Keamanan Jaringan dengan Metode *Access List Demilitarized Zone* pada *Cisco* RV042

Taufik Rahman[1], Rifqy Muzhaky Adha[2]
Universitas Bina Sarana Informatika, Jl. Kramat Raya No.98, RT.2/RW.9, Kwitang, Kec. Senen, Kota Jakarta Pusat, DKI Jakarta, Indonesia[1]
Universitas Nusa Mandiri, Jl. Raya Jatiwaringin No.2, RT.2/RW.13, Cipinang Melayu, Kec. Makasar, Kota Jakarta Timur, DKI Jakarta, Indonesia[2]
E-mail: taufik@bsi.ac.id[1], rifqy.ssm14@gmail.com[2]

Abstrack - Increasing users of mobile-based applications, making the network the backbone for every organization. It is very important to secure the network. Because many heterogeneous devices such as desktops, laptops, tablet pc, smartphones are connected on the network. Security is an important issue in the design and deployment of enterprise networks. Protecting servers from various network attacks and becomes a challenging task in providing security to servers and networks. Some of the challenges are, attacks that come from local networks other than the internet, connecting servers with internet and intranet networks. PT. Sarana Sistem Mikro is a company that relies heavily on fast and secure information access. It takes the development of existing computer networks at PT. Micro System Facilities. In conducting the analysis, using data collection methods, interviews, literature studies and research methods by conducting needs analysis, design, testing and implementation. Designing a network using the De-Militarized Zone method so that the network runs safely and optimally. And the results are applied to the specified DMZ drop protocol and port method, the server network security system at PT. Micro System Facilities are maintained.

Keywords - DMZ, Firewall, Cisco, Security, Network.

Intisari – Meningkatnya pengguna aplikasi berbasis mobile, menjadikan jaringan tulang punggung bagi setiap organisasi. Penting sekali mengamankan jaringan. Karena banyak perangkat heterogen seperti desktop, laptop, tablet pc, smartphone terhubung di jaringan. Keamanan isu penting dalam desain dan penyebaran jaringan perusahaan. Menjaga server dari berbagai serangan jaringan dan menjadi tugas menantang dalam memberikan keamanan ke server dan jaringan. Beberapa tantangannya adalah, Serangan yang datang dari jaringan Lokal selain internet, menghubungkan server dengan jaringan internet dan intranet. PT. Sarana Sistem Mikro adalah perusahaan ketergantungan tinggi pada akses informasi cepat juga aman. Sehingga dibutuhkan pengembangan jaringan komputer yang ada di PT. Sarana Sistem Mikro. Dalam melakukan analisa, menggunakan metode pengumpulan data, wawancara, studi pustaka dan metode penelitian dengan melakukan analisa kebutuhan, desain, testing dan implementasi. Merancang jaringan dengan menggunakan metode De-Militarized Zone agar jaringan berjalan dengan aman dan optimal. Dan hasil diterapkan metode DMZ drop protokol dan port yang ditentukan, sistem keamanan jaringan server pada PT. Sarana Sistem Mikro tetap terjaga.

Kata Kunci - *DMZ, Firewall, Cisco, Keamanan, Jaringan.*

I. PENDAHULUAN

Jaringan menjadi tulang punggung bagi setiap organisasi. Karena jaringan menyediakan berbagai fasilitas kepada pengguna. Penting untuk menjaga jaringan lebih aman dari luar, karena banyak perangkat heterogen seperti desktop, laptop, tablet pc dan smartphone terhubung di jaringan. Memberikan keamanan jaringan telah menjadi isu penting dalam desain dan penyebaran jaringan perusahaan. Inovasi dan difusi teknologi baru seperti komputasi universal,

mobilitas perusahaan, *E-commerce*, dan komputasi cloud, keamanan jaringan tetap menjadi tantangan yang semakin meningkat. Mencegah server dari berbagai serangan jaringan dan memberikan keamanan ke server adalah tugas yang sangat menantang. Beberapa tantangannya adalah, Serangan yang datang dari jaringan Lokal selain internet, menghubungkan server dengan jaringan internet dan intranet, dll., Seperti serangan jaringan yang berasal dari internet, server juga menghadapi serangan dari Jaringan Area Lokal. Jadi, disarankan untuk mencegah server dari serangan LAN (Local Area Network) juga.

Keamanan jaringan dapat menghentikan jaringan universitas dari berbagai jenis ancaman dan serangan. Kontribusi teoretis dari penelitian ini dapat menjadi model referensi desain jaringan kampus universitas yang dapat dirancang sebelumnya atau dibuat khusus untuk membuat jaringan yang kuat, namun serbaguna yang dibutuhkan oleh generasi berikutnya[1]. Setiap node akan berkomunikasi menggunakan pesan yang melaporkan status masing-masing ke node terdekat dan node master. Aplikasi atau data akan diminta dari server. Atas layanan yang diminta, mereka akan diberikan secara aman dengan teknik DMZ (Zona De-militerisasi). Mereka menyediakan tiga lapisan keamanan untuk permintaan data. Mereka memberikan keamanan terhadap kebocoran data dalam 3 lapisan dengan berbagai algoritma[2]. Kebocoran data diawali penyusupan dan untuk penyusupan pada HTTP di server web dapat menggunakan Teler[3].

