E-ISSN: 2715-2731

Implementasi *Firewall* Untuk Manajamen Hak Akses *Web Server* Berbasis *Application Gateway* Pada *Website* TNI

Muhamat Maariful Huda[1,*], Rizqi Darma Rusdiyan Yusron[2], Priska Choirina[3], Mochamad Luthfi Nazif Suryana[4]

[1,2] Program Studi Ilmu Komputer, Universitas Nahdlatul Ulama Blitar, Indonesia
[3] Program Studi Teknik Informatika, Universitas Islam Raden Rahmat, Indonesia
[4] Program Studi Telekomunikasi Militer, Politeknik Angkatan Darat, Indonesia

[1]hudha.maariful@unublitar.ac.id*; [2]rizqidarma@unublitar.ac.id; [3]priskachoirina@unira.ac.id; [4]luthfinazif@gmail.com
* corresponding author

INFO ARTIKEL

Sejarah Artikel
Diterima: 5 Agustus 2020
Direvisi: 10 Oktober 2020
Diterbitkan: 30 Desember 2020

Kata Kunci
Firewall
Application Gateway
Web Server
Penetration Testing

ABSTRAK

Selaras dengan perkembangan teknologi, keamanan menjadi isu yang sangat penting, khususnya di bidang jaringan yang terhubung dengan internet. Permasalahan yang ada saat ini adalah masih adanya *website* negara yang dikerjakan oleh pihak luar dalam hal sistem keamanan jaringan, dan yang paling banyak menjadi sasaran kejahatan adalah *web server*. Daripada mempercayakan sistem keamanan *web server* pada pihak lain, penulis mengaplikasikan penggunaan *application gateway* pada *firewall*. Berdasarkan hasil pengujian secara keseluruhan, *application gateway* memiliki kinerja yang lebih baik daripada jenis *firewall* lain di situs *web* lain, memiliki kemampuan yang lebih baik dalam menangani serangan DoS, karena *firewall* ini bekerja tidak hanya berdasarkan pada keamanan, tujuan dan atribut paket, tetapi dapat mencapai isi paket. Hal ini menyimpulkan bahwa aplikasi *gateway* sesuai dan aman digunakan pada *web server* TNI AD.

PENDAHULUAN

Cyber Security atau keamanan dunia maya adalah proteksi perlindungan dunia maya dari sumber–sumber bahaya. *Cyber security* berbeda dengan *security* atau keamanan biasa, karena ancaman *cyber* tidak bisa dimasukan begitu saja ke dalam kategori keamanan tradisional. Selain berasal dari dalam negeri atau *cyber threats* juga datang dari luar negeri. Namun, ancaman ini jarang mencapai taraf yang membutuhkan respon militer karena apapun yang dilakukan pemerintah dalam menanggapi ancaman *cyber* ini akan memiliki implikasi domestik dan internasional [1]. Pesatnya perkembangan teknologi informasi dan komunikasi ini merupakan tempat diletakkannya rahasia – rahasia penting negara. Selain itu teknologi informasi dan komunikasi memiliki berbagai macam pengaruh sebagai salah satu *cyber security* strategi negara besar dalam menghadapi ancaman perang *cyber* (*Cyber Warfare*) dikarenakan teknologi informasi dan komunikasi memiliki berbagai fungsi [2]. Dengan adanya kekhawatiran dunia terhadap ancaman *cyber warfare*, maka diperlukan penerapan keamanan *cyber* nasional yang baik untuk memberikan perlindungan terhadap informasi yang dimiliki satuan militer.

Firewall merupakan sistem keamanan untuk mengelola dan memantau *trafic* masuk dan keluar berdasarkan aturan keamanan yang sudah ditentukan [3]. *Firewall* berfungsi mencegah akses yang tidak diinginkan dari atau ke dalam jaringan atau *server*. *Application Gateway*.adalah *proxy firewall* yang menyediakan keamanan jaringan [4]. Orang kebanyakan mengira bahwa *firewall* adalah perangkat yang diinstall pada jaringan, dan mengontrol lalu lintas yang melewati segmen jaringan. Namun, kita dapat juga memiliki

firewall berbasis host yang dapat dijalankan pada sistem itu sendiri, seperti ICF (Internet Connection *Firewall*). Pada dasarnya, fungsi kedua *firewall* tersebut sama: untuk menghentikan intruksi dan menyediakan metode kebijakan kontrol akses kuat. Dalam definisi sederhana, *firewall* tidak lain adalah sistem yang melindungi komputer kita [5].

