PERANCANGAN SISTEM KEAMANAN JARINGAN PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU MENGGUNAKAN TEKNIK DEMILITARIZED ZONE (DMZ)

M. Agus Syamsul Arifin[1], Antoni Zulius[2]
[1,2] Program Studi Rekayasa Sistem Komputer,Universitas Bina Insan, Lubuklinggau
[1,2] Institution/affiliation; address, telp/fax of institution/affiliation
e-mail: [1] mas.agus1988@gmail.com, [2] anton.zulius@gmail.com

Abstrak

Pengamanan Jaringan merupakan salah satu tindakan untuk menjaga data yang terdapat di server selain menggunakan metode enskripsi data terdapat juga salah satu Teknik yang di gunakan untuk mengamankan jaringan yaitu dengan menggunakan Teknik DMZ (Demilitarized Zone). DMZ merupakan sebuah area dalam jaringan yang di bangun untuk melindungi sistem internal dengan cara memisahkan lalulintas Data yang ada pada jaringan. Lalulintas data pada Jaringan Universitas Bina Insan Lubuklinggau tidak terfilter sehingga sistem internal yang ada dalam hal ini adalah perangkat server tidak memiliki pengamanan selain sistem keamanan *built in* yang ada pada sistem operasi yang di gunakan oleh server Universitas (Firewall Sistem Operasi) pengguna yang mengakses jaringan Internet menggunakan IP Address yang biasa di gunakan mahasiswa dapat juga memasuki jaringan yang di gunakan oleh server secara langsung tanpa terfilter, dengan menggunakan Teknik DMZ lalulintas data Server yang ada akan dipisah dari Jaringan yang di gunakan oleh mahasiswa dan Jaringan Luar, sehingga mahasiswa dan pengguna hanya akan dapat mengakses port yang sudah di tentukan saja. Penggunaan Teknik DMZ nantinya akan menjadi sistem lapis pengamanan pertama dari server yang ada di Universitas Bina Insan Lubuklinggau agar beberapa port dapat terlindungi dari pengguna yang berusaha mengakses lebih dalam ke dalam Server.
Kata kunci : Demilitarized Zone (DMZ), Keamanan Jaringan, Server

Abstract

Network Security is one of the ways to maintain the data contained on the server besides using data encryption methods, there is also one of the techniques used to secure the network by using the DMZ (Demilitarized Zone) technique. DMZ is an area in a network that is built to protect internal systems by separating traffic data on the network. Data traffic on the Bina University Network Lubuklinggau Staff is not filtered so that the internal system in this case is that the server device has no security other than the built-in security system that is on the operating system used by the University server (Firewall Operating System) users accessing the Internet network using an IP address that is commonly used by students can also enter the network that is used directly by the server without filtering, using the DMZ technique data traffic Existing servers will be separated from the network used by students and the outside network, so students and users will only can only access the specified port. The use of the DMZ Technique will later become the first security layer system from the server at Bina University, Lubuklinggau, so that several ports can be protected from users trying to access deeper into the Server.
Keywords : Demilitarized Zone (DMZ), Network Security, Server

I. PENDAHULUAN

Pengamanan Jaringan merupakan salah satu tindakan untuk menjaga data yang terdapat di server selain menggunakan metode lain seperti enkripsi data, salah satu Teknik yang di gunakan untuk mengamankan jaringan adalah dengan menggunakan Teknik DMZ (Demilitarized Zone). Teknik ini bekerja dengan memisahkan traffic data dari IP Publik internet dan IP Lokal di Universitas Bina Insan untuk melindungai server dengan membuat lingkungan khusus dalam jaringan, dalam penelitian ini router yang di gunakan adalah Router Mikrotik. Cara kerja Teknik ini adalah dengan merancang dan mengatur IP perangkat yang di gunakan pengguna dapat diakses dari luar dan di petakan melalui IP Publik yang diberikan oleh firewall, biasanya perangkat yang menggunakan IP privat dan dapat diakses dari jaringan public adalah perangkat Server.

