**PERANCANGAN JARINGAN DAN KEAMANAN FIREWALL PACKET FILTERING MENGGUNAKAN METODE TOP DOWN**

**(Studi Kasus Asrama Mahasiswa J.C Oeavaang Oearay Kalimantan Barat)**

**1Jacky Murdianto, 2Prita Haryani, 3Joko Triyono**

1,2Jurusan Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta

3 Jurusan Rekayasa Sistem Komputer, Institut Sains & Teknologi AKPRIND Yogyakarta

Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029

Email:1[jackybontang@gmail.com1](mailto:jackybontang@gmail.com1), [priyaharyani@akprind.ac.id2](mailto:priyaharyani@akprind.ac.id2)[jack@akprind.ac.id](mailto:jack@akprind.ac.id)3

**Abstract**

J.C Oeavaang Oearay student dormitory in West Kalimantan previously had a WLAN (Wireless Local Area Network) network design. The design is only equipped with security using user and password validation. Of course this is less effective because outsiders can still access the network and without security are more vulnerable to data theft. The purpose of designing a network with firewall security using the Top-Down method is a solution to solving problems that exist in the student dormitory of J.C Oeavaang Oearay, West Kalimantan. Stages with the Top-Down method consist of needs analysis, logical network design, physical network design, implementation, testing, and maintenance. In this study using the PPDIOO method because with the increasingly complete network service requirements, a methodology that supports architectural design and network design is needed. Therefore, this research uses a firewall and tests such as Ping, Tracert, and Mail Server tests. The results of network design and firewall network security in the student dormitory of J.C Oeavaang Oearay West Kalimantan went well and could be used as guidelines for implementation.

***Keywords****: Design, Network, Firewall, Top-Down*

Abstrak

Asrama mahasiswa J.C Oeavaang Oearay Kalimantan Barat sebelumnya sudah mempunyai rancangan jaringan *WLAN* (*Wireless Local Area Network*). Rancangan tersebut hanya dilengkapi dengan keamanan menggunakan validasi *user* dan *password*. Tentu saja hal ini kurang efektif karena pihak luar masih dapat mengakses jaringan dan tanpa keamanan yang lebih sangat rentan dengan pencurian data. Tujuan membuat rancangan jaringan dan keamanan *firewall* dengan menggunakan metode *Top-Down* adalah solusi untuk menyelesaikan masalah yang ada di asrama mahasiswa J.C Oeavaang Oearay Kalimantan Barat. Tahapan dengan metode *Top-Down* terdiri dari analisis kebutuhan, desain jaringan logika, desain jaringan fisik, implementasi, pengujian, dan pemeliharaan. Dalam penelitian ini menggunakan metode *PPDIOO* karena dengan kebutuhan layanan jaringan yang semakin lengkap, maka dibutuhkan suatu metodologi yang mendukung perancangan arsitektur serta disain jaringan. Oleh karena itu, pada penelitian ini menggunakan *firewall* dan pengujian seperti tes *Ping*, *Tracert*, dan *Mail Server*. Hasil perancangan jaringan dan keamanan jaringan *firewall* di asrama mahasiswa J.C Oeavaang Oearay Kalimantan Barat berjalan dengan baik dan bisa dijadikan pedoman untuk diimplementasikan.

**Kata Kunci:** *Perancangan, Jaringan, Firewall, Top-Down*

# Pendahuluan

Pengaruh teknologi informasi sangat diperlukan oleh setiap orang untuk melakukan pekerjaan atau pembelajaran supaya kegiatan tersebut bisa lebih praktis. Pada saat ini teknologi tidak bisa terlepas dari seluruh aspek kehidupan manusia, terutama teknologi komputer. Jaringan komputer adalah suatu kumpulan beberapa komputer yang saling terkoneksi atau terhubung satu sama lainnya melalui perantara seperti *router*, *switch*, dan sebagainya. Jaringan mempunyai peranan penting untuk mendukung kelancaran serta mempermudah proses pengolahan dan pertukaran data.