Application gateway atau dikenal dengan nama lain *proxy server* adalah *firewall* yang berfungsi untuk menyalurkan aplikasi [6]. Cara kerjanya adalah apabila ada pengguna menggunakan salah satu aplikasi seperti FTP untuk mengakses secara remote, maka *gateway* akan meminta client memasukkan alamat remote host yang akan dipakai. Saat Client mengirimkan userID serta informasi lainnya yang sesuai maka *gateway* akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan mengirimkan data diantara kedua titik [7]. Apabila data tersebut tidak sesuai maka *firewall* tidak akan meneruskan data tersebut dan menolaknya.

METODE

Pengujian implementasi *Firewall* untuk manajamen hak akses *web server* diperlukan sedikitnya ada 3 tahap yaitu tahap pengujian pada *Firewall* dengan metode *whitelist*, kemudian pengujian *scanning web server* dengan menggunakan OWASP ZAP dimana dalam pengujian ini adalah untuk mengetahui celah dan kerentanan terhadap dua *website* disini menguji *website* buatan sendiri dengan *website* dari buatan *platform* lain seperti *wordpress*, selanjutnya adalah pengujian *penetration testing* (*Pentesting*) dimana pengujian ini memberikan serangan langsung terhadap *web server* dengan metode serangan manual menggunakan metode SYN DDoS *Attack* dan SQL *Injection*. Selain ketiga test, dilakukan juga test kenierja *web server* setelah dilakukan *penetration testing*.

HASIL DAN PEMBAHASAN

Berikut adalah pembahasan dari 3 tahap yang sudah dilakukan:

Analisa hasil pengujian *Firewall* dengan metode *Whitelist*

```
lutfi@lutfi-MS-7817:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80                         ALLOW IN    192.168.88.99
[ 2] 80                         ALLOW IN    192.168.88.146
[ 3] 80                         ALLOW IN    192.168.88.97
[ 4] 80                         ALLOW IN    192.168.1.22
[ 5] 80                         ALLOW IN    192.168.1.27

lutfi@lutfi-MS-7817:~$
```

Gambar 1. Tampilan rule *firewall*

Pada Gambar 1 adalah pengaturan hak akses pada *firewall*, dimana hanya IP yang telah dimasukkan ke dalam database *whitelist* yang dapat mengakses *webserver*. Selain IP yang tersimpan dalam database tidak dapat mengakses *server*. Di point pengujian *Firewall* dengan metode *whitelist*, dimana *firewall* digunakan untuk memanajemen hak akses *server* dengan *whitelist*, perangkat manapun yang tidak terinput IP nya ke dalam *server* tidak dapat di izinkan masuk oleh *firewall*. Sesuai dengan pengujian yang telah dilaksanakan, *firewall* berhasil menolak akses perangkat yang tidak terinput ke dalam database. Sebaliknya setelah

IP di input masuk ke dalam database, *firewall* mengizinkan masuk dan mendapatkan akses ke dalam *webserver*

Analisa hasil pengujuan *Scanning web server* dengan OWASP ZAP

Dengan metode scanning *web* sudah membuktikan bahwa *website* dan *server* buatan sendiri tidak kalah hebat dengan *website* tniad.mil.id berikut adalah perbandingan dari *website* sendiri dan *website* tniad.mil.id

Tabel 1. Hasil *Scanning Web* TNI AD

Host	Alert Group	Severity	Alert Count
Server Website tniad.mil.id	Style-src unsafe-inline	Medium	4
	Cross Origin Resource Sharing (CORS) misconfiguration on the *web server*	Medium	2
	Absence of Anti-CSRF tokens	Low	4
	Content-Security-Policy	Low	4