Pelayanan untuk mahasiswa yang ada di Universitas Bina Insan khususnya yang berkaitan dengan system akademik masih sering mengalamai kendala karena bandwidth internet yang terbatas. Bandwidth internet yang digunakan saat ini harus melayani mahasiswa yang mengakses server di Universitas Bina Insan melalui jaringan internet (di luar Jaringan Lokal Universitas Bina Insan) maupun mahasiswa yang sedang berada di dalam kampus, jika mahasiswa yang ada di dalam kampus tersebut ingin mengakses website yang ingin dikunjungi selain aplikasi yang ada pada system yang berada di Server Universitas Bina Insan, sehingga bandwidth ini harus melayani dua kebutuhan tersebut.

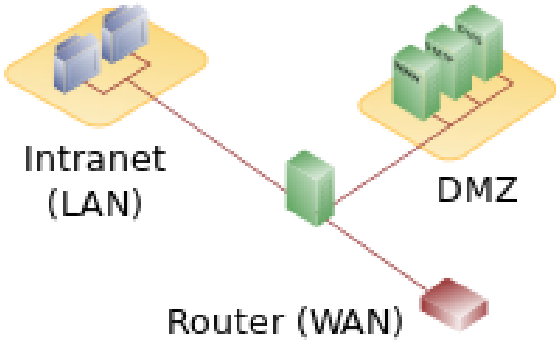
Belum adanya pemisahan antara lingkungan Server dan jaringan luar serta jaringan yang di gunakan Mahasiswa sehingga Server menjadi Rentan terhadap serangan – serangan Cyber.

Dengan teknik DMZ area jaringan Server akan di pisah dari Jaringan Luar dan jaringan yang di gunakan Mahasiswa.

II. TINJAUAN PUSTAKA

2.1 DMZ (Demilitarized Zone)

DMZ adalah kependekan dari Demilitarized Zone, suatu area yang digunakan berinteraksi dengan pihak luar. Dalam hubungannya dengan jaringan komputer, DMZ merupakan suatu sub network yang terpisah dari sub network internal untuk keperluan keamanan. [1]



Gambar 1. Contoh penggunaan DMZ pada sebuah Jaringan

2.2 Mikrotik

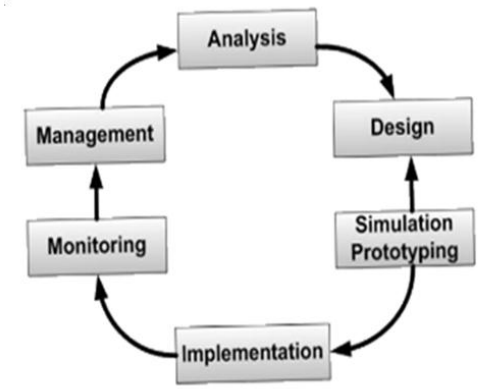
Mikrotik adalah sistem operasi beserta perangkat lunak yang dipasang dalam sebuah komputer sehingga komputer yang sudah terpasang tersebut bisa dioperasikan. adapun komputer yag sudah terhubung dengan mikrotik berperan sebagai jantung network, pengendali, pengatur lalulintas data. Jadi kesimpulannya mikrotik adalah sistem operasi khusus yang digunakan untuk router. Selain itu istilah Mikrotik juga akrab dipanggil dengan Router OS yang memiliki fungsi yang handal dan punya banyak sekali fitur yang mendukung kelancaran network. [2]

Gambar 2. Mikrotik Routerboard CCR1009-7G-1C-1S+ [3]

Pada gambar 2 adalah perangkat Router mikrotik yang di gunakan pada Universitas Bina Insan Lubuklinggau.

III. METODOLOGI PENELITIAN

Pada Penelitian ini Metode pengembangan yang di gunakan untuk pengembangan sistem adalah menggunakan metode Pendekatan Network Development Life Cycle (NDLC). Metode NDLC memiliki 7 bagian tahapan dalam melakukan pengembangan Sistem yaitu Analisis, Desain, Simulasi Purwarupa, Penerapan, Monitoring, dan Manajemen Sistem yang sudah di buat. Seperti pada Gambar 3 berikut :



Gambar 3. Network Development Life Cycle (NDLC)

1. Analisis

Hasil dari analisis kondisi Jaringan yang ada di Universitas Bina Insan Lubuklinggau adalah sistem keamanan Jaringan yang masih minim di Universitas Bina Insan akan terbantu dengan penerapan teknik DMZ untuk mengamankan Jaringan Server.

