Literatur Review Analisis metode De-Militarized Zone (DMZ) dan *Switch Port security* Sebagai Metode Keamanan Jaringan

Ni Komang Ayu Sri Anggreni[1] , Lie Jasa[2]

***Abstract*— Over time, the development of technology is very rapid. It is certainly inseparable from the role of networks that can connect devices to be able to exchange information. Therefore, there is a need to secure *computer* networks to prevent cyber crime. The most commonly used attacks are *Port Scanning* and DoS (Denial Of Service). There are various ways to secure a *computer* network, one of which is by *Switch*ing *port security*. In addition to using *Switch port security*, the technique for securing network crimes is to use the De-Militarized Zone (DMZ). This study aims to compare network security performance with the Port security and DMZ methods where the tests obtained based on the review literature concluded that the use of the DMZ method carries out security by filtering requests by clients through firewall routers while Port security can provide security to the network by providing access to the server to registered ports only.**

***Key Words*—DMZ, LAN, Network Security, Port security, Switch**

***Intisari*— Seiring berjalannya waktu. perkembangan teknologi tumbuh dengan sangat pesat. . Hal itu tentu saja tidak terlepas dari peran jaringan yang dapat menghubungkan perangkat sarana untuk dapat bertukar informasi. Maka dari itu perlu adanya pengamanan jaringan *computer* untuk mencegah adanya *cyber crime*. Serangan yang paling sering digunakan adalah *Port Scanning* dan DoS (*Denial Of Service*). Terdapat berbagai cara untuk mengamankan jaringan *computer* salah satunya adalah dengan *Switch port security*. Selain dengan menggunakan *Switch port security*, teknik untuk mengamankan kejahatan jaringan adalah dengan menggunakan De-Militarized Zone (DMZ). Penelitian ini bertujuan untuk membandingkan kinerja keamanan jaringan dengan metode *Port security* dan DMZ dimana pengujian yang didapatkan berdasarkan literatur review didapatkan kesimpulan bahwa penggunaan metode DMZ melakukan pengamanan dengan menyaring *request* oleh *client* melalui *router firewall* sedangkan *Port security* dapat memberikan keamanan kepada jaringan dengan memberikan akses ke server terhadap *port* yang telah terdaftar saja.**

Kata Kunci*—DMZ, Keamanan Jaringan, LAN, *Port security, Switch

I. PENDAHULUAN

Seiring berjalannya waktu, perkembangan teknologi amat sangat pesat. Hal itu tentu saja tidak terlepas dari peran jaringan yang dapat menghubungkan perangkat sarana untuk dapat bertukar informasi. Dengan adanya jaringan *computer* memudahkan pengguna untuk mencari maupun bertukar informasi yang bersifat penting dan rahasia. Keamanan jaringan merupakan aspek terpenting sebuah sistem dalam menjaga validitas dan integritas data, serta menjamin ketersediaan layanan bagi penggunaanya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak [1]. Dalam hal ini diperlukan pengaturan jaringan *computer* yang baik guna memaksimalkan proses pertukaran informasi dan mengamankan dari pihak yang tidak bertanggung jawab seperti *hacker*.

Kebutuhan akan jaringan komputer semakin bertambah penting, baik dalam pendidikan, pekerjaan maupun dalam sebuah permainan, dengan banyaknya akses ke jaringan tersebut maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan ataupun adanya peretas yang dapat mematikan sumber daya pada server [21].Maka dari itu perlu adanya pengamanan jaringan *computer* untuk mencegah adanya *cyber crime*.

Port Scanning dan DoS (*Denial Of Service*) ialah serang yang kerap dipergunakan. *Port Scanning* adalah serangan dengan melakukan mekanisme pencarian *open port* dalam sebuah jaringan komputerisasi, setelah mendapatkan hasil, maka hasilnya tersebut digunakan untuk mendeteksi dimana letak lemahnya dari sistemisasi *computer*. DoS ialah serangan yang melakukan mekanisme pengiriman permintaan pada server dengan kontinu dengan tujuan agar sever dalam keadaan sibuk untuk memberikan tanggapan pada permintaan tersebut kemudian terjadi rusaknya server (*hang*) [1]