Asrama Mahasiswa J.C Oeavaang Oearay Kalimantan Barat memiliki rancangan topologi jaringan *Wireless Local Area Network* (*WLAN*) yang sudah pernah dibuat sebelumnya menggunakan *Cisco Packet Tracer*. Rancangan tersebut untuk memudahkan kebutuhan seperti *media social*, *browsing*, dan *file sharing*. Namun topologi jaringan yang ada di Asrama Mahasiswa J.C Oeavaang Oearay Kalimantan Barat kurang efektif karena hanya memiliki keamanan jaringan menggunakan verifikasi *user* dan *password*. Oleh karena itu, pihak luar masih dapat mengakses jaringan tersebut karena terlalu rentan dengan pencurian data. Keamanan jaringan pada topologi sebelumnya harus dioptimalkan agar menghasilkan jaringan internet yang bagus. Maka peneliti memutuskan untuk membuat rancangan jaringan baru dengan menggunakan penerapan *firewall* untuk membatasi hak akses berdasarkan *IP Address* perangkat di Asrama Mahasiswa J.C Oeavaang Oearay Kalimantan Barat.

Penilitian yang membahas tentang Penerapan Metode *Top-Down* dalam Pengembangan Jaringan Komputer Lokal Perusahaan menyimpulkan bahwa keamanan jaringan dibangun untuk mengamankan seluruh informasi yang bersifat rahasia dan juga mengamankan akses perangkat jaringan dari pihak lain. Dengan dirancangnya keamanan jaringan, maka setiap aliran data yang rahasia tidak bisa diakses oleh sembarang orang. Pengamanan dilakukan menggunakan *firewall* dan *web proxy* pada jaringan. Hasil pengujian jaringan didapatkan bahwa *block* akses *router* dilakukan dengan membatasi semua *user* untuk mengakses ke *router* melalui *web browser* [1]*.*

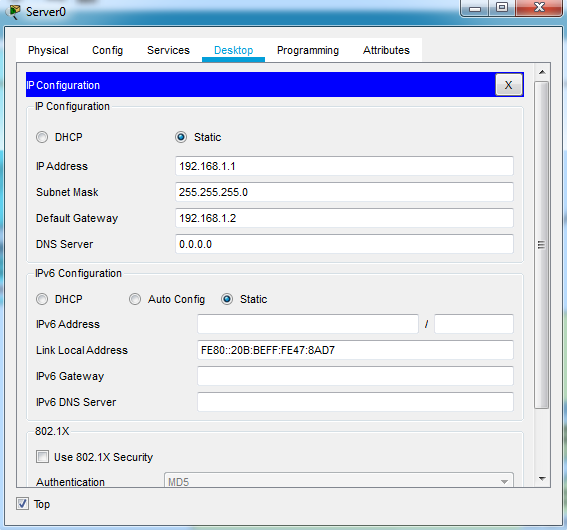
Penelitian yang membahas tentang Perancangan dan Implementas Sistem Keamanan Jaringan menggunakan *Firewall* dan *Web Proxy* Berbasis Mikrotik di SMA Negeri 1 Kota Sukabumi menyimpulkan bahwa Pemfilteran paket data pada lalu lintas jaringan memakai *firewall* dan *web proxy* secara efektif bergantung pada topologi jaringan serta konfigurasi dasar yang diterapkan. Hasil uji tes didapatkan bahwa *firewall* dan *web proxy* sudah berhasil mencatat alamat IP yang mencoba memasuki sistem kedalam *address-list* serta menolak koneksinya, sehingga menerapkan aturan pada *firewall* dan *web proxy* sudah bisa mengamankan jaringan [2].

Penelitian yang membahas tentang Perancangan Security Hak Akses dan Firewall pada Topologi Jaringan menyimpulkan bahwa keamanan jaringan wajib diperhatikan seperti mengendalikan akses pada jaringan kita, bukan sekedar mengontrol siapa saja yang boleh mengakses jaringan. Pengontrolan akses ini juga mengatur bagaimana subjek yang berupa *user*, *program*, *file*, *komputer*, serta objek yang berupa *database* dan infrastruktur pada jaringan. Jika pada jaringan tidak terdapat pembatasan hak akses maka *user* dengan praktis masuk ke dalam *server*. Dengan menggunakan *firewall* pada jaringan bisa dilakukan dengan mengatur bagian *inbound* dan *outbound* pada *windows*. Hasil dari penelitian membuktikan bahwa jaringan terhubung baik dan mempunyai hak akses yang sudah diberikan dalam setiap komputer [3].