II. SIGNIFIKANSI STUDI

Zona DeMiliterisasi adalah proses membangun jaringan semi-aman yang berfungsi sebagai garis pertahanan pertama untuk melindungi infrastruktur internal organisasi mana pun dari ancaman eksternal. Dengan menerapkan teknik kecil dan efisien ini, banyak masalah keamanan jaringan dapat diselesaikan. Makalah ini memberikan pandangan wawasan tentang berbagai tingkat desain DMZ dan berdasarkan tingkat desain ini, model DMZ kecil telah diusulkan untuk meningkatkan keamanan internal organisasi dengan mempertimbangkan masalah keamanan jaringan umum[4].

Hasil pemindaian kerentanan selama 13 tahun menunjukkan bahwa status keamanan di KEK-DMZ telah terjaga dalam kondisi baik. Selain itu, kami sedang mengembangkan kerangka kerja pemetaan relasional objek (ORM) DBPowder untuk meningkatkan fleksibilitas dan efisiensi dalam proses pengembangan Portal Pengguna DMZ[5]. Penelitian keamanan DMZ digabungkan dengan fitur *Load balancing*, *failover, IDS, QoS* dan *Vlan*[6]. Membandingkan DMZ Sains dengan jaringan tujuan umum, menyajikan hasil empiris dan kasus penggunaan yang berlaku untuk DMZ Sains saat ini dan masa depan[7].

Memberikan keamanan yang lebih ke server jaringan dengan mengonfigurasi NAT(Network Address Translation), Zona De-Militer, mencegah akses tidak sah ke situs web jurnal penelitian, Mengelola log terpusat untuk perangkat jaringan seperti switch jaringan, router, Menyediakan fasilitas internet untuk semua pengguna jaringan tanpa masalah dan manajemen ancaman. Dengan menerapkan berbagai teknik terbaru dalam jaringan, masalah di atas diperbaiki dan jaringan menjadi stabil setiap saat[8]. Penelitian DMZ dapat dikombinaasikan dengan menerapkan DDNS untuk remote router MikroTik dengan ceklist enable DDNS pada menu IPCloud[9]. Penggunaan DMZ pun menjadi lapis sistem pengamanan pada Universitas Bina Insan Lubuklinggau untuk melindungi jaringan internal[10].

Penelitian penerapan DMZ diuji dengan empat yakni *Ping Attack, Port Scanning, FTP Attack dan SSH Attack*[11]. Kemudian DMZ ditest pada server Computer Basic Test port dan protokol di belokkan[12]. untuk mencegah penetrasi atau *exploit* jaringan lokal atau jaringan lokal menerapkan DeMZ dan *Port Knocking*[13].

ASA menciptakan tiga antarmuka keamanan: Luar, Dalam, dan DMZ. Ini memberi pengguna luar akses terbatas ke DMZ dan tidak ada akses ke sumber daya internal. Pengguna

dalam dapat mengakses DMZ dan sumber daya luar. Metode yang digunakan pada artikel ini adalah Adaptive Security Device Manager (ASDM)[14]. DMZ dapat blokir virus dan akses illegal pada jaringan[15]. *penetration testing* adalah bagian dari kegiatan uji keamanan pada jaringan[16]. Keberadaan gateway router dengan firewall untuk misah jaringan internet dengan jaringan DMZ menjadi sangat rentan serangan (*Demilitarize Zone*) dan begitu pula dengan intranet[17].

PT. Sarana Sistem Mikro merupakan produsen mesin Absensi *Fingerprint* dan *Access control system* yang cukup besar dan berkembang di jakarta, saat ini perusahaan tersebut sedang melebarkan sayapnya untuk memasarkan produk ke seluruh nusantara bahkan manca negara. Maka dari itu perlu adanya keamanan jaringan pada PC (Personal Computer)/Laptop yang ada di PT. Sarana Sistem Mikro. Pada perusahaan tersebut pernah terjadi peristiwa pencurian data oleh seorang karyawan lama sehingga data-data yang cukup penting pada perusahaan sebagian telah diambil. Oleh karena itu, agar komunikasi dan pertukaran data yang terjadi antar kantor cabang tersebut berlangsung aman, maka tujuan dari penelitian untuk menganalisa dan merancang suatu konsep jaringan dengan metode *De-Militarized Zone* (DMZ) pada PT. Sarana Sistem Mikro agar perusahaan mempunyai suatu sistem keamanan yang baik.

Rencana pemecahan masalah dengan menerapkan konsep sistem keamanan jaringan non fisik dengan metode *De-Militarized Zone* (DMZ) yang dapat membuat atau mengontrol akses *network* untuk diizinkan masuk atau tidak didalam suatu jaringan sehingga user yang tidak memiliki izin untuk mengakses, maka user tersebut tidak diperbolehkan masuk ke dalam akses jaringan tersebut.

Pengembangan hipotesis dibuat pada PT. Sarana Sistem Mikro: apakah konsep DMZ dapat membatasi akses masuk ke jaringan terbatas? apakah konsep DMZ dapat mengontrol akses *network* komputer pada protokol yang disediakan server? Perangkat keras utama yang digunakan dalam penelitian ini adalah type CISCO RV042 sebagai router nya, dan Switch type D-LINK DGS-1024G 24 PORT, Sehingga dapat mempermudah dalam melakukan konfigurasi dengan konsep *De-Militarrized Zone.* Dalam penelitian menggunakan metode *De-Militarized Zone* yang menitik beratkan pada perangkat router. Agar dapat membatasi hak akses bagi user yang di izinkan atau tidak nya akses ke dalam network tersebut. Untuk mengetahui performance atau keamanan jaringan tersebut ada beberapa tahapan, diantaranya ada analisa, desain, peragaan prototype dan implementasi.