Terdapat berbagai cara untuk mengamankan jaringan *computer* salah satunya adalah dengan *Switch port security*. *Switch port security* adalah kemampuan perangkat *Switch* untuk mengamankan jaringan LAN (Local Area Network). Selain dengan menggunakan *switch port security*, teknik untuk mengamankan kejahatan jaringan adalah dengan menggunakan De-Militarized Zone (DMZ), yakni sebuah perlindungan pada system internal terhadap penyerangan *hacker* ataupun berbagai pihak yang mencoba masuk ke *system* namun tak memilik akses resmi. *Open port* adalah bagian yang membentuk DMZ, dimana bisa diketahui oleh pihak luar. Ini menyebabkan saat *hacker* melakukan penyerangan serta melaksanakan server *cracking* pada DMZ, menyebabkan *hacker* terbatas pada pengasesan pada *host*

[1]*Mahasiswa, Program Studi Pasca Sarjana Teknik Elektro Fakultas Teknik Universitas Udayana, Gedung Pascasarjana Jalan P.B. Sudirman Denpasar-Bali 80232 INDONESIA Phone: (0361) 261182 / (0361) 255345; Email: Pascasarjana@unud.ac.id*

[2,] *Dosen, Program Studi Pasca Sarjana Teknik Elektro Fakultas Teknik Universitas Udayana, Gedung Pascasarjana Jalan P.B. Sudirman Denpasar-Bali 80232 Phone: (0361) 261182 / (0361) 255345; Email: Pascasarjana@unud.ac.id*

p-ISSN:1693 – 2951; e-ISSN: 2503-2372

dalam DMZ serta tidak mampu menembus jaringan internal. Mekanisme ini juga dapat memotong jalan masuk di system internal, dimana menghalangi *viruses*, Trojan serta lainnya.[2]

II. TINJAUAN PUSTAKA

A. Jaringan Komputer

Jaringan komputer ialah koneksi dari banyak *computer* secara *Autonomous* yang menjalin keterhubungan melalui kabel ataupun tanpa kabel secara bersamaan. *Autonomous* ialah saat suatu *computer* gagal membuat pengaturan pada *computer* lainnya dengan penuh dalam perantara koneksi dan menyebabkan *computer* lain tersebut mati, mengalami *restart*, sampai melakukan akses pada dokumen yang kemudian melakukan pengerusakan pada sistem. Pada suatu jaringan itu, masing – masing *computer* beroperasi dengan *independent* pada proses mengatur dokumen mereka, salah satu contoh ialah internet dimana memberikan kemungkinan sebuah *computer* melakukan penerimaan dan pengiriman data, namun tak mampu mengendalikan *computer* lainnya dengan penuh [5]

Pengistilahan *client*-server yakni pendesainan jejaring yang dipergunakan dalam proses mengaplikasikan jejaring *computer*. *Client* ialah pihak yang melakukan permintaan atau yang melakukan penerimaan pada layanan, kemudian yang menyediakan ataupun yang melakukan pengiriman layanan ialah server [4]

B. Keamanan Jaringan Komputer

Ialah sebuah sistemasi yang dipergunakan dalam melindungi sebuah jaringan dari ragam ancaman dari luar yang dapat menyebabkan rusaknya jaringan serta mengantisipasi terjadinya data perusahaan dicuri [5][6]

Jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup semua jenis perangkat komputer (Komputer desktop, laptop, smartphone, PC, tablet) dan perangkat penghubung [11].

Selain itu, jaringan komputer adalah interkoneksi antara 2 komputer autonomous atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel *(wireless*). *Autonomous* adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh. Sehingga dapat membuat komputer lain. *Restart, shutdows,* kehilangan file atau kerusakan sistem. [20]

C. *Switch*

Switch ialah perangkat denan fungsi membuat koneksi dalam berbagai *computer*. Dari sisi bentuk fisik, *Switch* serupa hub namun *logical* memiliki kesamaan pada *brigde*. Kecerdasan yang meningkatkan dari hub, yakni mempunyai arti pada alamat MAC (*Medium Access Control*) ataupun dalam *link layer* model OSI dimana hanya melakukan pengiriman data ke *port* yang ditentukan (*unicast*). Mekanismenya yakni jika data *packet* tiba, dilakukan pengecekan pada *header* guna membuat penentuan terkait segmentasi tujuan dari paket data. Selanjutnya dilakukan pengiriman kembali data ke segmen yang dituju. Ada dua *Switch*, yakni:

