Perancangan Skema Sistem Keamanan Jaringan *Web Server* menggunakan *Web Application Firewall* dan *Fortigate* untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19

Gregorius Hendita Artha Kusuma
Teknik Informatika Universitas Pancasila
gregorius@univpancasila.ac.id

***Abstract*—Masa pandemi covid-19 menuntut kita untuk bisa beradaptasi dengan dunia digital. Sehingga, hal yang paling sering digunakan yaitu mengakses internet dan berkirim pesan melalui media sosial. Dengan seiring waktu, sebuah *website* pun akan muncul kerentanan sehingga bukan tidak mungkin ada penjahat yang menggunakan keahliannya untuk melakukan kejahatan pada *website-website* yang ada. Hal inilah yang harus diperhatikan secara bersama sehingga diperoleh perancangan skema sistem kemanan jaringan *web server* menggunakan *web application firewall* dan *fortigate* untuk mencegah kebocoran data khususnya di masa pandemi covid-19**

Kata kunci*—*perancangan sistem; firewall; web server; kebocoran data; pandemi.

I. PENDAHULUAN

Pada zaman yang semakin berkembang ini, kemajuan teknologi dinilai sangat meningkat drastis. Semua hal banyak beralih ke layanan internet. Mulai dari hal kecil seperti menonton hiburan, membaca berita, hingga memesan makanan menggunakan aplikasi *online*. Internet mengubah segala aspek kehidupan kita menjadi lebih mudah. Segala pekerjaan yang ada bisa kita selesaikan lebih cepat dengan hadirnya internet contoh nya seperti pada masa pandemi covid-19.

Pandemi covid-19 menjadi masa ketika orang-orang mengubah segala aktivitasnya menjadi serba *online*. Masyarakat tidak diperkenankan keluar rumah untuk menurunkan kasus penularan *virus*. Dampaknya yaitu masyarakat menjadi lebih sering membuka website dan segala hal *online* lainnya. Lalu lintas tiap *website* pun menjadi naik karena pada saat pandemi orang menjadi sulit jika harus beraktivitas keluar rumah. Dengan meningkatnya lalu lintas tersebut, tiap *website* yang ada pun tentu harus memiliki keamanan yang tinggi untuk menjaga data-data tetap aman dari segala kejahatan di dunia maya.

Tiap *website* pasti memiliki data-data yang biasanya tertanam pada *Web Server* agar para pengunjung dari seluruh dunia bisa mengakses *website* tersebut. Jika keamanan dari suatu *website* tidak bagus maka bukan hal yang sulit bagi para penjahat bisa mendapatkan data-data dari *website* tersebut.

Oleh karena itu, perlu adanya pengamanan yang terbaik untuk mencegah hal itu terjadi. Salah satunya yaitu dengan memanfaatkan teknologi *firewall* untuk bisa mem-*filter* lalu lintas pengunjung yang mengakses dan request yang dikirim kepada *Web Server* yang ada.

A. Tujuan

Tujuan dari penelitian ini yaitu untuk memperlihatkan rancangan yang bisa menjadi alternatif dalam menjaga keamanan *web server* dengan menggunakan *web application firewall* dan *fortigate* dalam kasus kebocoran data di masa pandemi covid-19

B. Batasan Masalah

Penelitian ini membatasi masalah yang dibahas agar pembahasan tidak keluar dari materi penelitian ini. Batasan masalahnya:

1) *Pengertian Web Server*
2) *Pengertian Apache*
3) *Pengertian Firewall*
4) *Pengertian Web Application Firewall*
5) *Pengertian Fortigate*
6) *Skema Perancangan Web Server berdasarkan contoh kasus yang ada*

II. LANDASAN TEORI

A. Web Server

Web server adalah sebuah *software* yang memberikan layanan berbasis data dengan menggunakan protokol HTTP atau HTTPS dari *client* menggunkan aplikasi *web browser* untuk *request* data dan *server* akan mengirim data dalam bentuk halaman *web* dan pada umumnya berbentuk dokumen HTML. Halaman *web* yang diminta bisa terdiri dari berkas teks, video, gambar, file dan banyak lagi [1].

