Sistem Firewall untuk Pencegahan DDOS ATTACK di Masa Pandemi Covid-19

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

Abstrak— **Internet saat ini sudah hampir digunakan oleh hampir seluruh bumi ini, salah satu layanan yang sering digunakan yaitu website. Banyaknya pengguna yang mengakses suatu website, maka bisa ada kemungkinan terjadinya celah yang mungkin bisa dimanfaatkan oleh orang yang tidak bertanggung jawab. Contoh kasus yang mungkin terjadi yaitu DDoS Attack. Dengan demikian, penelitian ini membahas tentang perancangan skema sistem web server dengan menggunakan layanan yang disediakan oleh *Cloudflare* yaitu *Cloudflare* Magic Transit untuk pencegahan terjadinya penyerangan DDoS.**

Kata kunci—*ddosattack, firewall,pandemi, internet.*

1. PENDAHULUAN

Seiring perkembangan zaman khususnya ketika pandemi covid-19 melanda seluruh dunia, tidak bisa dipungkiri bahwa hampir di seluruh penjuru dunia menggunakan internet dan bahkan angka penggunanya meningkat pesat ketika pandemi covid-19 berlangsung, mulai dari anak-anak hingga bahkan yang lanjut usia masih ada yang mengakses internet. Banyak hal yang dapat dilakukan di Internet. Membaca berita dari seluruh penjuru dunia, menyaksikan pertandingan sepak bola antar negara, menonton video dari berbagai negara, hingga video call dari amerika hingga eropa dari eropa hingga asia dari asia hingga afrika dan keseluruh penjuru dunia lainnya. Semua aktivitas dilakukan melalui internet. Dari pagi hingga malam hari bahkan bisa dihitung 24 jam akses internet tetap dilakukan. Dengan banyaknya *request* dalam melayani pengguna apalagi jika *request* yang dilakukan secara bersamaan, jika web server tersebut tidak mampu menahan *request* tersebut maka ada kemungkinan bahwa web server tersebut akan *down*.Jika web server tersebut *down* maka sangat berbahaya, karena attacker akan bisa masuk ke dalam server apalagi jika server tersebut tidak memiliki firewall atau keamanan yang baik maka bisa ditembus dengan mudah. Salah satu solusi yang bisa diterapkan untuk masalah ini yaitu penambahan layanan pihak ketiga di bagian tengah antara *user* dan server, sehingga attacker tidak bisa langsung request ke server dan layanan pihak ketiga ini diharapkan juga mampu membantu melancarkan bahkan meningkatkan arus lalu lintas data pada web server.

A. Tujuan

Tujuan dari artikel ini dibuat adalah untuk merancang skema sistem web server dengan *Cloudflare* Magic Transit untuk pencegahan dari serangan DDoS di masa pandemi covid-19.

B. Batasan Masalah

Artikel ini membatasi masalah yang dibahas agar pembahasan tidak keluar dari materi artikel ini. Batasan masalahnya:

1) *Pengertian web server*
2) *Pengertian DDoS*
3) *Pengertian firewall*
4) *Pengertian Cloudflare magic transit*
5) *Skema sistem web server dengan Cloudflare Magic Transit*

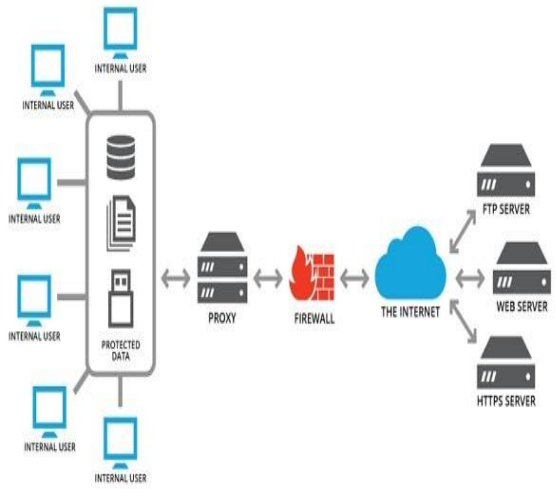
II. LANDASAN TEORI

A. Web Server

Web Server adalah suatu perangkat lunak (software) dalam *server* yang berfungsi untuk menerima permintaan (request) dari client atau browser berupa halaman website melalui protokol HTTP/HTTPS, lalu merespon permintaan tersebut dalam bentuk halaman website berupa dokumen HTML atau PHP[1].