A. Analisa

Kebutuhan yang akan diperlukan untuk membuat konsep jaringan dengan metode *De-Militarized Zone* dengan menerapkan konsep *Access control list, NAT* yang menitik beratkan pada perangkat router.

B. Desain

Mendesain konsep sistem rancangan yang akan digunakan dan dibangun dengan metode *De-Militarized Zone* seperti skema jaringan, topologi jaringan, simulasi jaringan dengan software Cisco Packet Tracer Versi 7.2.1.

C. Peragaan Prototype

Berupa peragaan dengan bantuan *Software* Cisco Packet Tracer Versi 7.2.1. Hal ini dimaksudkan untuk mengevaluasi kinerja sebelum dibentuk nya konsep DMZ dan hasil setelah diterapkan konsep DMZ.

D. Implementasi

Implementasi *network* menggunakan semua yang direncanakan dan *desain* awal. Jaringan yang telah disimulasikan akan di uji untuk melihat bagaimana kinerjanya dan mengevaluasikannya.

III. HASIL DAN PEMBAHASAN

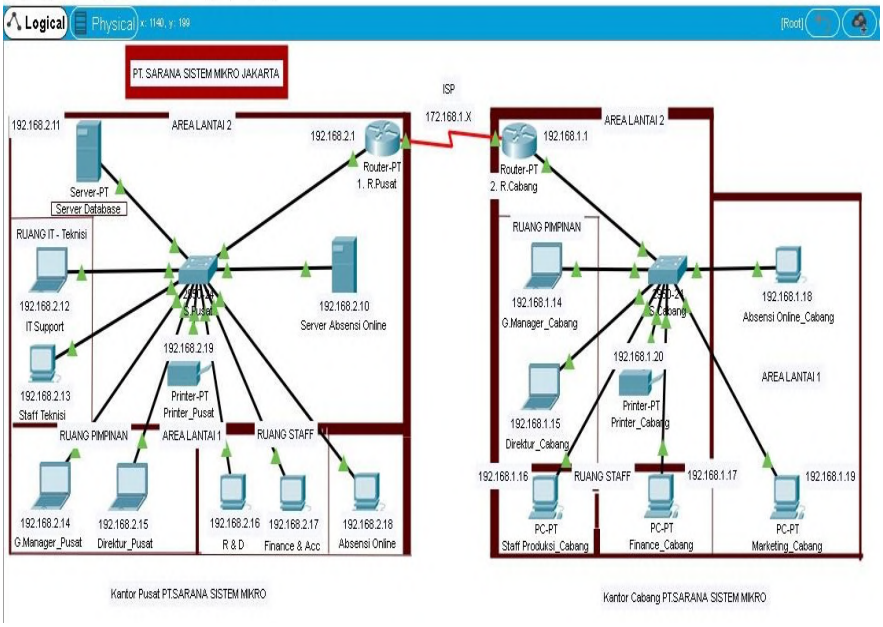
Penyelesaian untuk masalah pada PT. Sarana Sistem Mikro adalah dengan menggunakan metode *De-Militarized Zone* untuk memberi sistem keamanan pada jaringan internal kantor pusat.

A. Topologi Jaringan

PT. Sarana Sistem Mikro tetap menggunakan topologi bintang atau star. Alasan nya karna, jumlah pc atau laptop yang terkoneksi hanya sedikit serta *Maintenance service* lebih mudah dalam mendeteksi dan isolasi kesalahan atau kerusakan pengelolaan jaringan. Dan apabila jika ada komputer rusak, jaringan masih aktif tanpa menggangu aktivitas dari komputer yang lain.

B. Skema Jaringan

PT. Sarana Sistem Mikro, tetap menggunakan topologi bintang atau star dan berikut adalah skema jaringannya pada gambar 1.



Gambar 1. Skema Jaringan
(Sumber: PT. Sarana Sistem Mikro)

Pada perancangan keamanan jaringan, router digunakan sebagai perangkat keras untuk membatasi hak akses bagi user yang terkoneksi di jaringan tersebut.

C. Keamanan Jaringan

Dalam keamanan jaringan di PT. Sarana Sistem Mikro, merancang sebuah keamanan data dan mem-blok sebagian *Protocol* menggunakan metode *De- Militarized Zone* dengan konsep *Access Control List - NAT* yang nantinya akan di konfigurasi pada router type CISCO RV042 dalam proses penerapan metode *De- Militarized Zone*.

D. Rancangan Aplikasi

Aplikasi Cisco Packet Tracer versi 7.2.1 digunakan untuk merancang, men-simulasikan keamanan jaringan pada PT. Sarana Sistem Mikro dengan konsep yang simple dan dapat dimengerti.

E. Manajemen Jaringan

Berikut bentuk manajemen jaringan pada PT. Sarana Sistem Mikro.

1. Topologi Jaringan

PT. Sarana Sistem Mikro tetap menggunakan topologi bintang atau star. Alasan nya karna, jumlah pc atau laptop yang terkoneksi hanya sedikit serta *Maintenance service* lebih mudah dalam mendeteksi dan isolasi kesalahan atau kerusakan pengelolaan jaringan. Dan apabila jika ada komputer rusak, jaringan masih aktif tanpa menggangu aktivitas dari komputer yang lain.

2. IP Alamat

IP *Alamat* yang digunakan pada jaringan usulan di PT. Sarana Sistem Mikro menggunakan IP *Alamat* kelas C. Komputer yang terkoneksi ke jaringan tersebut di setting dengan IP *Static* yang telah di tentukan untuk setiap divisi nya. Dengan daftar IP *Alamat Static* sebagai berikut: Daftar IP *Alamat Static* Kantor Pusat pada tabel I.