Tabel 2. Hasil *Scanning Web* wordpress

Host	Alert Group	Severity	Alert Count
Server Website 192.168.1.28	Style-src unsafe-inline	Medium	4
	Cross Origin Resource Sharing (CORS) misconfiguration on the *web server*	Medium	2
	Absence of Anti-CSRF tokens	Low	3
	Content-Security-Policy	Low	4

Pada Tabel 1 dan Tabel 2 terlihat persamaan dalam beberapa kerentanan, yaitu Style-src unsafe-inline atau opsi inline yang tidak aman untuk digunakan saat memindahkan atau menulis ulang baris kode pada *website*, pada jenis kerentanan ini resiko yang dihasilkan adalah medium dengan peringatan 4. Kerentanan selanjutnya adalah 2) COSR Misconfiguration on *Web server*. COSR adalah mekanisme yang memungkinkan sumber daya terbatas di laman *web* diminta dari domain lain di luar domain tempat sumber daya pertama ada, resiko yang dihasilan juga sama pada kedua *website* yaitu medium dengan jumlah peringatan sebanyak 2. Kerentanan berikutnya ada pada Absence of Anti-CSRF Tokens, hal ini terjadi karena fungsionalitas aplikasi dalam menggunakan URL / formulir yang dapat diprediksi dengan cara yang dapat diulang. Sifat serangannya adalah mengeksploitasi keamanan yang dimiliki situs *web* kepada pengguna dengan tingkat kerentanan low. Kerentanan yang terakhir adalah Content Security Policya atau standar keamanan komputer yang diperkenalkan untuk mencegah skrip lintas situs, clickjacking, dan serangan injeksi kode lain yang dihasilkan dari eksekusi konten berbahaya dengan tingkat kerentanan low.

Analisa hasil pengujian dengan *penetration testing*

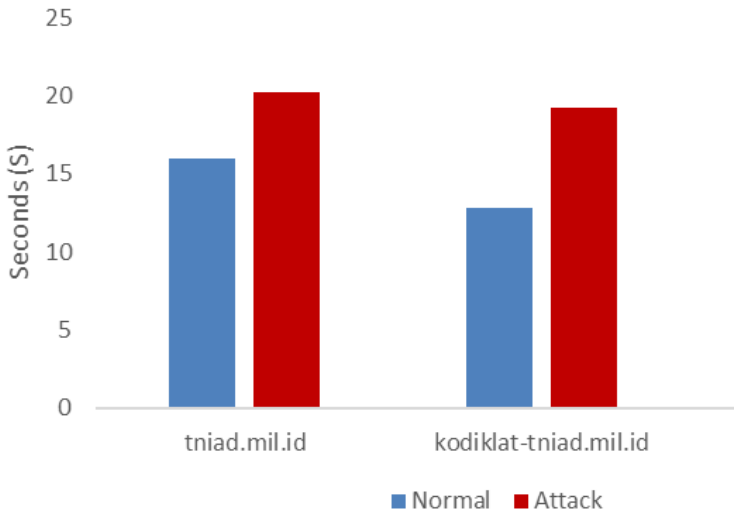
Pengujian manual menggunakan SYN Ddos Attack adalah dengan cara mengirimkan paket data berjumlah 3.000.000 dan hasilnya baik *website* tniad.mil.id tidak terpengaruh, pada *website wordpress* buatan sendiri juga tidak terpengaruh. Selanjutnya dengan menggunakan SQL injection, dengan diimplementasikannya *firewall* pada kedua *website* maka serangan SQL injection tidak terpengaruh, akan tetapi jika diujicobakan pada *website* dengan alamat

http://testphp.vulnweb.com maka akan dapat membuka database pada *web* tersebut. Pengujian selanjutnya adalah dengan menggunakan virus. Pengujian dengan menggunakan virus semua *website* berhasil masuk. Karena pada dasarnya *firewall* sendiri hanya memanajemen hak akses pada *web server* yang masuk dan yang keluar bukan memanajamen file yang masuk dan yang keluar, karena pada hakikatnya virus sendiri akan menyerang sistem dari *server* tersebut bukan pada *firewall* nya. Sebaliknya yang bertugas untuk mengisolasi dan mengkarantina virus hanyalah antivirus bukan *firewall*.