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. 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 1. *Proxy Service*

C. DDoS

DDoS adalah suatu jenis serangan yang dilakukan oleh suatu attacker yang bertujuan untuk membanjiri lalu lintas jaringan supaya menghabiskan sumber daya yang dimiliki oleh suatu komputer atau server[2]. Beberapa jenis serangan DDoS yang paling umum muncul dan paling sering digunakan meliputi beberapa jenis seperti :

1) Banjir UDP

Banjir UDP, menurut definisi, adalah serangan DDoS yang membanjiri target dengan paket *User* Datagram Protocol (UDP). Tujuan serangan ini adalah untuk membanjiri port acak pada host jarak jauh. Hal ini menyebabkan host berulang kali memeriksa aplikasi yang mendengarkan di port tersebut, dan (jika tidak ada aplikasi yang ditemukan) membalas dengan paket ICMP 'Destination Unreachable'. Proses ini menghabiskan sumber daya host, yang pada akhirnya dapat menyebabkannya tidak dapat diakses.

2) Banjir ICMP (Ping)

Serupa pada prinsipnya dengan serangan banjir UDP, banjir ICMP membanjiri sumber daya target dengan paket Echo Request (ping) ICMP yang umumnya mengirim paket secepat mungkin tanpa menunggu balasan. Jenis serangan ini dapat menghabiskan bandwidth keluar dan masuk, karena server korban akan sering mencoba merespons dengan paket ICMP Echo Reply, mengakibatkan perlambatan sistem secara keseluruhan yang signifikan.

3) Banjir SYN

Serangan SYN flood DDoS mengeksploitasi kelemahan yang diketahui dalam urutan koneksi TCP ("3 way handshake"), di mana permintaan SYN untuk memulai koneksi TCP dengan host harus dijawab oleh respons SYN-ACK dari host tersebut, dan kemudian dikonfirmasi oleh respon ACK dari pemohon. Dalam skenario banjir SYN, pemohon mengirim beberapa permintaan SYN, tetapi tidak menanggapi respons SYN-ACK host, atau mengirim permintaan SYN dari alamat IP palsu. Bagaimanapun, sistem host terus menunggu pengakuan untuk setiap permintaan, mengikat sumber daya hingga tidak ada koneksi baru yang dapat dibuat, dan pada akhirnya mengakibatkan penolakan layanan.

4) Ping of Death

Serangan ping of deatch ("POD") melibatkan penyerang mengirim beberapa ping yang salah atau berbahaya ke komputer. Panjang paket maksimum dari sebuah paket IP (termasuk header) adalah 65.535 byte. Namun, Data Link Layer/Lapisan Data Link biasanya membatasi ukuran bingkai maksimum, misalnya 1500 byte melalui jaringan Ethernet. Dalam hal ini, paket IP yang besar dibagi menjadi beberapa paket IP (dikenal sebagai fragmen), dan host penerima memasang kembali fragmen IP tersebut ke dalam paket lengkap. Dalam skenario Ping of Death, setelah manipulasi konten fragmen yang berbahaya, penerima akan mendapatkan paket IP yang lebih besar dari 65.535 byte saat dipasang kembali. Ini dapat meluap buffer memori yang dialokasikan untuk paket, menyebabkan penolakan layanan untuk paket yang sah.

5) Slowloris

Slowloris adalah serangan yang sangat bertarget, memungkinkan satu server web untuk menjatuhkan server lain, tanpa mempengaruhi layanan atau port lain di jaringan target. Slowloris melakukan ini dengan menahan sebanyak mungkin koneksi ke server web target selama mungkin. Serangan ini menyelesaikan masalah dengan membuat koneksi ke server target, tetapi hanya mengirim sebagian permintaan. Slowloris terus-menerus mengirim lebih banyak header HTTP, tetapi tidak pernah menyelesaikan permintaan. Server yang ditargetkan membuat setiap koneksi palsu ini tetap terbuka. Ini akhirnya meluap karena kumpulan koneksi bersamaan maksimum, dan mengarah pada penolakan koneksi tambahan dari klien yang sah.