TABEL I.
IP *ALAMAT STATIC* KANTOR PUSAT

Pemilik	IP Alamat
Router	192.168.2.1
Netmask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	192.168.2.10
Server Database	192.168.2.11
IT Support	192.168.2.12
Staff Teknisi	192.168.2.13
General Manager	192.168.2.14
Direktur	192.168.2.15
R & D	192.168.2.16
Finance & Accounting	192.168.2.17
Absensi Absensi Online	192.168.2.10
Printer Sharing	192.168.2.19

Daftar IP *Alamat Static* Kantor Cabang pada tabel II.

TABEL II.
IP *ALAMAT STATIC* KANTOR CABANG

Pemilik	IP Alamat
Router	192.168.1.1
Netmask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	192.168.2.10
General Manager Cabang	192.168.1.14
Direktur Cabang	192.168.1.15
Produksi Cabang	192.168.1.16
Finance Cabang	192.168.1.17
Marketing Cabang	192.168.1.19
Absensi Online Cabang	192.168.1.18
Printer Sharing	192.168.1.20

3. Konfigurasi pada Router Pusat dan Router Cabang

Konfigurasi untuk router pusat dan router cabang di perlihatkan pada gambar 2 sebagai berikut.

```
Router_Pusat#show running-config
Building configuration...
!
hostname Router_Pusat
!
enable password t3kn1k
!
ip cef
no ipv6 cef
!
ip domain-name www.serverssm.com
ip host www.serverssm.com 192.168.2.11 ip name-server 192.168.2.11
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
duplex auto speed auto
!
interface FastEthernet1/0 no ip address
duplex auto speed auto shutdown
!
interface Serial2/0 bandwidth 64
ip address 172.168.1.1 255.255.0.0
!
interface Serial3/0 no ip address clock rate 2000000 shutdown
!
interface FastEthernet4/0 no ip address
shutdown
!
interface FastEthernet5/0 no ip address
shutdown
!
router rip version 2
network 172.168.0.0
network 192.168.1.0
network 192.168.2.0
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4 login
!
end
```

(a)

```
Router_Cabang#show running-config
Building configuration...
!
hostname Router_Cabang
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip access-group 101 in duplex auto
speed auto
!
interface FastEthernet1/0 no ip address
duplex auto speed auto shutdown
!
interface Serial2/0 bandwidth 64
ip address 172.168.1.2 255.255.0.0
clock rate 64000
!
interface Serial3/0 no ip address clock rate 2000000 shutdown
!
interface FastEthernet4/0 no ip address
shutdown
!
interface FastEthernet5/0 no ip address
shutdown
!
router rip version 2
network 172.168.0.0
network 192.168.1.0
network 192.168.2.0
!
ip classless
!
access-list 101 deny tcp host 192.168.1.16 host 192.168.2.10 eq www
access-list 101 deny tcp host 192.168.1.16 host 192.168.2.10 eq ftp
access-list 101 deny tcp host 192.168.1.17 host 192.168.2.10 eq www
access-list 101 deny tcp host 192.168.1.17 host 192.168.2.10 eq ftp
access-list 101 deny tcp host 192.168.1.19 host 192.168.2.10 eq www
access-list 101 deny tcp host 192.168.1.19 host 192.168.2.10 eq ftp
access-list 101 deny tcp host 192.168.1.19 host 192.168.2.11 eq www
access-list 101 deny tcp host 192.168.1.19 host 192.168.2.11 eq ftp
access-list 101 deny tcp host 192.168.1.17 host 192.168.2.11 eq www
access-list 101 deny tcp host 192.168.1.17 host 192.168.2.11 eq ftp
access-list 101 deny tcp host 192.168.1.16 host 192.168.2.11 eq www
access-list 101 deny tcp host 192.168.1.16 host 192.168.2.11 eq ftp
access-list 101 permit ip any any
!
line con 0
line aux 0
line vty 0 4 login
!
!end
```

(b)

Gambar 2. (a) Running-Config pada Router Pusat (b) Running-Config pada Router Cabang