Penelitian yang membahas tentang Implementasi Sistem Keamanan Jaringan menggunakan Firewall Security Port pada Vita Multi Oxygen menyimpulkan bahwa kebutuhan informasi jaringan komputer begitu penting terutama administrator Keamanan jaringan komputer menggunakan pemberian *default*/ *static* *port* *security* (sebuah kemampuan *switch* untuk mendaftarkan serta membatasi perangkat yang bisa terkoneksi pada suatu *port*), *port security dynamic learning* (kemampuan *switch* untuk mengenali *mac* *address* secara dinamis saat perangkat komputer terhubung ke *switch* serta akan menyimpan *mac addre*ss tersebut ke *mac address table*), *sticky port security* (kemampuan *switch* dalam mengenal *mac address* di setiap perangkat yang terhubung serta akan memblokir *mac address* yang sudah terdaftar). Dengan *Security port*, maka sistem keamanan jaringan diterapkan lebih aman untuk menghidari koneksi jaringan dari akses yang tidak berkepentingan, serta menjaga data tersebut karena bisa dicuri oleh pihak yang tidak bertanggung jawab [4].

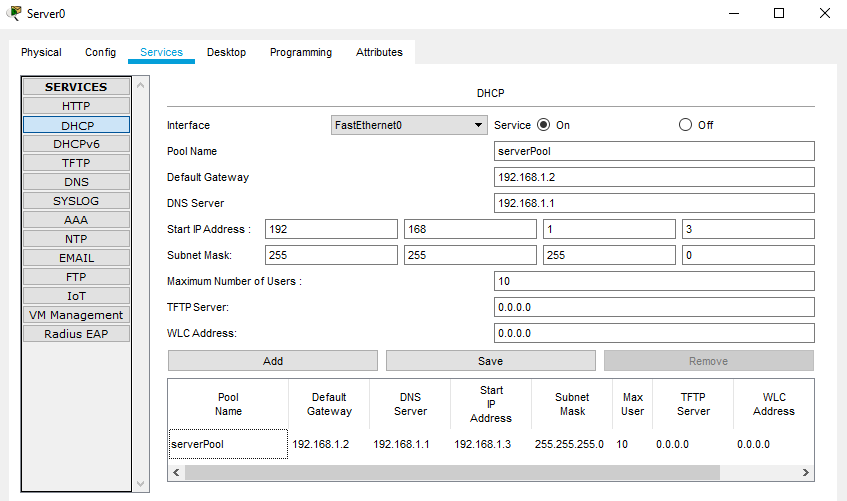
Penelitian yang membahas tentang Analisa Sistem Keamanan Jaringan Komputer Firewall menggunakan Shorewall pada PT. Indofarma Global Medika menyimpulkan bahwa *Packet filtering* melakukan pemeriksaan sederhana paket data, kemudian informasi yang ditemukan seperti nomor *port*, alamat *ip address* asal dan tujuan, juga informasi lainnya diperiksa tanpa melihat isi paket yang dikirim. Langkah terakhir jika paket informasi telah diperiksa tetapi tidak lulus inspeksi, maka paketnya akan dibuang. *Client* saat mengirim paket data ke komputer *server* (*firewall*), sistem *firewall* akan mencari komputer asal dan komputer tujuan, lalu mencari aturan dirules, di cek actionnya apakah *ACCEPT*, *DROP*, serta *REJECT*, kemudian di tampilkan sesuai action yang ditemukan [5].