6) Amplifikasi NTP

Dalam serangan amplifikasi NTP, pelaku mengeksploitasi server Network Time Protocol (NTP) yang dapat diakses publik untuk membanjiri server yang ditargetkan dengan lalu lintas UDP. Serangan tersebut didefinisikan sebagai serangan amplifikasi karena rasio query-to-response dalam skenario tersebut berkisar antara 1:20 dan 1: 200 atau lebih. Ini berarti bahwa setiap penyerang yang mendapatkan daftar server NTP terbuka misalnya, dengan menggunakan alat seperti Metasploit atau data dari Proyek NTP Terbuka, dapat dengan mudah menghasilkan serangan DDoS dengan bandwidth tinggi dan volume tinggi yang menghancurkan.

7) Banjir HTTP

Dalam serangan HTTP flood DDoS, penyerang mengeksploitasi permintaan HTTP GET atau POST yang

tampaknya sah untuk menyerang server web atau aplikasi. Banjir HTTP tidak menggunakan paket yang salah format, spoofing atau teknik refleksi, dan membutuhkan lebih sedikit bandwidth daripada serangan lain untuk menjatuhkan situs atau server yang ditargetkan. Serangan tersebut paling efektif jika memaksa server atau aplikasi untuk mengalokasikan sumber daya semaksimal mungkin sebagai respons untuk setiap permintaan.

8) Serangan DDoS Zero-day

Definisi "Zero-day" mencakup semua serangan yang tidak diketahui atau baru, mengeksploitasi kerentanan yang belum ada patch yang dirilis. Istilah ini terkenal di kalangan anggota komunitas hacker, di mana praktik perdagangan kerentanan zero-day telah menjadi aktivitas yang populer.

D. Firewall

Firewall atau dinding api adalah sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk dapat melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Pada dasarnya sebuah firewall dipasang pada sebuah router yang berjalan pada gateway antara jaringan lokal dengan jaringan Internet. [3]

Firewall adalah sebuah sistem pengaman, jadi firewall bisa berupa apapun baik hardware maupun software. Firewall dapat digunakan untuk memfilter paket-paket dari luar dan dalam jaringan di mana ia berada. Jika pada kondisi normal semua orang dari luar jaringan anda dapat bermain-main ke komputer anda, dengan firewall semua itu dapat diatasi dengan mudah[4].

1) Jenis-jenis firewall

a) Firewall berbasis hardware

Firewall berbasis hardware adalah piranti 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 adalah solusi untuk perlindungan jaringan bagi pengguna internet di rumah. Biasanya firewall ini diciptakan dalam bentuk aplikasi terpisah maupun sebagai fitur tambahan dari anti virus. Jenis firewall macam ini melindungi trafik inbound dan juga outbound, selain juga menghindarkan dari virus Trojan serta Worm.

2) 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 diakses melalui computer.

c) Monitor *Bandwith*

Firewall tidak hanya bermanfaat untuk memastikan keamanan jaringan komputer terjaga. Di samping fungsi *firewall* yang utama, ia juga dapat digunakan untuk memonitor dan membatasi *bandwidth* yang digunakan. Sebagai contoh, pengguna bisa menetapkan batasan untuk konten hiburan, gambar, dan musik. Kemudian memprioritaskan bandwidth untuk konten-konten lebih penting untuk bisnis

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.

3) Cara Kerja Firewall

Firewall bekerja dengan menyaring data (packet) antara jaringan di internet. Ia bisa membolehkan atau tidak membolehkan suatu packet diakses oleh sebuah komputer.