Salah satu *web server* yang bersifat *open source* ialah apache yang digunakan untuk melayani dan melakukan pengaturan fasilitas web, pada umumnya memiliki fungsi untuk memperoleh berkas berisi permintaan (*request*) dari *client* melalui web *browser*, kemudian apache akan memproses data tersebut dengan menghasilkan keluaran (*output*) yang diinginkan oleh *client*. *Output* didapatkan berdasarkan data yang tersimpan dalam database *website* tersebut [2].

B. Apache

Apache adalah sebuah nama *web server* yang bertanggung jawab pada *request-response* HTTP dan *logging* informasi secara detail (kegunaan dasarnya). Selain itu, Apache juga diartikan sebagai suatu *web web server* yang kompak, modular, mengikuti standar protokol HTTP, dan tentu saja sangat digemari. Kesimpulan ini bisa didapatkan dari jumlah pengguna yang jauh melebihi para pesaingnya. Sesuai hasil survei yang dilakukan oleh Netcraft, bulan Januari 2005 saja jumlahnya tidak kurang dari 68% pangsa *web server* yang berjalan di Internet. Ini berarti jika semua *web server* selain Apache digabung, masih belum bisa mengalahkan jumlah Apache [3].

C. Firewall

1) Pengertian

Firewall adalah salah satu sistem pengaman jaringan untuk melindungi data dari pengguna yang tidak memiliki hak akses terhadap data tersebut. *Firewall* berperan sebagai filter antara komputer internal dan eksternal [5]. Selain itu, *firewall* juga berfungsi mengatur dan mengontrol lalu lintas data yang diijinkan untuk mengakses jaringan *privat*. *Firewall* melakukan kontrol berdasarkan alamat IP dari sumber, port TCP/UDP sumber dan tujuan, alamat IP tujuan, serta informasi dari header yang disimpan dalam paket data. Manfaat *Firewall* sebagai filter dapat digunakan untuk mencegah trafik yang mengalir ke suatu *subnet* jaringan untuk mencegah pengguna berbagi file rahasia. [4]

2) Jenis-jenis Firewall

a) Firewall berbasis hardware

Firewall berbasis *hardware* adalah perangkat keras yang terdapat dalam sistem jaringan, misalnya *router*. *Firewall* macam ini memerlukan konfigurasi untuk dapat bekerja secara efektif. Untuk dapat bekerja, *firewall* menggunakan teknik filter untuk menentukan *packet* utama, sumber, dan tujuannya. Secara internal sistem akan membandingkan data menurut aturan yang ditetapkan. Kemudian, ia memutuskan data mana yang perlu di-*drop* atau diteruskan ke tujuan.

b) Firewall berbasis software

Firewall berbasis *software* merupakan *firewall* yang biasanya diciptakan dalam bentuk aplikasi terpisah maupun sebagai fitur tambahan dari anti virus. Jenis *firewall* macam ini melindungi trafik *inbound* dan juga *outbound*, selain itu juga menghindarkan dari *virus* Trojan serta Worm.

3) Fungsi Firewall

a) Melindungi Data dari Hacker dan Pengguna Tidak Terotorisasi

Firewall berfungsi layaknya sekat antara data internal dengan akses luar. Karena *firewall*, *hacker* dan pengguna asing tidak bisa mengakses data yang dimiliki pengguna. Dengan kata lain, data akan rawan dicuri ketika komputer tidak terinstal *firewall*.

b) Block Konten dan Pesan yang Tak Diinginkan

Firewall dapat digunakan untuk memblok *website* atau konten dari alamat yang spesifik. Pengguna dapat mengatur secara manual konten-konten macam apa yang tidak diperbolehkan untuk diakses melalui komputer.