# HASIL



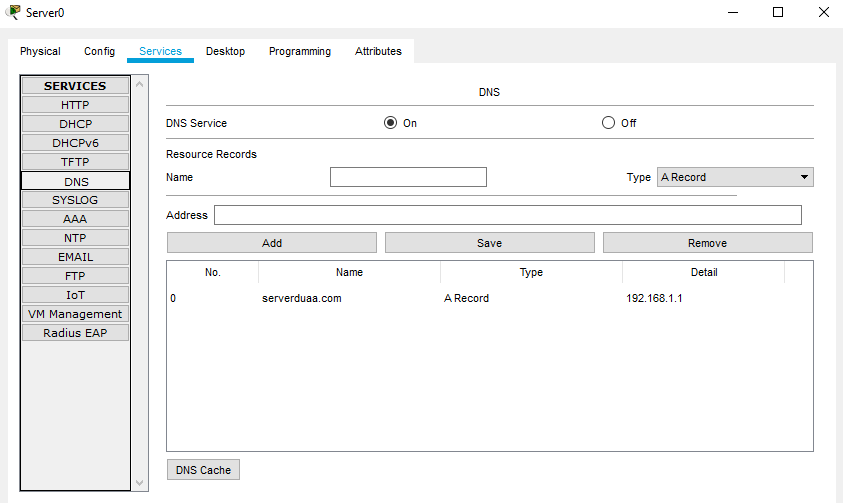
Gambar 1 Konfigurasi Server

Gambar 1 adalah tampilan pada bagian konfigurasi *Server*. Langkah pertama klik perangkat *Server* dan pilih menu *Dekstop*, kemudian pilih menu *IP* *Configuration*. Untuk *Server* menggunakan *IP* *Address* 192.168.1.1, *Subnet* *Mask* 255.255.255.0, *Default* *Gateway* 192.168.1.2, dan *DNS* *Server* 0.0.0.0.



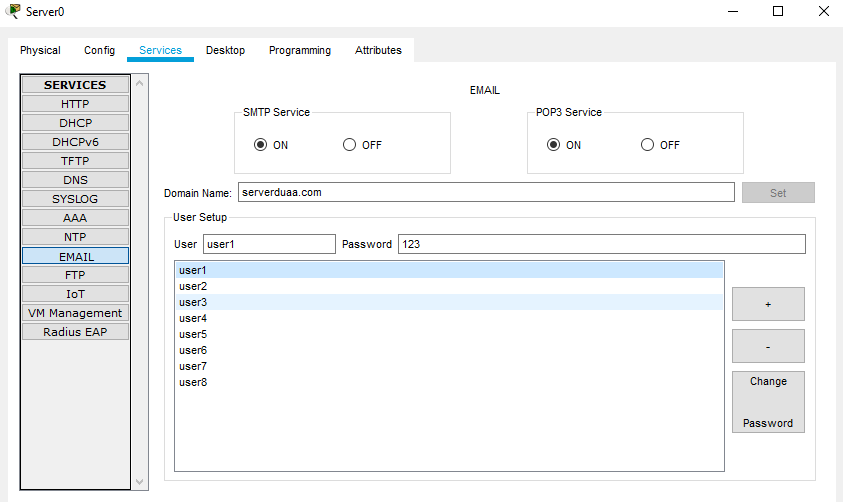
Gambar 2 Konfigurasi DHCP Server

Gambar 2 adalah tampilan pada bagian konfigurasi *DHCP* *Server*. Langkah pertama klik perangkat *Server* dan pilih menu *Services*, kemudian pilih menu *DHCP*. Pada *Server* menggunakan *DHCP* yang membatasi jumlah pengguna sebanyak 10 *user* mulai dari *IP* *Address* 192.168.1.3 sampai 192.168.1.12.



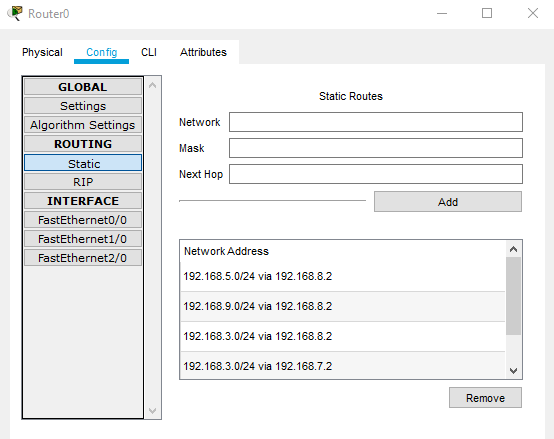
Gambar 3 Konfigurasi DNS Server

Gambar 3 adalah tampilan pada bagian konfigurasi *DNS* *Server*. Langkah pertama klik perangkat *Server* dan pilih menu *Services*, kemudian pilih menu *DNS*. Aktifkan *DNS Services* dengan mengklik *on*, kemudian isi *DNS Name* dan *IP Address* yang digunakan. Pada gambar diatas peneliti mengisikan nama *serverduaa.com* dan *IP Address* 192.168.1.1.