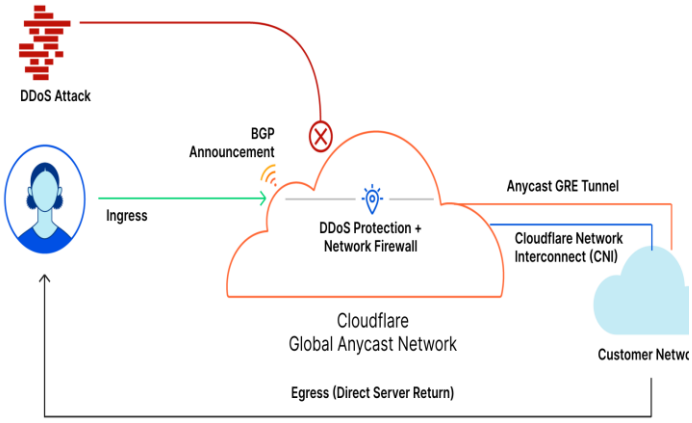
E. Cloudflare Magic Transit

Cloudflare Magic Transit adalah salah satu layanan yang disediakan oleh perusahaan Amerika Serikat bernama *Cloudflare* yang menyediakan jasa jaringan pengantaran konten, pencegahan DDoS, keamanan internet dan lainnya. *Cloudflare Magic* Transit ini adalah salah satu solusi keamanan jaringan yang memiliki berbagai macam fitur mulai dari proteksi dari penyerangan DDoS, akselerasi lalu lintas data, dan banyak lainnya.

Cloudflare Magic Transit dapat melindungi seluruh alamat IP subnets dari penyerangan DDoS sekaligus mempercepat lalu lintas jaringan. *Cloudflare* menjamin semua aset jaringan baik di tempat atau di lingkungan cloud yang dihosting pribadi atau public akan dilindungi.

Infrastruktur pada *Cloudflare Magic* Transit ini bisa dilihat pada gambar di bawah ini:

 E-ISSN : 2722-0346



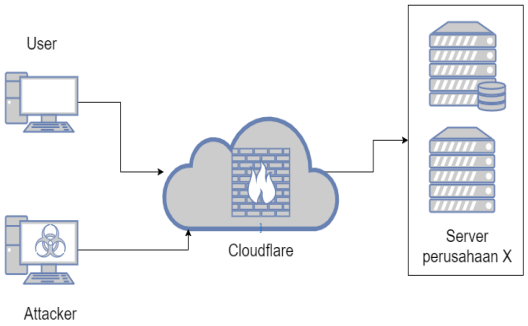
Gambar 2. Infrastruktur dari *Cloudflare* Magic Transit

III. PEMBAHASAN

Ada sebuah perusahaan yang bernama X, sebuah perusahaan yang melayani pelanggan di bidang jasa kalender janji temu. Perusahaan ini memiliki pelanggan hampir sekitar 5 juta pelanggan di seluruh dunia. Pada suatu saat perusahaan ini *down* akibat serangan DDoS dari orang-orang yang tidak dikenal, alhasil sebagian besar data berhasil bocor ke *dark web*, tempat dimana biasanya para hacker berkumpul atau yang jago di bidang IT, dan beberapa data yang bocor diantaranya identitas karyawan, profil pengguna, dan beberapa nomer kartu kredit.

Solusi

Kejadian yang dialami oleh perusahaan X di atas adalah salah satu dari banyaknya kejadian yang dialami oleh banyak perusahaan terutama perusahaan yang memberikan layanan melalui media internet. Salah satu cara yang bisa digunakan untuk menanggulangi masalah tersebut adalah dengan melakukan penambahan pertahanan di tengah antara *user* dan server, jadi *user* tidak langsung request ke server melainkan melalui *Cloudflare* terlebih dahulu. Berikut ini skema sederhana yang dimaksud:



Gambar 3. Skema Sederhana Solusi DDoS *Attack*

Cara sederhana dari skema tersebut adalah dengan menambahkan layanan dari *Cloudflare* di bagian tengah yaitu *Cloudflare* Magic Transit, jadi semua aktivitas request akan ditampung dan diolah oleh *Cloudflare*, bahkan jika ada attacker yang mencoba untuk mengacaukan lalu lintas data server perusahaan X, maka *Cloudflare* akan berusaha untuk menahan serangan itu tanpa membebani server perusahaan X tersebut. Magic Transit ini menggunakan jaringan global *Cloudflare* untuk mengurangi serangan dengan menggunakan protokol jaringan berbasis standar seperti BGP, GRE, dan IPsec untuk *routing* dan enkapsulasi.