- *Switch Unmanageable*

Switch memiliki funsgi dalam melakukan distribusi data paket pada *computer* yang disambungkan ke sebuah jaringan yang sama. Selain itu berfungsi melakukan pengenalan pada topologi jaringan dengan banyak *layer* dimana menyebabkan data menjadi cepat didistribusikan serta secara langsung sampai ke tujuannya. *Switch* melakukan kinerjanya dengan *plug-play*, dimana *Switch* langsung bekerja saat disambungkan ke sumber daya serta perangkat lain. *Switch* ini tak mampu melaksanakan konfigurasi pengaturan, yang mana mampu bekerja sebatas pengaturan *default* dari pabrik. Gambar 1 memperlihatkan *Switch unmanageable* [5]

Gambar 1. *Switch Unmanageable*

- *Switch manageable*:

Switch ini mempunyai kegunaan serupa *switch unmanageable* tetapi mempunyai atribut pelengkap serta bisa diterapkan konfigurasi pengaturan pada *user*. Contohnya atribut *Quality of Service*, yakni konfigurasi *bandwidth* dalam memberikan prioritas pada data. Selanjutnya ada atribut monitoring kinerja jaringan yakni *Simple Network Management Protocol* (SNMP). *Virtual Local Access Network* (VLAN) merupakan fitur yang sering dipergunakan. Selanjutnya *Switch* ini mampu lebih meningkatkan keamanan melalui pengaturan keamanan *port security*, yang dilakukan dengan pemeriksaan pada hak akses ke tiap perangkat yang sudah disambungkan. Gambar 2 memperlihatkan contoh *Switch manageable* .[5]

Gambar 2. *Switch Manageable*

D. *Port security*

Port ialah lokasi terdapatnya informasi keluar-masuk atas *computer* yang mana *port scanning* melakukan identifikasi pada *open gate* atas komputer. *Port* mempunyai mendapatkan akses resmi untuk pengelolaan jaringan, namun *scanning port* dapat membahayakan bila sebuah pihak melakukan pencarian *access point* yang lemah untuk digunakan sebagai jalur masuk ke *computer*.

Pada suatu jaringan *computer* pengamanan bisa dinaikkan dengan memanfaatkan kapabilitas suatu *Switch manageable* yakni memanfaatkan *port-port* yang ada. Ada tiga tipe *Switch port security* yakni:

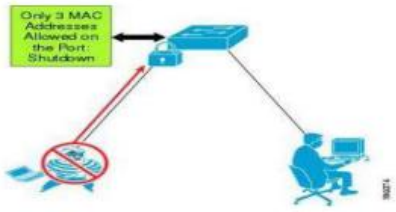
- *Default / static port security*

Saat *port security* diberfungsikan, *mac address port security* juga dibuat aktif pada *port Switch*, konfigurasi *mac address* dalam *port security* tersebut berguna sebagai sistem yang mengenali *mac address* dengan manual serta

alamat *mac* yang diatur diperbolehkan agar terhubungkan pada *port*, bila sumber alamat bukan alamat yang sudah ditentukan oleh *port*, maka tidak akan ada penerusan dari paket data

- *Port security dynamic learning*

Alamat MAC dipelajari dalam sistem dinamis ketika *computer* telah dihubungan pada *Switch* Selanjutnya Alamat MAC kemudian disimpan pada tabel Alamat MAC

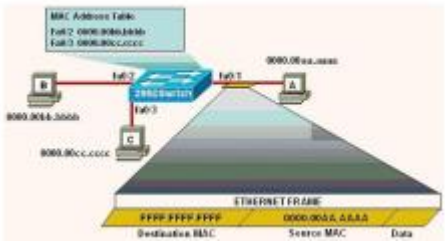


Gambar 3. MAC *Address*

Gambar 3 memperlihatkan media *switch* yang dipergunakan oleh user guna membagikan sumber daya tetapi *switch* memiliki kapabilitas dalam melakukan pengamanan pada jaringan,*switch* memperbolehkan tiga Alamat MAC saja untuk dihubungkan pada *port* selain itu tidak diberi izin akses.