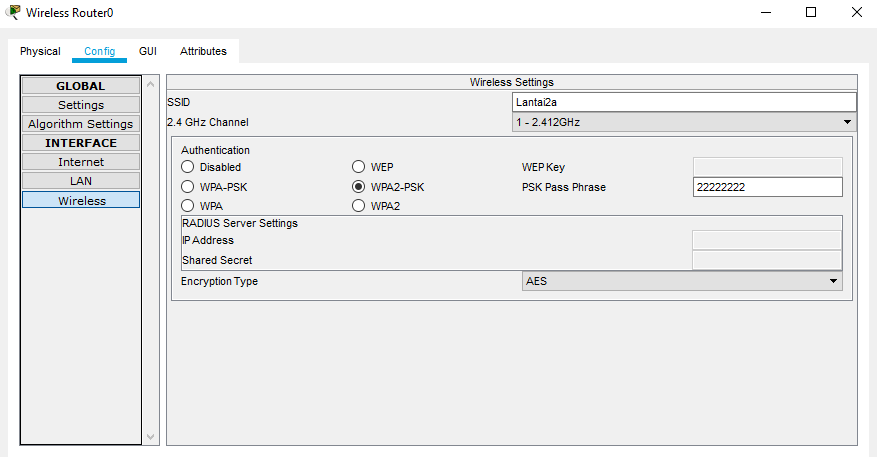
Gambar 4 Konfigurasi Mail Server

Gambar 4 adalah tampilan pada bagian konfigurasi *Mail* *Server*. Langkah pertama klik perangkat *Server* dan pilih menu *Services*, kemudian pilih menu *Email*. Aktifkan *Mail Server* dengan mengklik *on* pada *SMTP* *Service* dan *POP3* *Service*, biasanya secara *default* sudah aktif. Isi *domain* *name* dengan *serverduaa.com* sesuai yang diisi pada *DNS Server* lalu klik *set*, kemudian isikan *username* dan *password*. Gambar diatas peneliti mengisikan 8 *username* dan *password* karena di *Server0* memiliki 8 pengguna yang terhubung.



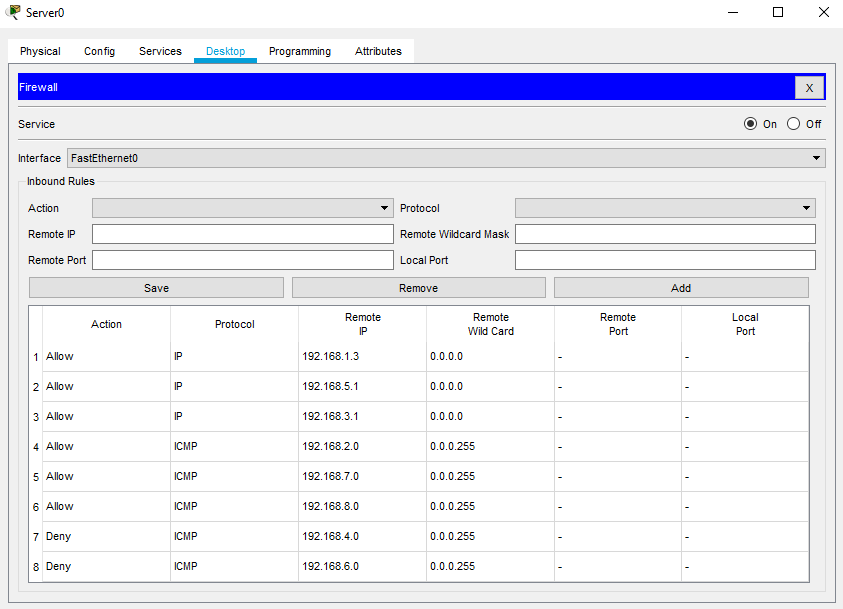
Gambar 5 Konfigurasi Router

Gambar 6 adalah tampilan pada bagian konfigurasi *Router* denganmenggunakan *static routing*. Langkah pertama klik perangkat *Router* dan pilih menu *Config*, kemudian pilih menu *Routing* dan *Static*. *Gateway* bisa berupa *next* *hop* (*ip address* pada *router* selanjutnya yang akan dilewati paket) seperti 192.168.5.0 melalui *router* 192.168.8.2, 192.168.9.0 melalui *router* 192.168.8.2, 192.168.3.0 melalui *router* 192.168.8.2, dan 192.168.3.0 melalui *router* 192.168.7.2.