IV. KESIMPULAN

Berdasarkan hasil di atas bisa disimpulkan bahwa saat ini masyarakat di seluruh penjuru dunia sudah mengakses internet, dan ketika pandemi covid-19 melanda angka pengguna internet meningkat pesat. Dengan meningkatnya pengguna internet tentu kemungkinan masalah yang akan dihadapi tentunya juga meningkat salah satunya yaitu penyerangan DDoS. Pengertian secara singkat tentang DDoS yaitu serangan yang dilakukan oleh suatu penyerang secara bersamaan untuk membanjiri lalu lintas jaringan supaya sumber daya yang dipunya habis. Salah satu yang bisa dilakukan untuk menanggulangi permasalahan ini yaitu dengan melakukan penambahan layanan dari pihak ketiga yaitu *Cloudflare* Magic Transit. *Cloudflare* Magic Transit ini berada di antara *user* dan server, jadi ketika ada seseorang yang ingin mengakses suatu website maka akan *request* ke *Cloudflare* terlebih dahulu jadi tidak langsung request ke web server perusahaan tersebut.

V.SARAN

Untuk meningkatkan keamanan dari serangan DDoS dapat ditambah dengan menggunakan hardware yang sudah tersertifikasi dan juga software yang berlisensi sehingga meminimalis penyerangan dalam sebuah website perusahaan. Selain itu juga digunakan enkripsi data dengan algortima kunci private sehingga data – data yang ada tidak bisa secara langsung dibuka oleh *user* pada umumnya. Kemudian juga ditambah dengan monitoring server yang secara otomatis sehingga secara *realtime* dapat secara langsung terlihat hasilnya.

DAFTAR PUSTAKA

[1] Arrafi, M. A. (2021). *Sistem Penyaring Situs Situs Terlarang Berbasis Mikrotik Dengan Fitur Firewall Pada Wlan (Studi Kasus Gedung Kuliah Vi Politeknik Negeri Sriwijaya)* (Doctoral dissertation, Politeknik Negeri Sriwijaya).
idcloudhost. 2020. "Mengenal Apa Itu Serangan dan Definisi Denial-of-service DDos Attack", https://idcloudhost.com/mengenal-apa-itu-serangan-dan-definisi-denial-of-service-ddos-attack/#Jenis_Umum_Serangan_DDoS_Attack, diakses pada 19 Januari 2022

[2] Aryadi, M. T., Trisnawan, P. H. & Siregar, R. A. (2019). Pendeteksian Serangan Black Hole terhadap Protokol Routing Ad Hoc OnDemand Distance Vector (AODV) pada Mobile Ad Hoc Network (MANET). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*. Vol. 3, No. 7

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

[4] Fasehan, B. (2021). *Rancang Bangun Sistem Keamanan Jaringan Komputer Menggunakan Firewall Filter Pada Laboratorium Jurusan Teknik Komputer* (Doctoral Dissertation, Politeknik Negeri Sriwijaya).

[5] Istiana, A. (2020). *Penerapan Intrusion Prevention System (Ips) Sebagai Pengamanan Dari Serangan Distributed Denial Of Service (Ddos)* (Doctoral dissertation, Institut Teknologi Telkom Purwokerto).

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

[7] 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].

[8]. Widhiyanto, A. C. (2019). *LKP: Rancang Bangun Web Server Berbasis Jaringan Cisco Catalyst Series 2960 di PT. Telekomunikasi Indonesia DIVRE V Jatim* (Doctoral dissertation, Universitas Dinamika).

[9] Wahyunanda Kusuma Pertiwi. [Online] from https://tekno.kompas.com/read/2021/08/31/10262687/data-13-juta-pengguna-aplikasi-e-hac-kemenkes-diduga-bocor (2021) [*Acessed* on 18 January 2022].