- *Sticky port security*

Suatu *switch* dengan kapabilitas untuk melakukan pengenalan pada alamat *mac address* dari setiap komputer yang sudah dihubungan dimana kemudian melakukan *blocking* pada tiap *mac* yang melampaui *mac* terkonfigurasikan



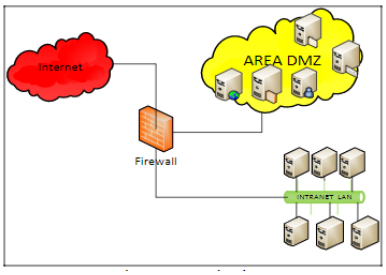
Gambar 4. *Sticky Port security*

Gambar 4 memperlihatkan *switch* yang akan melakukan pembacaan pada alamat *mac* atas setiap *computer* yang memiliki hubungan padanya, melalui pemanfaatan *sticky port security* selanjutnya bisa dibuat *list* jumlah pemakai *computer* yang memiliki hubungan dengan *switch*, contohnya: bila dalam daftar terdapat tiga *mac* maka saat timbul perangkat keempat secara langsung *sticky port security* melakukan pencegahan. Proses mengenali alamat *MAC* dilaksanakan dengan langsung, bila suatu *computer* sudah dihubungan ke *switch* kemudian dilakukan permintaan (ping) ke *computer* lainnya maka *computer* yang menerapkan penerimaan selanjutnya melakukan pengiriman alamat MAC ke *switch* yang dilalui, sehingga pembuatan daftar alamat *mac* tidak perlu diatur satu persatu [9]

E. De- Militarized Zone

Firewall DMZ (jaringan perimeter) ialah *security boundary* diantara seperangkan jaringan *private* LAN serta publik (internet). DMZ ialah suatu *host computer* dalam suatu zona netral pada perantara jaringan privat serta publik. DMZ melakukan penghalangan pada pengguna luar untuk melakukan akses ke suatu server yang memuat informasi dari perusahan (Gambar 5). Pengistilahan ini diambil dari zona penyangga korea utara serta selatan menanggapi aturan dari PBB di 1950.

Konsep DMZ menerapkan konsep NAT (*Network Address Translation*) yang memiliki fungsi dalam pengarahan *real address* ke dalam *internal address* serta PAT (*Port Address Translation*) yang memiliki fungsi melakukan pengarahan data yang memasuki *port* ataupun kumpulan *port* serta protokol.



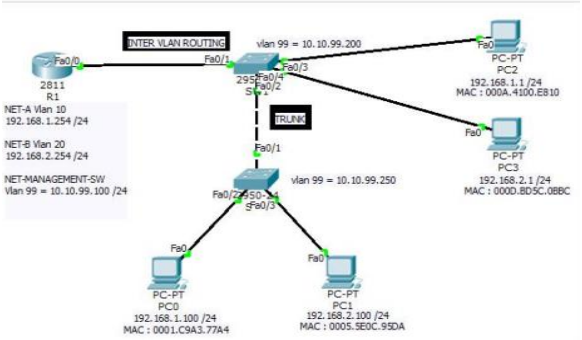
Gambar 5 Topologi DMZ

Gambar 5 ialah penggambaran dari skema lalulintas data di suatu DMZ dasar. Trafik ke DMZ dapat diberi izin ataupun mengalami penolakan. *Firewall* DMZ melakukan pengaturan penuh pada aliran data. Tiap layanan pada user dalam jaringan eksternal bisa diterapkan pada DMZ. Hal yang umum dari layanan ialah webserver, mail server, ftp server, VoIP server serta DNS server.

III. METODE PENELITIAN

Ada sejumlah metoda dalam penelitian mengenai keamanan jaringan LAN dengan metode *De-Militarised Zone* (DMZ) dan *Port security*. Berikut penjelasan pada penelitian-penelitian terkait mengenai metode algoritma yang digunakan.

Penelitian[8] melakukan riset pada pengaman jejaring dengan mendayagunakan *Switch port security* dengan topologi jaringan[8] sebagai berikut



Gambar 6. Topologi jaringan

Dengan topologi jaringan seperti pada gambar diatas, mendapatkan hasil di *Switch* S1 dimana dilaksanakan pengaturan *sticky port security* yang menyebabkan alamat MAC masuk dalam daftar otomatis saat proses ping usai

9 772503 237160

dilakukan, dalam kasus ini, alamat PC0 dipergunakan. *Switch* tersebut mendayagunakan *violation mode shutdown* dimana bila terdapat alamat MAC tak dikenali melakukan pengiriman data *output* menjadi *request timed out* sehingga hubungan dan *Switch - host* diputus. *Switch* S2 memiliki pengaturan alamat MAC dalam sistem manual yang memanfaatkan *violation mode restrict*. Alamat MAC PC2 otomatis terdaftarkan namun tidak diklasifikan menjadi *sticky* MAC *address*. Kemudian *Switch* S3 memiliki pengaturan *sticky port security* pada jumlah maksimum alamat MAC yakni dua alamat serta *violation mode protect*. Alamat MAC kemudian terdaftarkan langsung usai dilaksanakan ping.