c) Monitor Bandwidth

Firewall juga dapat digunakan untuk memonitor dan membatasi *bandwidth* yang digunakan. Contohnya, pengguna bisa menetapkan batasan untuk konten hiburan, gambar, dan musik. Kemudian memprioritaskan *bandwidth* untuk konten-konten yang lebih penting.

d) Mengakses Layanan VPN

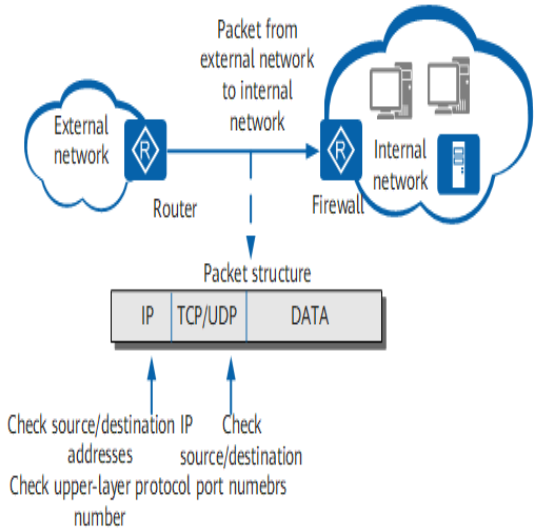
Firewall juga dapat dipakai untuk memfasilitasi koneksi *Virtual Private Network* atau VPN. Lewat layanan ini, pengguna dapat mengakses jaringan internal pengguna. Dengan layanan yang sama, pengguna bisa mengakses konten atau *website* yang sedianya diblokir oleh pihak tertentu. Hal ini tentunya bisa meningkatkan produktivitas, kolaborasi, dan data *sharing*.

4) Cara Kerja Firewall

Di dalam *firewall* sendiri dibagi lagi menjadi tiga metode untuk dapat mengontrol lalu lintas data yang masuk dan keluar dari jaringan, diantaranya adalah sebagai berikut.

a) Pernyaringan Paket atau Filtering

Pada metode menggunakan paket potongan kecil data yang nantinya dianalisis terhadap sebauh satu set filter (gambar 1). Ketika sebuah packet dianggap berbahaya maka ia takkan diijinkan masuk. Sebaliknya, ketika *packet* dianggap aman maka dia akan diteruskan ke sistem yang meminta.

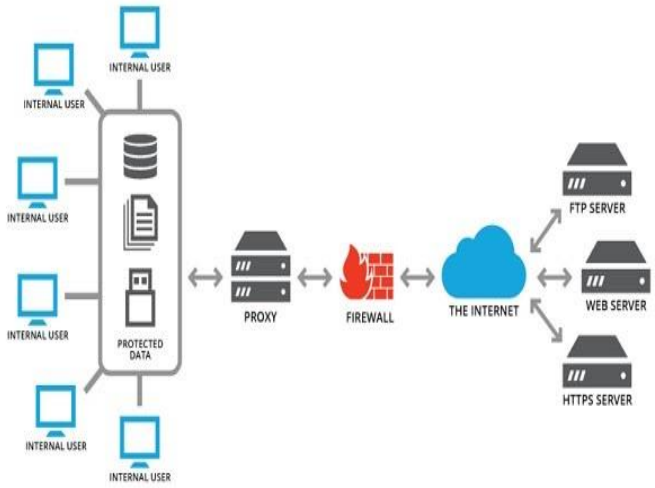


Gambar 1. Penyaringan Paket

b) Proxy Service

Ini merupakan aplikasi yang bekerja sebagai penghubung antara sistem jaringan. Aplikasi *proxy* berada di dalam *firewall* dan bertugas untuk memeriksa *packet* yang saling ditukarkan dalam jaringan. Sistem ini bisa dikatakan lebih efektif. Sebab, semua informasi yang diperiksa secara tersentralisasi (gambar 2). Cara kerja macam ini bisa dikatakan lebih canggih karena *proxy service* berusaha menciptakan hubungan antarjaringan

yang mirip. *Proxy* seolah menghubungkan jaringan secara langsung, padahal ia hanya berusaha meng-*copy* mekanisme yang mirip.