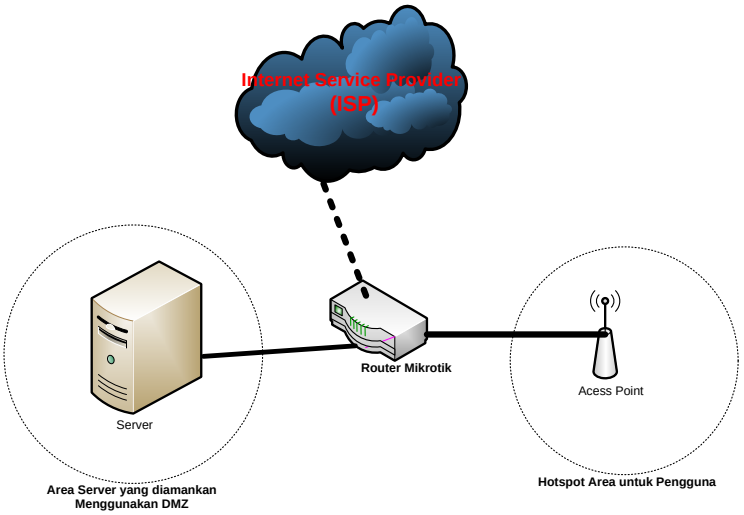
2. Desain

Desain Jaringan dan Pengalamatan IP Address yang akan di gunakan untuk teknik DMZ seperti pada Tabel 1 dan Gambar 4 berikut :

Tabel 1. Pengalamatan IP

No	Perangkat	IP Network	IP Address	Ket
1	Mikrotik	180.250.44.160	180.250.44.163	IP Publik
		99.99.99.0	99.99.99.1	IP Ke Server
		100.100.100.0	100.100.100.1	IP Pengguna
2	Server	99.99.99.0	99.99.99.2	IP Server

IP address yang di gunakan oleh pengguna dan server di buat berbeda karena untuk pembuatan firewall pada pengaturan di Mikrotik.



Gambar 4. Topologi Perancangan Penerapan DMZ

3. Simulasi Purwarupa

Simulasi yang dilakukan adalah dengan melakukan test ping dari komputer pengguna ke alamat IP Lokal yang di gunakan oleh server dan hasil yang harus didapatkan adalah *request time out* pada komputer pengguna atau *Destination Host Unreachable*.

4. Penerapan

Penerapan Sistem keamanan akan di laksanakan apabila simulasi yang dilakukan berhasil apabila komputer pengguna tidak bisa melakukan koneksi secara langsung ke Server menggunakan IP Lokal yang di gunakan Server.

5. Monitoring

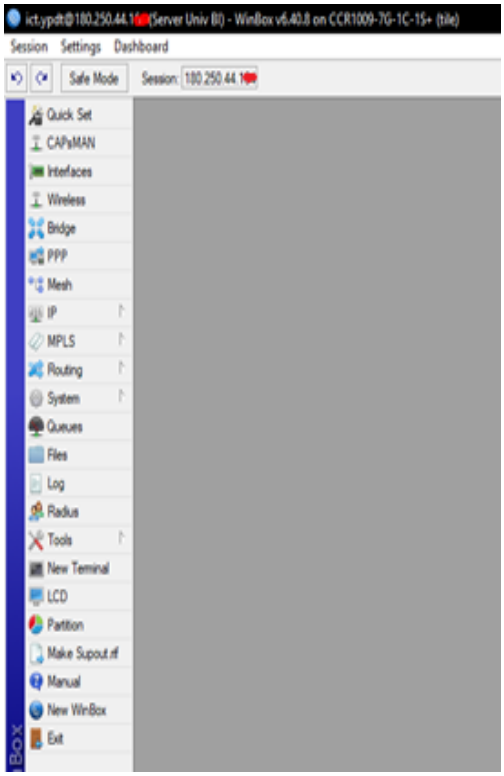
Monitoring pada penelitian ini bertujuan untuk memantau hasil penerapan sistem keamanan yang sudah di pasang pada jaringan Universitas Bina Insan Lubuklinggau. Pada tahapan ini akan dilihat apakah DMZ berjalan sesuai dengan yang diinginkan atau belum.