Penelitian[17] melaksanakan riset pada server *security* melalui pengaturan koneksi jaringan yang tak memiliki filter yang menyebabkan sistem internal bisa difilterisasi. Pemanfaatan DMZ bisa dijadikan lapisan keamanan dari server yang akan melindunginya dari *user* yang melakukan akses lebih dalam ke dalam server.

Penelitian [10] melaksanakan riset terkait keperluan pengamanan pada jaringan guna meningkatkan pengamanan pada server dari serangan dengan *port scanning* serta DoS (*Denial of Service*) dimana ditemukan implementasi *De-Militarised Zone* (DMZ) mampu melaksanakan filterisasi *Dos Attack* dengan baik.

IV. Hasil Dan Pembahasan

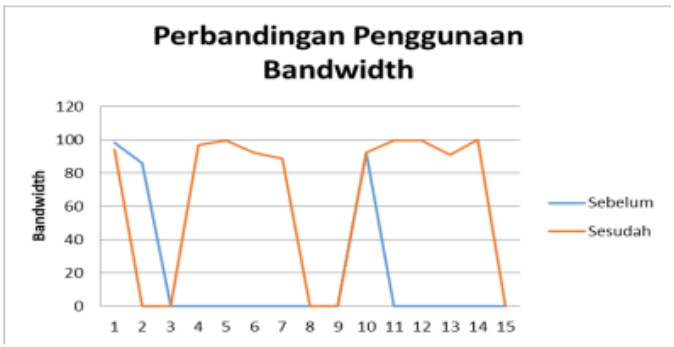
Pada penelitian[18] melaksanakan riset dengan menerapkan metode keamanan jaringan menggunakan *port security* dengan cara mendaftarkan *mac-address* pada *port* yang telah tersedia sehingga tidak sembarangan *port* atau hanya *port* yang telah terdaftar saja yang dapat mengakses server. Penelitian[5] dengan konfigurasi *switch port security* mendapatkan hasil paling efektif dengan menggunakan metode *sticky port security* dikarenakan dengan metode ini MAC *Address* dengan jumlah yang tidak sedikit secara otomatis.

Perbandingan bandwith sebelum dan sesudah menerapkan *port security* dapat dilihat pada tabell dibawah ini

TABEL I
HASIL PERBANDINGAN SEBELUM DAN SESUDAH *PORT SECURITY*

No.	Sebelum		Sesudah	
	Max *Bandwidth* (Mbps)	Presentase Penggunaan	Max *Bandwidth* (Mbps)	Presentase Penggunaan
1.	1,96	98%	1,88	94%
2.	1,72	86%	0	0%
3.	0,002	0,1%	0	0%
4.	0	0%	1,94	97%
5.	0	0%	1,99	99,5%
6.	0,0015	0.075%	1,85	92,5%
7.	0,0024	0.12%	1,77	88,5%
8.	0,0017	0.085%	0	0%
9.	0,0021	0.105%	0	0%
10	1,85	92.5%	1,85	92,5%

Dengan adanya Implementasi *port security* sangat berpengaruh pada penggunaan *bandwidth* dikarenakan hanya *computer* yang didaftarkan yang diperbolehkan melakukan akses pada *switch* agar *bandwidth* bisa beroperasi dengan level maksimum seperti pada Tabel I. tabel I memperlihatkan lost *bandwidth* berkisaran pada 4,6 persen yang kemudian dilakukan implementasi pada *port security* sehingga *bandwidth* dapat mengalami pengurangan yakni 74,79 persen - 4,6 persen =70,19 persen .



Gambar 7. Grafik Perbandingan Penggunaan *Bandwidth*

Pada Gambar 7 bisa dilihat bahwa grafik penggunaan sebelum dan sesudah implementasi sistem keamanan dengan menggunakan *port security* sangat bermanfaat, karena dengan implementasi ini pencurian dan penggunaan *bandwidth* yang tidak berkepentingan bisa dicegah.

