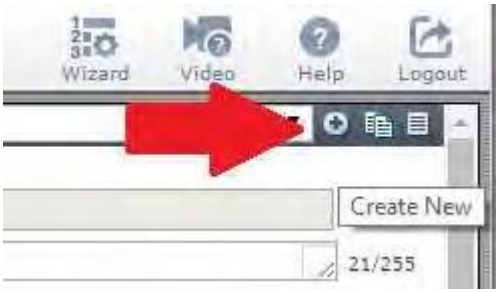
Selanjutnya masukan nama group akses Group yang di Open, lalu klik tambah pada kolom Members dan pilih device SVR Test 2. Device yang ada di group ini akan disetting bebas akses.

d. Web Filter

Web filtering merupakan saringan konten website yang digunakan oleh perorangan, kelompok, maupun organisasi untuk melakukan penyaringan terhadap situs-situs yang tidak diperbolehkan oleh pihak berwenang maupun yang tidak berhubungan dengan tujuan bisnis atau organisasi agar tidak dapat diakses(Ramadhan & Herdianto, 2020) .Secara default web filtering yang ada pada Fortigate masih mengijinkan semua website untuk diakses. Web Filtering ditambah dengan fitur Application Control yang berfungsi untuk mengantisipasi karyawan yang menggunakan teknologi VPN. Kategori-kategori yang ada pada database Fortigate ditunjukan pada Gambar 3.5. Di dalam menu Web Filtering dapat dibuat beberapa profile. Maka akan disetting profil Web Filtering sesuai kebijakan Manager IT PT. Karlin Mastrindo.

Langkah-langkah untuk membuat profil Web Filtering adalah sebagai berikut.

Masuk menu Security Profile > Web Filter kemudian tambahkan profil baru dengan menekan tombol + yang ada di pojok kanan atas seperti pada



Berikut kategori-kategori website yang di block karena tidak sesuai dengan tugas pekerjaan karyawan PT. Karlin Mastrindo :

a. File Shatring & Storage
b. Internet Radio & TV
c. Internet Telephony

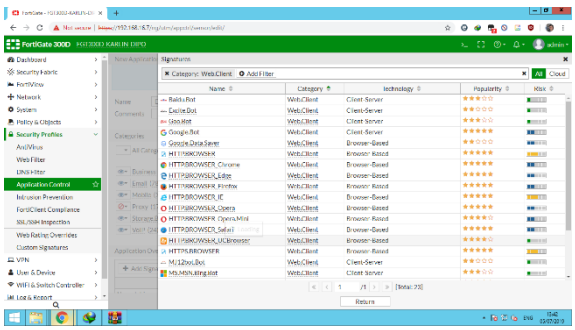
e . DNS Filter

Pada menu DNS Filter untuk melakukan pemblokiran, cara yang paling mudah adalah dengan menggunakan DNS filtering fortigate yang cara kerjanya me-redirect request DNS dari pengguna ke halaman web tertentu yang berisi peringatan bahwa situs yang berusaha diakses telah diblokir (Series & Science, 2020).

Selanjutnya masuk ke menu DNS Filter dan perlu untuk di konfigurasi dengan kategori website yang sama pada saat konfigurasi di menu Web Filter, terlihat hanya beberapa kategori website yang diberi akses, selain itu di block seperti pada Gambar III.25.

f. Application Control

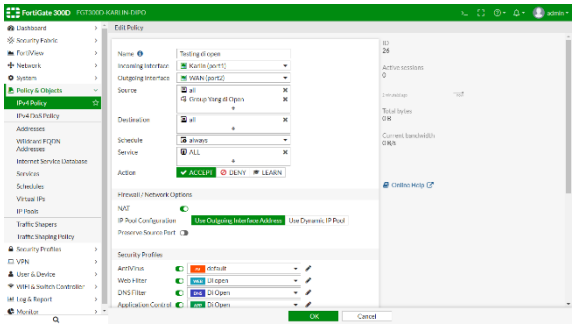
Pada menu Application Control Fortigate penulis akan membatasi akses jaringan kepada karyawan atau client yang menggunakan akses dari aplikasi-aplikasi yang terdapat pada smartphone atau komputer.



g. IPV4 Policy

Selanjutnya pada menu IPV4 Policy, seperti terlihat dalam gambar III.32 ini, saatnya penulis melakukan konfigurasi atau membuat kebijakan (policy) akhir dengan nama Testing Block untuk mengatur akses jaringan kepada komputer client(Lottin, Marcel, Study, & Camtel, 2020)