6. Manajemen

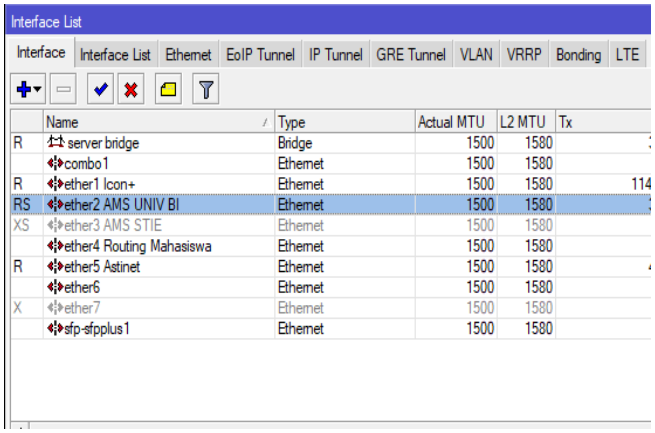
Manajemen pada penelitian ini bertujuan untuk melakukan pengaturan konfigurasi yang di butuhkan agar sistem tetap bisa berjalan dengan baik sesuai dengan fungsinya

IV. HASIL DAN PEMBAHASAN

4.1 Hasil

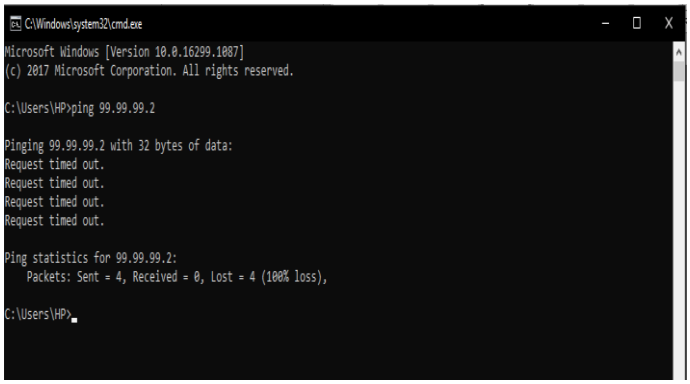


Gambar 5. Tampilan Awal Winbox untuk memulai melakukan Konfigurasi DMZ

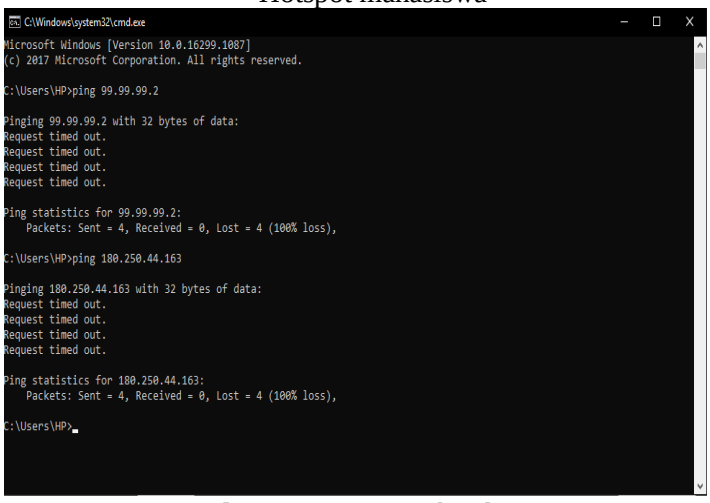


Gambar 6. Daftar Interface yang ada pada perangkat Mikrotik yang di gunakan

Pengujian dilakukan dengan melakukan Ping test pada Komputer pengguna ke alamat IP Lokal Server di Universitas Bina Insan Lubuklinggau.



Gambar 7. Test Ping ke alamat IP lokal Server menggunakan jaringan Hotspot mahasiswa

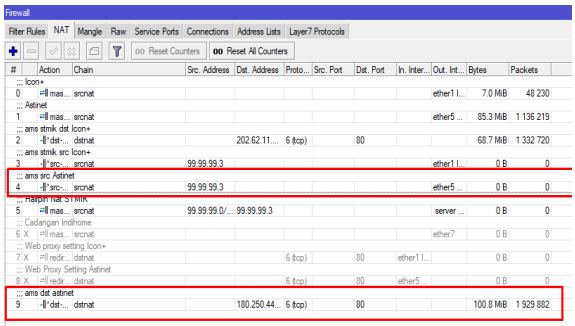


Gambar 8. Test Ping ke alamat IP Publik Server menggunakan jaringan Hotspot mahasiswa