Gambar 2. *Proxy Service*

c) Inspeksi Stateful

Sistem ini menelusuri *packet* yang diterima dengan aktivitas-aktivitas sebelumnya. *Packet* yang diterima kemudian diperiksa dalam database *packet*. Jika paket berkonotasi positif atau tidak menunjukkan risiko bahaya, maka ia akan diteruskan ke sistem yang meminta (gambar 3).

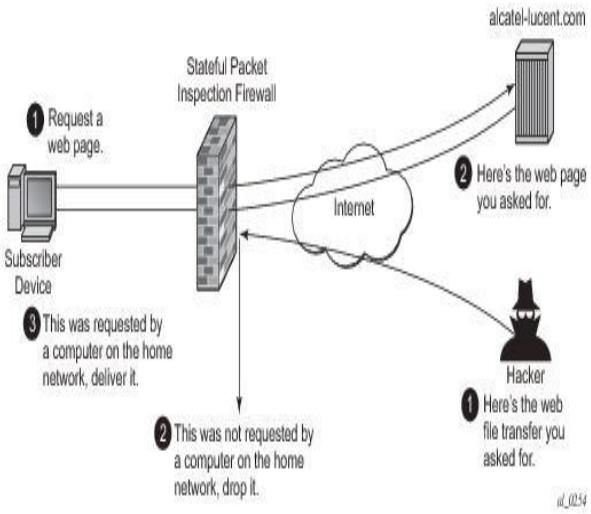
Ketika *firewall* selesai memeriksa packet, ia kemudian akan merespons dengan salah satu dari tiga cara. Pertama, *accept* atau terima. Artinya, *firewall* akan memperbolehkan trafik untuk melewati jaringan. Kedua, *reject* atau tolak. Ini berarti *firewall* menolak trafik untuk lewat dan membalasnya dengan tampilan "*unreachable error*". Terakhir, *drop* atau lewati di mana *firewall* menolak trafik tanpa mengirimkan pesan.

D. Web Application Firewall

Menurut *Web Application Security Consortium* (WASC) *Web application firewall* (WAF) diartikan sebagai sebuah perangkat perantara, yang berada antara *web client* dan *web server*, menganalisis pesan pada OSI Layer 7 ketika terjadi pelanggaran dalam kebijakan keamanan yang telah ditentukan. *Firewall* merupakan sebuah perangkat perantara, yang berada antara *web client* dan *web server*, menganalisis pesan pada OSI Layer-7 ketika terjadi pelanggaran dalam kebijakan keamanan yang telah ditentukan [6].

E. Mod Security

Mod Security adalah *Web Application Firewall* yang bersifat *open source* yang merupakan modul tambahan pada Apache. Beberapa fitur *mod_security* adalah pemeriksaan *log*, akses ke setiap bagian dari *request* yang ditujukan ke *server* (termasuk isi *request* atau *body*) dan memberikan respon terhadap hasil pemeriksaan, memiliki rule yang berdasarkan aturan *regular expression* yang fleksibel, pemeriksaan berkas yang diunggah, *validasi real-time* dan juga perlindungan *buffer-overflow*.



Gambar 3. Inspeksi Stateful

F. Fortigate

Fortigate adalah sebuah sistem keamanan yang dikeluarkan oleh perusahaan Fortinet. Fortinet merupakan perusahaan, penyedia layanan, dan badan pemerintah di seluruh dunia, termasuk mayoritas dari perusahaan Fortune Global 100 tahun 2009. Fortinet merupakan pemimpin pasar untuk *unified threat management* (UTM)(*Documentation*, 2014). *Fortigate* sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai *gateway* dan *router* bagi jaringan LAN sehingga tak dibutuhkan lagi *router* ataupun perangkat tambahan *load balancing* bila ada lebih dari satu koneksi WAN [7].