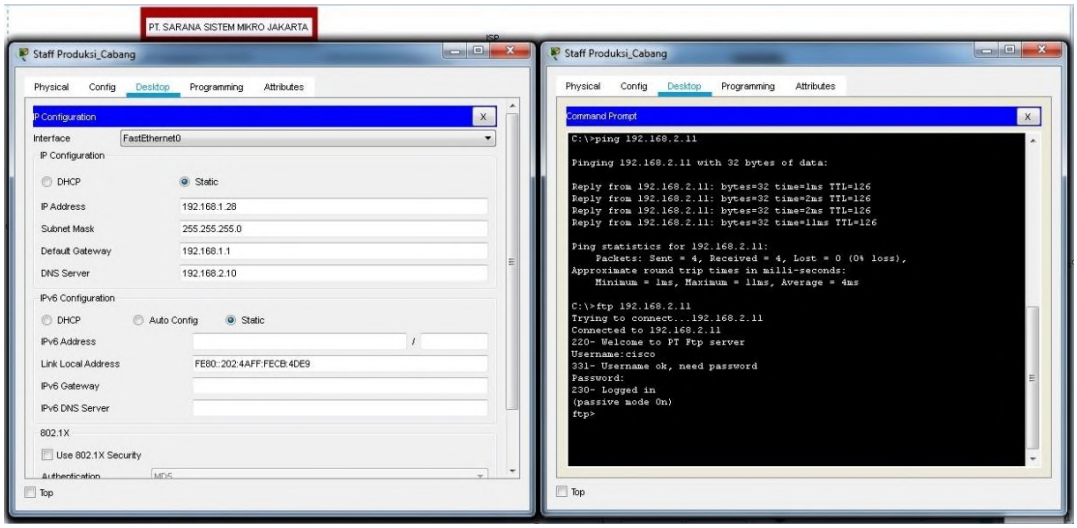
F. Pengujian Jaringan

Dalam merancang dan membangun jaringan untuk menjadi lebih baik, maka harus dilakukan pengujian pada jaringan awal dan usulan. Adapun pengujian jaringannya menggunakan Aplikasi Cisco Packet Tracer, sebagai berikut:

1. Pengujian Sebelum DMZ

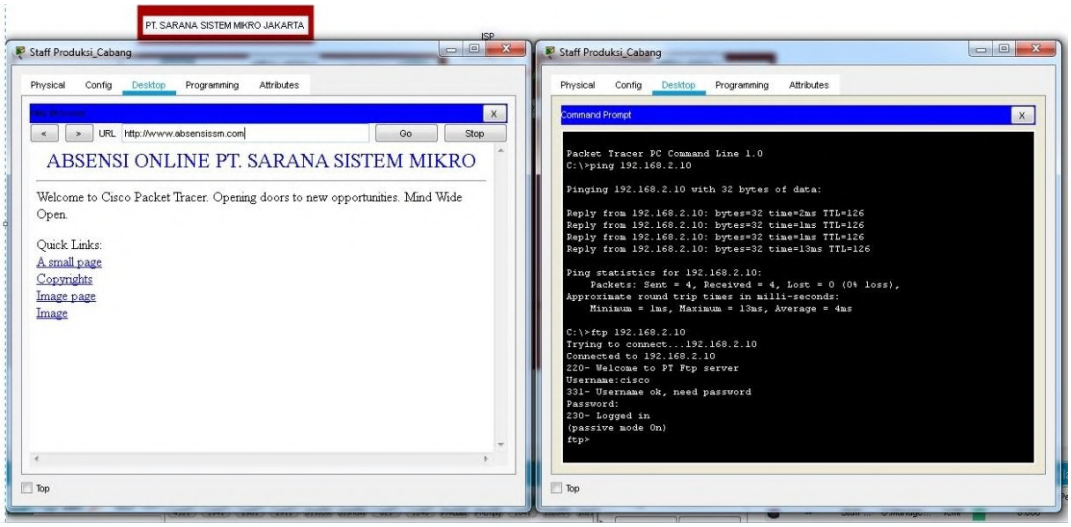
adalah awal test jaringan pada PT. Sarana Sistem Mikro sebelum DMZ. Pada pengujian jaringan awal karyawan di PT. Sarana Sistem Mikro (external kantor cabang) sering mengakses *web server* kantror pusat dan *file transfer protocol* (FTP) untuk mengambil data yang ada. Sehingga sangat berbahaya sekali apabila ada karyawan yang tidak mempunyai akses mengambil data akan tetapi bisa mengambil bebas data-data penting yang ada di kantor pusat. Kinerja sebagian karyawan sedikit menurun karena bisa mengakses jejaring sosial secara bebas. Berikut gambar dan keterangan masing-masing komputer yang dapat di akses oleh semua user

a) PC Staff Produksi_Cabang yang bisa akses ftp Server Database Kantor Pusat.



Gambar 3. Koneksi PC Staff Produksi_Cabang ke Server Database Kantor Pusat
(Sumber: PT. Sarana Sistem Mikro)

b) Koneksi PC Staff Produksi_Cabang ke www.absensissm.com dan ftp Server Absensi Online Kantor Pusat.



Gambar 4. Koneksi PC Staff Produksi_Cabang ke Server Absensi Online Kantor Pusat
(Sumber: PT. Sarana Sistem Mikro)

Hasil pengujian jaringan sebelum menggunakan DMZ disajikan pada tabel III.