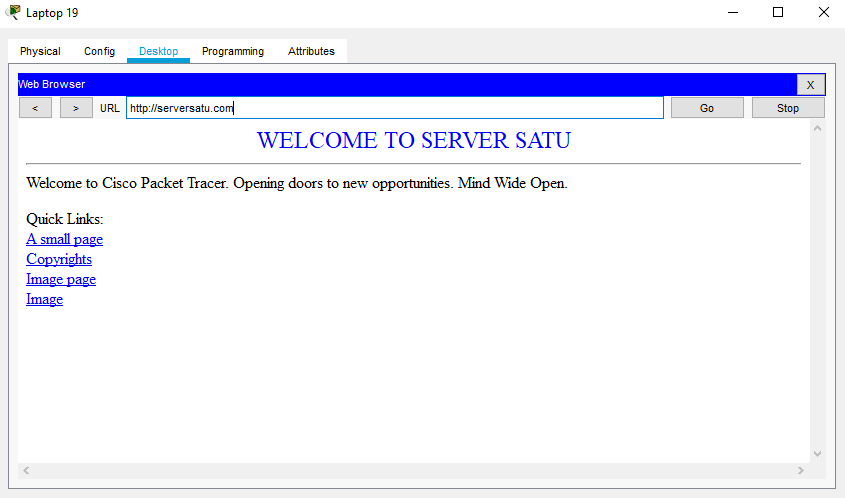
Gambar 6 Konfigurasi Access Point

Gambar 6 adalah tampilan pada bagian konfigurasi *Access Point0.* Langkah pertama klik perangkat *Access Point* dan pilih menu *Config*, kemudian pilih menu *Wireless*. *SSID* diberikan nama Lantai2a dan menggunakan keamanan *WPA2-PSK* dengan *password* 22222222.



Gambar 7 Konfigurasi Firewall Server

Gambar 7 adalah tampilan pada bagian konfigurasi *firewall Server.* Langkah pertama klik perangkat *Server* dan pilih menu *Dekstop*, kemudian ke menu *Firewall IPv4*. Pada gambar diatas kita memberikan akses kepada *Access Point0* dengan *IP* 192.168.1.3, *Server2* dengan *IP* 192.168.5.1, *Server1* dengan *IP* 192.168.3.1, dan lainnya. Kita juga melakukan pemblokiran akses kepada semua *user* di lantai 2b dengan *IP address* 192.168.4.0 dan juga *user* di lantai 1 dengan *IP* *address* 192.168.6.0.

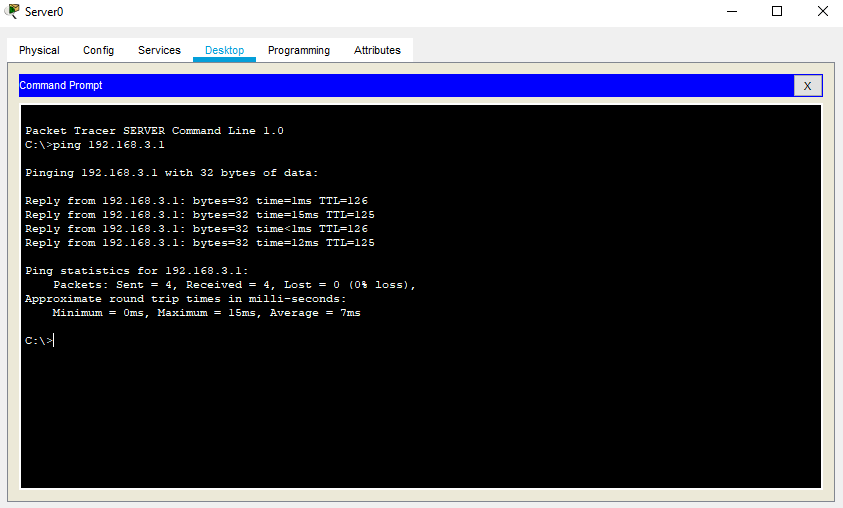


Gambar 8 Tampilan Web Browser

Gambar 8 adalah tampilan hasil *web browser* dengan menggunakan laptop yang sudah terhubung ke jaringan, disini *user* mengakses *website* dengan mengetikkan alamat pada *URL* di *address bar* pada peramban *website*. *Web browser* secara otomatis menerima permintaan *user* dan menjalankan pengambilan data pada *DNS Server*, kemudian *web* *browser* dapat mengakses *server* tujuan menggunakan *IP* yang diperoleh dari *DNS Server*. *Server* memberikan data dari konten dalam bentuk *HTML* atau file lainnya dan peramban *web* menampilkan beragam konten sesuai permintaan pengguna. Gambar diatas peneliti mengakses *website* dari *serversatu.com* dan menampilkan isi yang ada pada *website* tersebut.