Fasilitas utama dari *Fortigate* adalah mencegah serangan DDOS atau *Distributed Denial of Service Attacks* yang dilakukan *hacker* untuk menembus sistem keamanan komputer dan mencuri data internal [8]. Selain itu *Fortigate* juga menyediakan layanan yang dapat disesuaikan dengan kebutuhan pengguna seperti :

1) *Layanan jaringan switching dan routing, baik statis ataupun dinamis.*
2) *Layanan keamanan jaringan, seperti Firewall, koneksi VPN yang aman dan juga untuk keamanan endpoint.*
3) *Layanan keamanan aplikasi, yakni dapat mengontrol spam dan virus, penyaringan konten web, dan juga mencegah terjadinya kebocoran data serta kontrol penuh aplikasi. Fitur ini dapat dinonaktifkan jika tidak diperlukan.*

G. Pandemi Covid-19

Pandemi COVID-19 adalah wabah yang terjadi secara serempak di mana-mana, meliputi daerah geografis yang luas. Pandemi merupakan penyakit menular (*epidemi*) yang menyebar hampir di seluruh negara atau benua dan biasanya mengenai banyak orang. Contoh penyakit yang menjadi pandemi adalah *Coronavirus Disease* 2019 (COVID-19) [9].

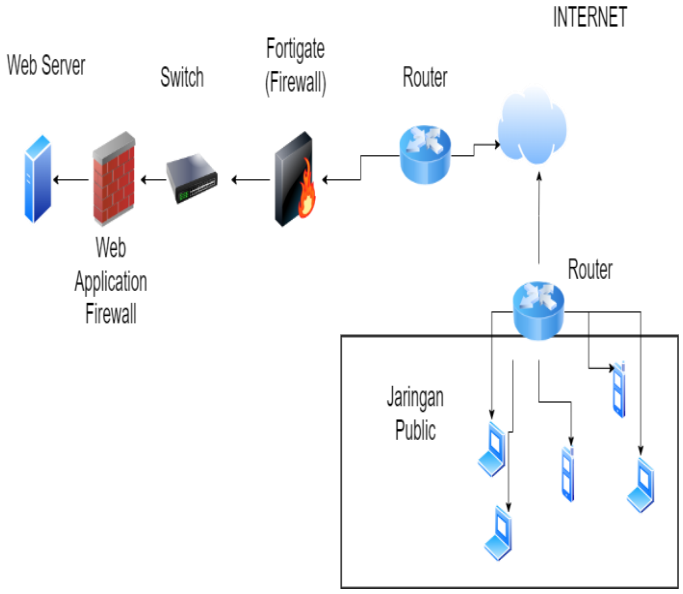
III. PEMBAHASAN

A. *Contoh Kasus*

Pada masa pandemi covid-19, internet menjadi hal yang sangat wajib dimiliki oleh semua orang. Internet menjadi keperluan sehari-hari mulai dari hal kecil seperti mencari hiburan sampai memesan makanan menggunakan aplikasi *online*. Kita menjadi tidak lepas dengan internet. Ketika membahas internet tidak lupa juga dengan data. Data yang ada pada suatu *website* tentu bisa diakses jika kita menggunakan internet tapi bukan berarti setiap data yang ada akan selalu aman. Sebuah *web server* bisa ditembus oleh penjahat dunia maya untuk mengambil data-data pribadi seseorang atau perusahaan untuk kembali dijual sehingga mereka bisa mendapatkan uang dari situ mengingat pandemi covid-19 ini membuat kebanyakan orang merugi. Kebocoran data sangat mungkin terjadi jika suatu *website* tidak aman.

B. *Solusi Penanganan*

Untuk menangani masalah kebocoran data bisa diterapkan alternatif dengan menggunakan skema seperti gambar di bawah ini.