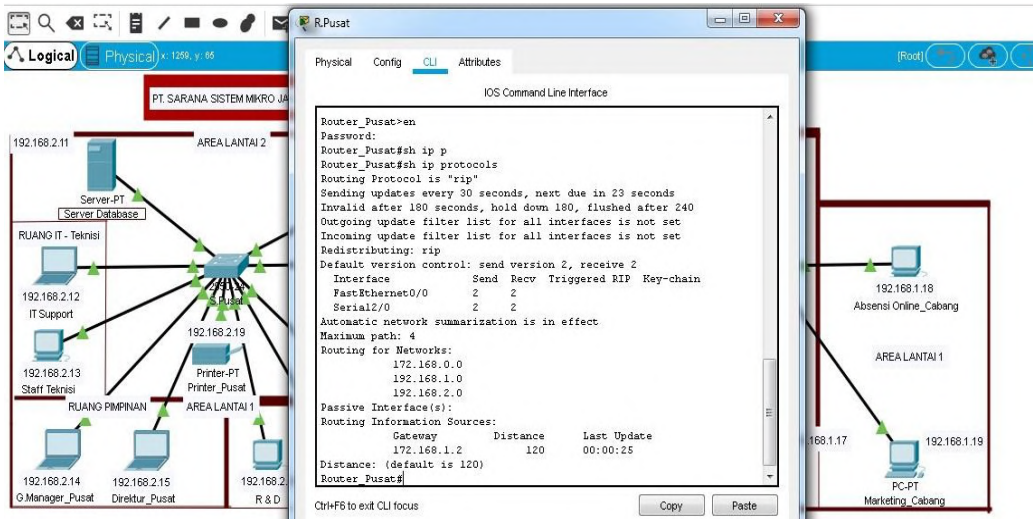
TABEL III.
HASIL PENGUJIAN JARINGAN SEBELUM DMZ

Personal Computer	Server Absensi Pusat			Server Database Pusat		
	icmp	**http**	**ftp**	**icmp**	**http**	**ftp**
PC Staf Produksi Cabang	bisa	bisa	bisa	bisa	bisa	bisa
PC Staf Finance Cabang	bisa	bisa	bisa	bisa	bisa	bisa
PC Sataf Marketing Cabang	bisa	bisa	bisa	bisa	bisa	bisa

2. *Pengujian DMZ Berjalan*

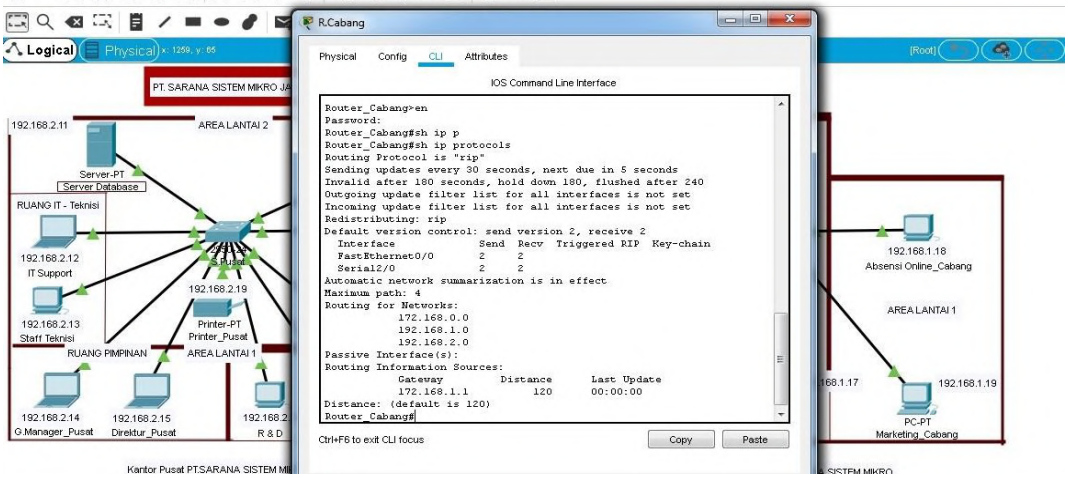
Pengujian DMZ bejalan adalah test uji jaringan pada saat DMZ diterapkan pada PT. Sarana Sistem Mikro Jakarta. Pada pengujian jaringan akhir ini PC Staff Produksi_Cabang tidak bisa mengakses ftp dan web server, pada PC Finance_Cabang tidak bisa mengakses ftp dan web server, begitu juga denga PC Marketing_Cabang tidak bisa mengkases ftp dan web server. Metode ini diterapkan agar kinerja karyawan meningkat dan keamanan pada jaringan internal Kantor Pusat PT. Sarana Sistem Mikro tetap terjaga dari Internet maupun External Kantor Cabang.

a) Agar komunikasi tetap terhubung antara Kantor Pusat dan Kantor Cabang, perlu adanya IP yang di NAT di Router. Berikut adalah daftar NAT Router Pusat :



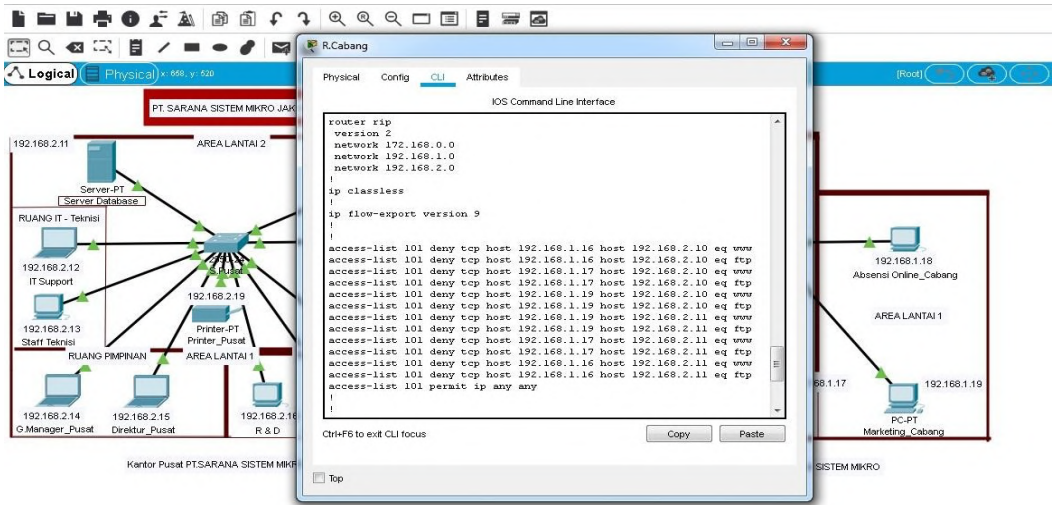
Gambar 5. Daftar NAT Router Pusat PT. Sarana Sistem Mikro
(Sumber: PT. Sarana Sistem Mikro)

b) Begitupun dengan Kantor Cabang, agar komunikasi tetap terhubung antara Kantor Cabang ke Kantor Pusat, perlu adanya IP yang di NAT di Router. Berikut adalah daftar NAT Router Cabang :