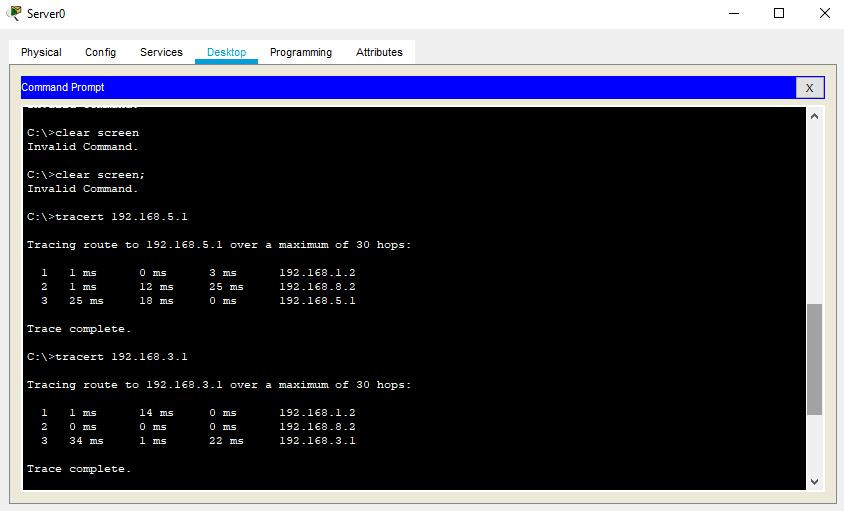
# PEMBAHASAN

Pembangunan jaringan ini dibuat dengan melakukan analisa terlebih dahulu karena sangat dibutuhkan untuk mendefinisikan masalah yang ada dan mengamati kebutuhan jaringan secara keseluruhan. Pembangunan jaringan ini membutuhkan suatu analisis yang benar agar jaringan yang dibuat sesuai dengan yang diharapkan di Asrama Mahasiswa J.C Oeavaang Oearay Kalimantan Barat. Adapun perangkat jaringan yang dibutuhkan dalam membangun jaringan di asrama yaitu 3 *Server*, 3 *Router*, 3 *Switch*, 3 *Access Point*, *Crimping Tools*, *Roll* kabel UTP, *Konektor RJ-45*, dan tester kabel.



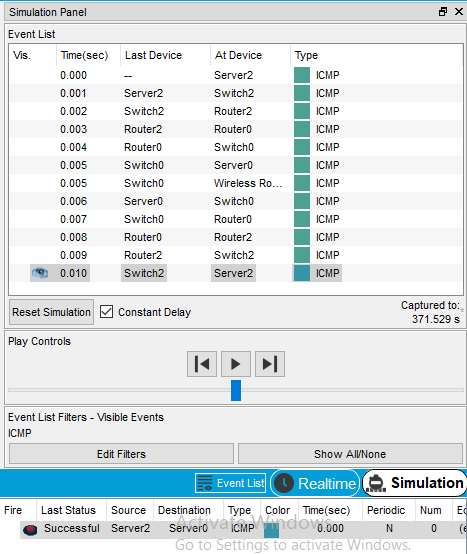
Gambar 9 Hasil Pengujian Tes Ping

Gambar 9 adalah tampilan kita melakukan uji coba konektivitas untuk mengetahui apakah sudah terhubung atau tidak dengan tes *ping*. Gambar diatas kita melakukan tes *ping* dari *Server0* ke *Server1* dengan menggunakan *IP address* 192.168.3.1. Hasil yang kita dapat berupa data-data seperti paket yang dikirim sebesar 4, paket yang diterima berjumlah 4, paket yang hilang berjumlah 0, dan mendapatkan *round trip time* sebesar 7ms.