Gambar 4. Skema Sistem *Web Server* dengan *Firewall*

Penjelasan untuk gambar 4, *Web Server* yang digunakan yaitu jenisnya Apache karena akan diterapkan modul *Mod Security* pada pada sisi *web server*nya. Lalu, *Web Server* dihubungkan dengan *switch* yang terhubung dengan alat *Fortigate* sebagai perlindungan ganda agar jika ada serangan tidak langsung masuk ke sisi *web server* nya. *Fortigate* disambungkan dengan *router* yang terhubung ke Internet. Lalu jaringan *public* pun bisa mengakses *Web Server* yang ada melalui internet.

Untuk metode yang dipakai bisa menggunakan Inspeksi *Stateful* dan Penyaringan Paket. Alasan dari pemilihan metode itu:

1) Cara kerja yang cukup efektif dengan pengecekan secara tersentralisasi untuk semua akses ke *web server*
2) *Request* yang masuk bisa lebih terpantau untuk meminimalisir kebocoran data

IV. KESIMPULAN

Dengan meningkatnya lalu lintas pengguna internet yang tinggi membuat suatu *website* perlu ditingkatkan keamanannya agar data yang ada tidak bisa bocor oleh tindakan pelaku kejahatan internet. Dari penjelasan yang sudah dijelaskan sebelumnya bisa disimpulkan bahwa penerapan modul *Mod Security* untuk *Web Server* Apache dan *Fortigate* bisa menjadi alternatif dalam menjaga keamanan *web server* dari kebocoran data khusus nya pada masa pandemi covid-19.

DAFTAR PUSTAKA

[1] Rahmatulloh, A., & Firmansyah, M. S. N. (2017). Implementasi load balancing web server menggunakan haproxy dan sinkronisasi file pada sistem informasi akademik Universitas Siliwangi. Jurnal Nasional Teknologi Dan Sistem Informasi, 3(2), 241-248.

[2] Syafitri, "Pengertian Apache Beserta Fungsi, kelebihan dan kekurangan Apache yang perlu Anda Ketahui," 2018. [Online] Tersedia di: https://www.nesabamedia.com/pengertian-apache/. [Diakses pada: 19 Januari 2022].

[3] Agusvianto, H. (2017). Sistem Informasi Inventori Gudang Untuk Mengontrol Persediaan Barang Pada Gudang Studi Kasus: PT. Alaisys Sidoarjo. JIEET (Journal of Information Engineering and Educational Technology), 1(1), 40-46.

[4] Agustini, S., & Mudzakir, A. (2019). Rancang Bangun Jaringan Komputer Dengan Bandwidth Management Menggunakan Teknik Brust Limit Dan Firewall Sebagai Pengaman Jaringan. Network Engineering Research Operation, 4(3), 189-195.

[5] Imas Indra. "Apa itu Firewall? ". 2021. [Online]. Tersedia di: https://www.niagahoster.co.id/blog/firewall-adalah/. [Diakses pada: 19 Januari 2022].

[6] Alfiani, I., Widjajarto, A., & Budiyono, A. (2021). Implementasi Dan Analisis Open Source Raptorwaf Pada Aplikasi Web Berdasarkan Standar Ptes. eProceedings of Engineering, 8(5).

[7] Darojat, A., & Nurhaida, I. (2019). Analisa Qos Administrative Distance Static Route Pada Failover Vpn Ipsec. J. Ilmu Tek. dan Komput, 3(1), 11.

[8] "Fungsi dan Cara Kerja dari FortiGate Firewall". [Online] Tersedia di: https://nds.id/fungsi-dan-cara-kerja-dari-fortigate-firewall/. [Diakses pada: 20 Januari 2022]

[9] Mutiasari, Kanya Anindita. "Pengertian Pandemi Covid-19, Statusnya di Indonesia Diperpanjang Jokowi". 2022. [Online] Tersedia di: https://news.detik.com/berita/d-5881903/pengertian-pandemi-covid-19-statusnya-di-indonesia-diperpanjang-jokowi. [Diakses pada: 19 Januari 2022].