Gambar 6. Daftar NAT Router Cabang PT. Sarana Sistem Mikro

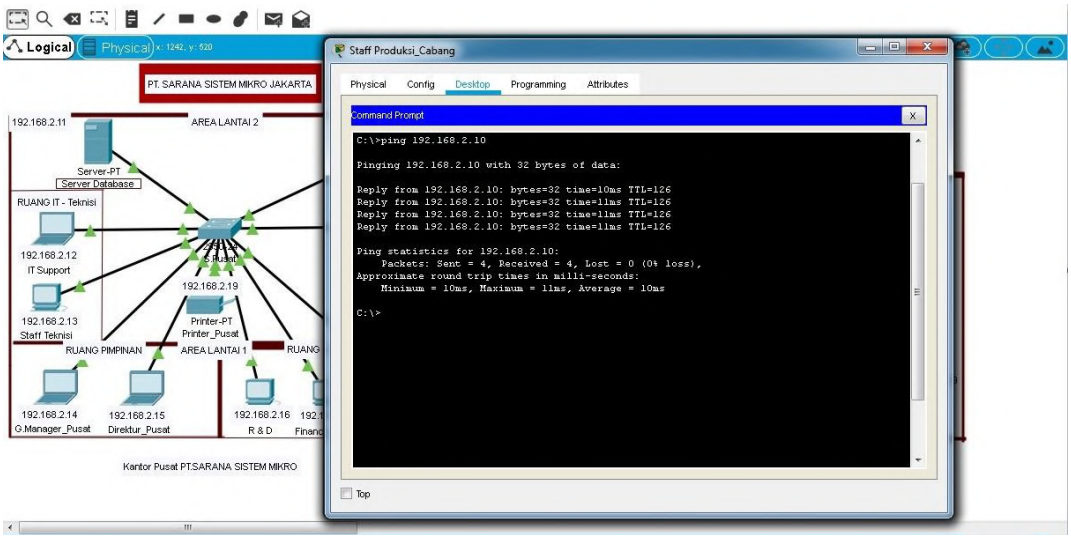
c) Berikut adalah daftar *Access Control List* Router Cabang, 3 PC *Client* di Kantor Cabang tidak di izin kan untuk mengakses Server dan Ftp dari Kantor Pusat, di karena kan untuk mencegah terjadi nya pengambilan data-data penting perusahaan di Kantor Pusat.



Sumber : PT. Sarana Sistem Mikro

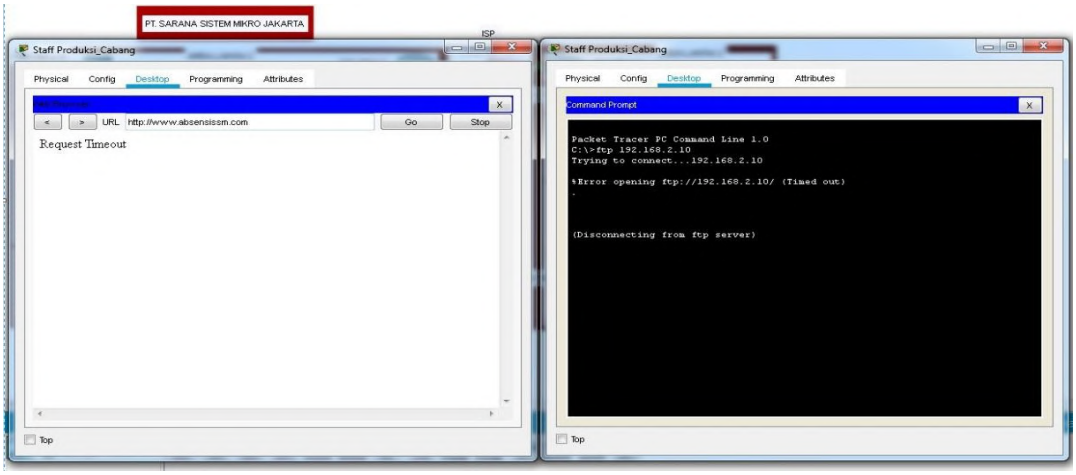
Gambar 7. Daftar Access Control List Router Cabang PT. Sarana Sistem Mikro

d) Test PING dari PC Staff Produksi_Cabang ke Server Absensi Online Kantor Pusat. IP tersebut Reply, akan tetapi PC Staff Produksi_Cabang tidak bisa Akses ke www.absensissm.com dan ftp Server Absensi Online Kantor Pusat.



Gambar 8. Test PING PC Staff Produksi_Cabang ke Server Absensi Online Kantor Pusat
(Sumber: PT. Sarana Sistem Mikro)

e) PC Staff Produksi_Cabang tidak bisa akses ke Server Absensi Online atau www.absensissm.com dan ftp Server Absensi Online Kantor Pusat.



Gambar 9. Koneksi PC Staff Produksi_Cabang yang tidak bisa akses ke Server Absensi Online Kantor Pusat (Sumber : PT. Sarana Sistem Mikro)

Hasil pengujian pada PC staf produksi, finance dan marketing cabang setelah implementasi DMZ pada router cabang sehingga tidak bisa akses ke protokol http port 80, ftp pada server database, absen pusat. Protokol yang diijinkan atau bisa hanya icmp untuk melakukan test koneksi jaringan sebagaimana pada tabel 4.