Penelitian [10] melakukan pengujian dengan melakukan serangan DoS ICMP *Flooding Attack* ke server yang ditambahkan teknik DMZ dan tanpa DMZ. hasil dari pengujian tersebut adalah *loging* ICMP *flooding attack* terhadap server yang tidak menerapkan teknik DMZ rata-rata menghasilkan 16391,4 paket yang diterima dan rata-rata paket yang diterima oleh server yang menerapkan teknik DMZ sebanyak 32,2 paket. Terjadi penurunan jumlah paket saat terjadi *DoS attack* sebesar 16359,2 paket setelah mengimplementasikan teknik DMZ ke server, dimana hal tersebur membuktikan bahwa teknik DMZ berhasil melakukan filter pada *DoS attack* hal tersebut terjadi karena server yang menggunakan Teknik DMZ melakukan *filter* terhadap serangan DoS ICMP *Flooding Attack*.

Pada perbandingan antara server yang menggunakan DMZ dangan yang tidak menggunakan DMZ dengan menggunakan simulaton GNS3[1]

TABEL II
HASIL PERBANDINGAN SERVER MENGGUNAKAN DMZ DAN TANPA DMZ

Tanpa DMZ		Dengan DMZ	
Bandwidth (Mbits/s)	*Jitter* (ms)	*Bandwidth* (Mbits/s)	*Jitter* (ms)
9.60	0.530	9.80	0.099
9.98	0.529	10.0	0.089
10.1	0.473	9.98	0.203
10.0	0.319	9.98	0.091
9.97	0.357	9.98	0.084
10.0	0.383	9.97	0.104
9.98	0.380	10.0	0.163
9.97	0.367	9.98	0.125
10.0	0.648	9.98	0.088
9.98	0.572	9.98	0.017

Dari kedua pengukuran DMZ yang dilakukan pada tiap topologi diperoleh hasilnya yang cukup kecil, ini menyebabkan kualitas jejaring dimasukan dalam kategori baik. Dikarenakan besaran *jitter* yang makin mengecil,

menyebabkan kualitas jaringan menjadi membaik. Begitu pula bila besaran *jitter* mengalami peningkatan maka kualitas jejaring juga menurun.

Variasi *delay* (*jitter*) adalah variasi *delay* yang terjadi dalam pengiriman data pada suatu jaringan dimana *delay* antrian pada sebuah *router* dan *switch* menghasilak *jitter*[11] Berdasarkan perbedaan pada besaran *jitter* tersebut, bisa dibuat simpulan yang mana jaringan menggunakan DMZ mempunyai kualitas yang unggul dari jaringan yang tidak menggunakan DMZ. Dikarenakan besaran *jitter* yang dihasilkan lebih kecil.

V. KESIMPULAN

Berdasarkan hasil studi literatur dapat diberikan informasi yaitu pada pengamanan jaringan LAN dengan menggunakan *port security* menghasilkan pengurangan *bandwidth* dikarenakan hanya *computer* yang didaftarkan yang diperbolehkan melakukan akses pada *switch*. Sedangkan pengamanan dengan menggunakan DMZ sebelum memasuki layanan server akan dilakukan penyaringan *request* oleh *client* melalui *router firewall*. Sehingga apabila terjadi serangan maka yang pertama diserang adalah server *firewall* (*router*). Terjadi penurunan jumlah paket saat terjadi *DoS attack* sebesar 16359,2 setelah mengimplementasikan teknik DMZ dikarenakan server yang menggunakan Teknik DMZ melakukan *filter* terhadap serangan DoS ICMP *Flooding Attack*.

Penggunaan fungsi DMZ dan *Port security* dapat memberikan keamanan kepada jaringan. Akan tetapi keamanan itu bisa diberlakukan sebatas pada jangkauan luar (*outside*), di sisi lain jangkauan dalam (*inside*) mempunyai *system* pengamanan yang berbeda, hal ini menyebabkan diperlukannya tindakan menambahkan pengamanan contohnya pengamanan pada ruang penyimpanan serta sistemasi enksripsi *password* pada server.

REFERENSI

[1] I. Wira, L. S. I. Putri, S., A, and A. S. Rachman, "Uji Kinerja Dmz (De-Militarized Zone) Dengan Simulator Gns3 (Graphical Network Simulator)," *J. Tek. Inf.*, vol. 3, no. 1, pp. 1–10, 2018, doi: http://eprints.unram.ac.id/id/eprint/11326.