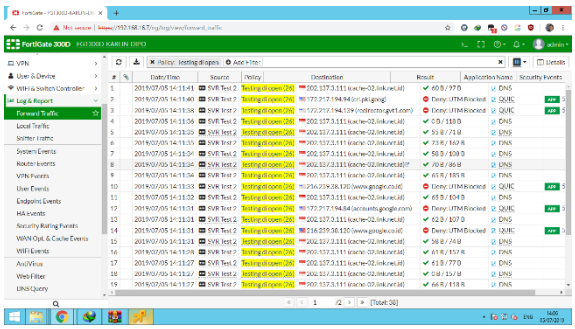
(karyawan) agar dibatasi aksesnya.



h. Forward Traffic

Pada menu Forward Traffic penulis dapat melihat lalu lintas jaringan client (karyawan) atau mengetahui akses website yang dikunjungi oleh karyawan.

1. Berikut Forward Traffic pada SVR Test 1 (akses diblock) :



KESIMPULAN

Setelah mempelajari dan menganalisa sistem jaringan maka penulis dapat menyimpulkan bahwa jaringan komputer yang berada di PT. Karlin Mastrindo sebagai berikut Sistem jaringan komputer LAN yang terdiri dari router Fortigate FG300D dan menggunakan 2 buah switch, yaitu switch 48 Port Cisco Catalyst 2960 dan switch 24 Port D-Link 1024A yang berada di PT. Karlin Mastrindo dan dapat mentransfer data 50 Mbps dan menggunakan server Lenovo System x3650 M5 untuk melakukan hubungan dengan jaringan luas seperti internet. Pada sistem jaringan kabel sudah di bangun ruang kabel (wiring closet) sebagai pusat untuk mempermudah dalam hal pendistribusian kabel penghubung dan untuk mempermudah dalam hal melacak kesalahan dalam jaringan. Jaringan komputer LAN yang terinstal pada ruang data centre dan staff karyawan PT. Karlin Mastrindo ini telah mewujudkan kebutuhan jaringan LAN yang saling terkoneksi pada suatu gedung untuk memenuhi kebutuhan fasilitas infrastruktur komunikasi guna mengatasi kebutuhan akan cara penanganan yang terkoordinasi. Terdapat ketidak disiplinan karyawan dalam bekerja di PT. Karlin Mastrindo, karena kebebasan akses jaringan atau website yang dapat mengurangi efektifitas kinerja perusahaan dan kurang adanya Hotspot/Wifi, sehingga akses internet belum sepenuhnya berjalan dengan baik.

REFERENSI

Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (2020). *Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis*. *8*(1), 128–139.

Faizan, M., Hegde, S. S., & Yaligar, N. V. (2019). *Comparison between Cisco ASA and Fortinet FortiGate Comparison between Cisco ASA and Fortinet FortiGate*. (May). https://doi.org/10.9790/0661-2103033436

Farly, K. A., Najoan, X. B. N., & Lumenta, A. S. M. (2017). *Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi*. *11*(1).

Ipsec, J. V. B. (2021). *Swadharma (jeis)*. *01*.

Lottin, M., Marcel, C., Study, A. C., & Camtel, T. (2020). *Integration of a Voice Over Internet Protocol (VoIP) Solution with Internet Protocol Version 6 Data Network to Increase Employee Productivity Integration of a Voice Over Internet Protocol (VoIP) Solution with Internet Protocol Version 6 (IPv6) in an Internet Protocol Version 4 (IPv4) Data Network to Increase Employee Productivity*. *6*.

Of, O., & Xx, N. (2011). *Interactive Website Filter for Safe Web Browsing*. 1–18.

Ramadhan, A. N., & Herdianto, D. (2020). *Securing Web-Based E-Voting System Using Captcha and SQL Injection Filter*. *14*(3), 277–286.

Series, I. O. P. C., & Science, M. (2020). *DNS tunneling Detection Using Elasticsearch DNS tunneling Detection Using Elasticsearch*. https://doi.org/10.1088/1757-899X/722/1/012064

Sistem, R., Agustina, W., & Rifqi, M. (2021). *JURNAL RESTI Implementasi Dual Link IPVPN dan GSM Berbasis IPSec pada Fortigate*. *1*(10), 228–236.

Supriyanto, B. (2019). Perancangan Jaringan VPN Menggunakan Metode Point To Point Tunneling Protocol. *Jurnal Teknik Komputer AMIK BSI*, *V*(2). https://doi.org/10.31294/jtk.v4i2