TABEL IV.
HASIL PENGUJIAN JARINGAN SETELAH DMZ

Personal Computer	Server Absensi Pusat			Server Database Pusat		
	icmp	**http**	**ftp**	**icmp**	**http**	**ftp**
PC Staf Produksi Cabang	bisa	tolak	tolak	bisa	tolak	tolak
PC Staf Finance Cabang	bisa	tolak	tolak	bisa	tolak	tolak
PC Sataf Marketing Cabang	bisa	tolak	tolak	bisa	tolak	tolak

IV. KESIMPULAN

Berdasarkan pengujian yang dilakukan dengan menggunakan metode *De-Militarized Zone* dapat menjaga sistem keamanan dengan cara memblok protokol dan port jaringan dengan IP *Alamat* yang telah ditentukan pada jaringan yang sekiranya dapat membahayakan dalam jaringan tersebut. Memblok *protocol* seperti *FTP* dan *DNS* pada sebagian *Personal Computer* yang ada pada jaringan PT. Sarana Sistem Mikro yang berfungsi untuk membatasi hak akses bagi user-user yang tidak diperbolehkan akses protocol tersebut, tetapi masih bisa akses pada protokol icmp untuk pengecekan koneksi dan untuk absen staff melakukan tap finger pada alat fingerprint. Penelitian lanjut dapat mencatat log ip alamat yang mencoba mengakses protokol dan port yang dibatasi sehingga dapat dimonitoring aktifitas pada jaringan berjalan.

REFERENSI

[1] G. Michael, “ijpam.eu,” vol. 116, no. 8, pp. 303–307, 2017.
[2] M. Buvaneswari, M. P. Loganathan, and S. Sangeetha, “Cloud challenges of load balancing and security issues using ICLoS algorithm,” *Proc. 2017 2nd Int. Conf. Comput. Commun. Technol. ICCCT 2017*, pp. 103–105, 2017.
[3] A. Tedyyana and O. Ghazali, “Teler Real-time HTTP Intrusion Detection at Website with Nginx Web,” *Int. J. Informatics Vis.*, vol. 5, no. September, pp. 327–332, 2021.
[4] K. Dadheech, A. Choudhary, and G. Bhatia, “De-Militarized Zone: A Next Level to Network Security,” *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2018*,

no. Icicct, pp. 595–600, 2018.
[5] T. Murakami, "Design and development of vulnerability management portal for DMZ admins powered by DBPowder," *EPJ Web Conf.*, vol. 214, p. 08014, 2019.
[6] A. Wijaya and T. D. Purwanto, "Implementasi Metode Rekayasa Sistem Jaringan Komputer untuk Pengembangan Jaringan Komputer," *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 3, p. 294, 2019.
[7] J. Crichigno, E. Bou-Harb, and N. Ghani, "A Comprehensive Tutorial on Science DMZ," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 2041–2078, 2019.
[8] T. Shanmugam and B. Malarkodi, "Analysis of Recent Challenges and Solutions in Network Security," *2019 2nd Int. Conf. Intell. Comput. Instrum. Control Technol. ICICICT 2019*, pp. 902–907, 2019.
[9] S. Oei, "Implementasi Ip Cloud Dan Demilitarized Zone (Dmz) Untuk Pengontrolan Router Jarak Jauh," *Semin. Nas. Teknol. dan Sains*, no. September, 2019.
[10] M. A. S. Arifin and A. Zulius, "Perancangan Sistem Keamanan Jaringan Pada Universitas Bina Insan Lubuklinggau Menggunakan Teknik Demilitarized Zone (DMZ)," *Jusikom J. Sist. Komput. Musirawas*, vol. 4, no. 1, pp. 19–24, 2019.
[11] F. Siti, L. Z. Azhar, and L. Widyawati, "Jaringan Pada Server Menggunakan De-Militarised Zone (Dmz)," 2021.
[12] I. Dayasa, "Analisa Penerapan De-Militarized Zone (DMZ) Pada Server Computer Based Test (CBT)," pp. 1–6, 2020.
[13] A. Saputro, N. Saputro, H. Wijayanto, and P. S. Informatika, "Metode Demilitarized Zone Dan Port Knocking Untuk Demilitarized Zone and Port Knocking Methods for Computer," vol. 3, no. 2, pp. 22–27, 2020.
[14] A. K. Durianto, "Konfigurasi Cicso ASA Firewall Menggunakan ASDM," vol. 5, no. 2, pp. 298–305, 2021.
[15] M. A. Al Fauzan and T. D. Purwanto, "Perancangan Firewall Router Menggunakan Opnsense Untuk Meningkatkan Keamanan Jaringan Pt. Pertamina Asset 2 Prabumulih," *Pros. Semhavok*, pp. 137–146, 2021.
[16] Haeruddin, "Security Design And Testing of Lan and Wlan Network in Mikrotik Router Using Penetration Testing Method FROM Mitm Attack," *J. Informatics Telecommun. Eng.*, vol. 4, no. 1, pp. 119–127, 2020.
[17] A. D. Alexander, R. Salkiawat, and J. Warta, "Perancangan Intrusion Detection System Menggunakan Honeypot Pada Universitas Bhayangkara Jakarta Raya," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 33–37, 2021.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih disampaikan kepada Tim *Jurnal Informatika Polbeng* yang telah meluangkan waktu untuk mereview artikel ini guna menunjang penelitian ini dengan baik dan dapat terbit pada *Jurnal Informatika Polbeng*.