[2] A.Saputro, N. Saputro, and H. Wijayanto, "Metode Demilitarized Zone Dan *Port* Knocking Untuk Demilitarized Zone and *Port* Knocking Methods for *Computer*," *Metode*, vol. 3, no. 2, pp. 22–27, 2020, [Online]. Available: http://ejournal.uinsuka.ac.id/saintek/cybersecurity/article/download/2150/1801.

[3] Dasmen, R. N., Nugraha, M. D., & Adelia, A. (2022). Penerapan Pembatasan User Wi-Fi Pada Kantor Yayasan Patra Mandiri 01 Palembang. Jurnal Komputer Dan Informatika, 10(1), 18–23. https://doi.org/10.35508/jicon.v10i1.6286

[4] Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big [1] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," J. Sist. Informasi-J-SIKA, vol. 02, pp. 1–7, 2020.Data. Jurnal Sistem Informasi-J-SIKA, 02, 1–7.

[5] K. Al Fikri, "Keamanan Jaringan Menggunakan *Switch Port security*," *InfoTekJar J. Nas. Inform. Dan Teknol. Jar.*, vol. 5, no. 2, pp. 71–76, 2021, https://doi.org/10.30743/infotekjar.v5i2.3501.

[6] Z. Munawar and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J. Sist. Informasi-J-SIKA*, vol. 2, no. 1, pp. 1–7., 2020.

[7] Bhuse, V., Kalafut, A., & Dohn, L. (2019). Detection of a Rogue Switch in a Local Area Network. In *International Conference on Internet Monitoring and Protection, Nice, France*.

[8] Adams, N. P. H., Chisnall, R. J., Pickering, C., & Schauer, S. (2020). How port security has to evolve to address the cyber-physical security threat: lessons from the SAURON project. *International Journal of Transport Development and Integration*, *4*(1), 29-41.

[9] S. Sudaryanto, "Implementation *Port security* for Security Systems Network at the Computing Laboratory of Adisutjipto College of Technology," *Conf. Senat. STT Adisutjipto Yogyakarta*, vol. 4, no. 1, pp. 1–10, 2018, doi: https://doi.org/10.28989/senatik.v4i0.239.

[10] I. Anugrah and R. H. Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 5, no. 2, pp. 91–106, 2018, doi: https://doi.org/10.33558/piksel.v5i2.271.

[11] Putra, I. B. A. E. M., Adnyana, M. S. I. D., & Jasa, L. (2021). Analisis Quality of Service Pada Jaringan Komputer. *Majalah Ilmiah Teknologi Elektro*, *20*(1), 95. https://doi.org/10.24843/mite.2021.v20i01.p11

[12] Suteja, E., Kumalasari, E. N., & Raharjo, S. (2021). *PERANCANGAN SISTEM KEAMANAN JARINGAN UNTUK MENGURANGI KEJAHATAN CYBER MENGGUNAKAN TEKNIK DEMILITARIZED ZONE (DMZ) DAN FIREWALL RULES (Studi Kasus: Laboratorium Basis Data IST AKPRIND)*. *09*(01), 71–80.

[13] Desmira, D., & Wiryadinata, R. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *5*(1), 28–33. https://doi.org/10.55338/jikomsi.v5i1.242

[14] Saputro, A., Saputro, N., Wijayanto, H., & Informatika, P. S. (2020). Metode Demilitarized Zone Dan Port Knocking Untuk Demilitarized Zone and Port Knocking Methods for Computer. *Metode*, *3*(2), 22–27.https://scholar.archive.org/work/vuzz46kj7zb3rpanfhuilpg3aq/access/wayback/http://ejournal.uinsuka.ac.id/saintek/cybersecurity/article/download/2150/1801

[15] Pramana, Surya; JASA, Lie. Penerapan Metode Forward Chaining Untuk Rekomendasi Instalasi Local Area Network (LAN). Majalah Ilmiah Teknologi Elektro, [S.l.], v. 18, n. 2, p. 165--172, june 2019. ISSN 2503-2372.

[16] HERDIAN, Rama Beta; JASA, Lie; LINAWATI, Linawati. Manajemen Bandwidth Berdasarkan Prediksi Perilaku Pengguna Pada Jaringan TCP/IP Dengan Jaringan Syaraf Tiruan. Majalah Ilmiah Teknologi Elektro, [S.l.], v. 19, n. 1, p. 73-82, oct. 2020. ISSN 2503-2372.