Hasil yang didapat pada pengujian ping test adalah RTO (*Request Time Out*) karena pengguna hanya di izinkan untuk mengakses port 80 yang di gunakan untuk menampilkan program aplikasi yang ada pada server. Sedangkan Ping test menggunakan Protokol ICMP (Internet Control Message Protocol). ICMP berada pada Network Layer di OSI Layer Model dan merupakan bagian dari Protokol TCP/IP.[4]

4.2 Pembahasan

Hasil dari konfigurasi DMZ yang akan diterapkan dapat dilihat pada gambar 9 berikut



Gambar 9. Hasil Komfigurasi DMZ pada Mikrotik Routerboard CCR1009-7G-1C-1S+

Port yang di gunakan untuk program aplikasi yang ada pada server adalah menggunakan port 80 sehingga pengguna akan dialihkan menuju port 80 untuk dapat mengakses server.

Pada area DMZ digunakan untuk melindungi system internal yang berhubungan dengan serangan *hack attack*. DMZ bekerja pada seluruh Layanan dasar pada jaringan yang membutuhkan akses terhadap jaringan internet ke jaringan yang lainnya sehingga semua port yang di buka yang berhubungan dengan internet akan berada pada jaringan yang berada dalam jangkauan pengelola jaringan, sehingga apabila ada yang ingin melakukan serangan dan melakukan crack pada server yang menggunakan sistem DMZ pelakunya hanyaa akan dapat mengakses host (IP Public) saja dan bukan pada jaringan internal. Secara umum DMZ dibangun berdasarkan NAT (Network Address Translation), PAT (Port Addressable Translation), dan Access List pada Mikrotik. NAT berfungsi untuk menunjukkan kembali paket-paket yang datang dari "real address" ke alamat internal. Sebagi contoh pada penelitian ini IP Public yang di gunakan adalah 180.250.44.163, pada penelitian ini dapat membuat NAT pada lalulintas data yang ke 99.99.99.4 (sebuah alamat jaringan internal). Kemudian PAT berfungsi untuk menunjukan data yang datang pada particular port, atau range sebuah port dan protocol (TCP/UDP atau lainnya) dan alamat IP ke sebuah particular port atau range sebuah port ke sebuah alamat internal IP. Sedangkan access list berfungsi untuk mengontrol secara tepat apa yang datang dan keluar dari jaringan dalam suatu pertanyaan. Dalam penelitian ini peneliti menolak ICMP yang datang ke seluruh alamat IP kecuali untuk sebuah ICMP yang diinginkan.

V. KESIMPULAN

Pada Penelitian ini kesimpulan yang dapat di ambil adalah :

1. DMZ digunakan untuk melindungi system internal yang berhubungan dengan serangan *hack attack*.
2. DMZ bekerja pada seluruh Layanan dasar pada jaringan yang membutuhkan akses terhadap jaringan internet ke jaringan yang lainnya sehingga semua port yang di buka yang berhubungan dengan internet akan berada pada jaringan yang berada dalam jangkauan pengelola jaringan.
3. Server pada Universitas Bina Insan hanya bisa diakses pada port tertentu yaitu salah satunya port 80 yang di gunakan oleh program aplikasi.

VI. SARAN

Pada penelitian ini tidak di lakukan pengujian serangan dari luar untuk menguji keamanan jaringan menggunakan DMZ. Pengujian yang dilakukan hanya dengan menggunaka pengiriman paket data menggunakan protokol ICMP.

VII. DAFTAR PUSTAKA

[1] Pengertian Demilitarized Zone (https://www.proweb.co.id/articles/ict/dmz.html, diakses tanggal 1 Mei 2019)
[2] Mikrotik (https://blog.dimensidata.com/pengertian-mikrotik-dan-fungsi-mikrotik-pada-jaringan-komputer/, diakses tanggal 1 Mei 2019)
[3] Routerboard CCR1009-7G-1C-1S+ (http://www.mikrotik.co.id/produk_lihat.php?id=609, diakses tanggal 1 Mei 2019)
[4] ICMP (https://www.pcwdld.com/what-is-icmp-and-port, diakses tangga 1 Mei 2019)