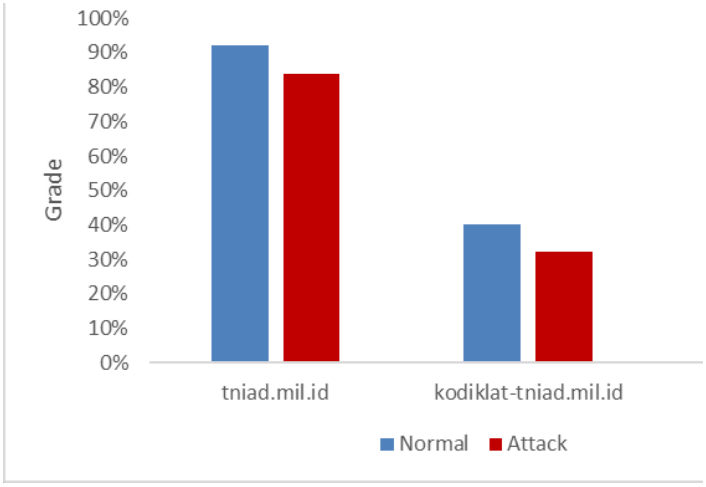
Tabel 3. Hasil pengujian menggunakan penetration testing.

	SYN DDoS Attack	SQL Injection	Virus Attack
Tniad.mil.id	Tidak mempengaruhi	Tidak dapat menjangkau *web server*	Mempengaruhi *web server*
192.168.1.28	Tidak mempengaruhi	Tidak dapat menjangkau *web server*	Mempengaruhi *web server*

Tes Kinerja



Gambar 1. Perbandingan *loading webserver* pada waktu normal dan pada waktu dilakukan penetration testing



Gambar 2. Perbandingan kecepatan *webserver* pada waktu normal dan pada waktu dilakukan penetration testing

Pada Gambar 1 dan 2, terdapat perbandingan waktu membuka *server* dan keceptan akses *server* pada waktu dilakukan serangan dan waktu tidak dilakukan serangan. Terlihat tidak terlalu jauh perbedaan diantara keduanya.

KESIMPULAN

Dalam penelitian ini diketahui bahwa metode *application gateway* untuk mengamankan *web server* tidak kalah dengan suatu sistem keamanan diluar perusahaan walaupun masih terdapat kekurangan, metode *application gateway* pada *website* tniad.mil.id sudah sedikit kerentanan dibandingkan situs buatan sendiri. dan juga pada tes kinerja, seperti yang kita lihat pada Gambar 1 dan 2 situs *web* Poltekad memiliki penurunan kinerja yang tidak cukup jauh antara pengujian normal dan tes serangan dibandingkan dengan dua besite lainnya. Kesimpulannya, penerapan poltekad *Website* merupakan aplikasi *gateway* dengan metode yang sesuai dan aman pada *web server* TNI AD.

REFERENSI

[1] Maheshwari R, Krishna C R and Brahma M S 2014 Defending network system against IP spoofing based distributed DoS attacks using DPHCF-RTT packet filtering technique Proc. 2014 Int.
[2] Maj S P, Makasiranondh W and Veal D 2010 An Evaluation of *Firewall* Configuration Methods IJCSNS Int. J. Comput. Sci. Netw. Secur. pp 1–7
[3] Azzam A T, Munadi R and Mayasari R 2019 Performance Analysis Of *Firewall* As Virtualized Network Function On VMware ESXi Hypervisor J. Infotel pp 11-29
[4] Gupta S and Gupta B B 2017 Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art Int. J. Syst. Assur. Eng. Manag. pp 512–30
[5] M. O'Leary, Cyber Operations: Building, Defending, and Attacking Modern Computer Networks. 2015.
[6] J. Scambray and S. McClure, Hacking Exposed: Windows. 2008.
[7] D. Gibson, Windows Seccurity Essential. 2011.