[17] Arifin, M. A. S., & Zulius, A. (2019). Perancangan Sistem Keamanan Jaringan Pada Universitas Bina Insan Lubuklinggau Menggunakan Teknik Demilitarized Zone (Dmz). Jusikom : Jurnal Sistem Komputer Musirawas, 4(1), 19–24. https://doi.org/10.32767/jusikom.v4i1.443

[18] Sutiman, Gunawan, A. (2021). Firewall Port Security Switch Untuk Keamanan Jaringan Komputer Menggunakan Cisco Router 1600S Pada Pt. Tirta Kencana Tata Warna Sukabumi. *CONTEN (Computer and Network Technology)*, *1*(1), 13–22.

[19] Wardi, W., Basri Hasanuddin, Z., Andani, A., Jo Salli, J., & Muhammad Syafaat, A. (2020). Improving Network Performance of IP PBX Based Telecommunication System. Lontar Komputer : Jurnal Ilmiah Teknologi Informasi, 11(2), 101. https://doi.org/10.24843/lkjiti.2020.v11.i02.p04

[20] I. Sari, M. Yamin, L. M. F. Aksara, J. T. Informatika, F. Teknik, and U. H. Oleo, "Sistem Monitoring Serangan Jaringan Komputer Berbasis WEB Service Menggunakan Honeypot Sebagai Intrusion Prevention System," vol. 5, no. 1, pp. 35–44, 2019.

[21] R. Apriani, A. H. Jatmika, dan I. W. A. Arimbawa, "Implementasi Metode Intrusion Detection System (IDS) dan Port Knocking Pada Serangan Sistem Keamanan Dalam Jaringan Komputer," vol. 1, no. 1, 2019.

[22] Setiawan, Aidil, and Tamsir Ariyadi. "Manajemen VLAN Dan Switch Port Security Sebagai Keamanan Jaringan PT. PLN (Persero) Unit Layanan Pelanggan Ampera." *Prosiding Seminar*

Hasil Penelitian Vokasi (Semhavok). Vol. 3. No. 1. 2021.

[23] PRATAMA, MUHAMMAD FIERO PANGESTU, Ahmad Heryanto, and Tri Wanda Septian. *Implementasi Port Security Untuk Membatasi Akses Port Pada Switch Cisco*. Diss. Sriwijaya University, 2021.

[24] BERNADUS, I Nyoman; GUNANTARA, Nyoman; SAPUTRA, Komang Oka. Analisis Kinerja Jaringan Internet dengan Metode Class Based Queueing di Universitas Dhyana Pura. Majalah Ilmiah Teknologi Elektro, [S.l.], v. 18, n. 1, p. 133-140, may 2019. ISSN 2503-2372.

[25] Zara, Sukma Syaida, Andi Marwan Elhanafi, and Divi Handoko. "Pemodelan Jaringan Wan Dengan Teknologi Frame Relay Dengan Memanfaatkan Switch Port Security Sebagai Sistem Keamanan Jaringan." *SEMINAR NASIONAL TEKNOLOGI INFORMASI & KOMUNIKASI*. Vol. 1. No. 1. 2020.

[26] Sudaryanto, S. (2018). Implementation Port Security for Security Systems Network at the Computing Laboratory of Adisutjipto College of Technology. *Conference SENATIK STT Adisutjipto Yogyakarta*, *4*. https://doi.org/10.28989/senatik.v4i0.239

[27] Al Fikri, Khashaaisha, and Djuniadi Djuniadi. "Keamanan Jaringan Menggunakan Switch Port Security." *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan* 5.2 (2021): 302-307.

[28] Dandi, Muhammad. *Analisis Keamanan Jaringan Wireless Pada Smp Negeri 1 Walenrang Menggunakan Switch Security*. Diss. Universitas Cokroaminoto Palopo, 2020.

[29] Imani, Muhamad Yusuf, Nur Rachman Supadmana Muda, and Prisca Chorina. "Implementasi Backbone Network Security System Menggunakan Firewall Pada Komunikasi Hybrid." *Jurnal Telkommil* 2.Mei (2021): 49-54.

[30] Fahrizal, F., & Candra, B. A. (2022). Implementasi Access Control List Dalam Perancangan Virtual Local Area Network Pada PT CAKRAMEDIA INDOCYBER. *JEIS: Jurnal Elektro dan Informatika Swadharma*, *2*(2), 36-43.