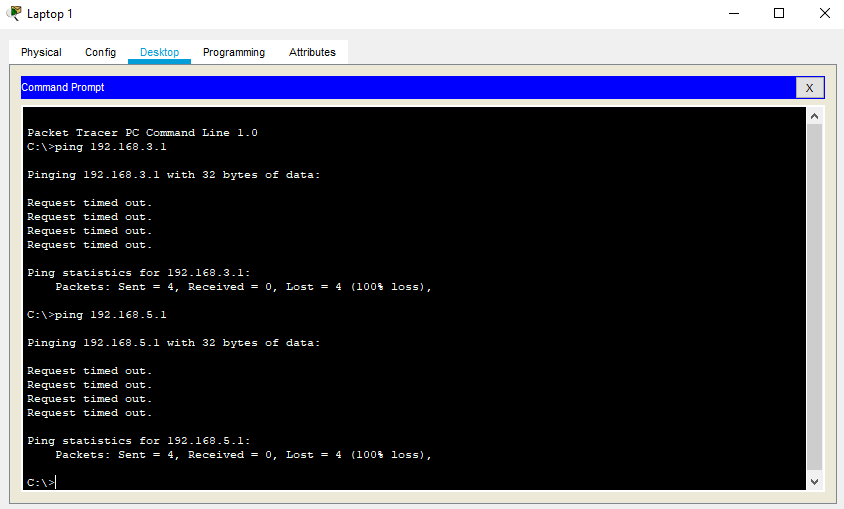
Gambar 10 Hasil Pengujian Tracert

Gambar 10 adalah tampilan kita melakukan uji coba *tracert* yaitu dengan melakukan pelacakan pada jalur perjalanan paket jaringan yang digunakan. Dari gambar diatas kita melakukan 2 percobaan dengan mengirimkan data dari *Server0* dikirim ke *Server1* dan *Server2*. Percobaan pertama kita mengirimkan paket data ke *Server1* dengan melewati jalur *Router0* 192.168.1.2 kemudian melalui *Router1* 192.168.7.2 dan sampai ke *Server1* 192.168.3.1. Percobaan kedua kita mengirimkan paket data ke *Server2* dengan melewati jalur *Router0* 192.168.1.2 kemudian melalui *Router2* 192.168.8.2 dan sampai ke *Server2* 192.168.3.1.



Gambar 11 Hasil Pengujian Simulasi

Gambar 11 adalah tampilan kita melakukan uji coba menggunakan simulasi dengan tipe *ICMP* (*Internet Control Message Protocol*) yaitu seperti *tracert* yang melakukan pelacakan pada jalur perjalanan paket jaringan yang digunakan, namun simulasi ini lebih detail daripada *tracert* melalui *command*. Pada gambar diatas kita menguji pengiriman paket dari *Server2* ke *Server0* dengan melewati jalur yang sudah ditentukan menggunakan *static* *routing*. Pertama paket dikirim dari *Server2* yang melewati *Switch2*, *Router2*, *Router0*, *Switch0*, dan paket akan sampai ke *Server0*. Paket yang telah diterima *Server0* akan diperiksa, kemudian paket akan dikirim kembali melalui jalur yang sebelumnya sudah dilewati dan status pengiriman paket berhasil dilakukan.



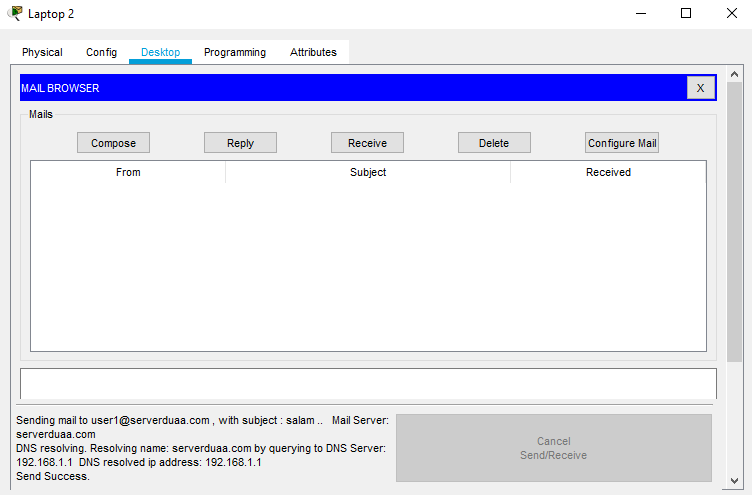
Gambar 12 Hasil Pengujian Firewall

Gambar 12 adalah tampilan kita melakukan uji coba *firewall* dengan menggunakan tes *ping*. Pada gambar diatas kita mencoba 2 pengujian menggunakan laptop yang ada pada jaringan lantai2a dengan melakukan *ping* ke *Server1* dengan *IP* 192.168.3.1 dan *Server2* dengan *IP* 192.168.5.1. Hasil dari pengujian ini berupa *RTO* (*Request Timed Out*) yang berarti *Server1* dan *Server2* berhasil memblokir *IP address* laptop.

Tabel 1 Pengujian Firewall dari PING

|  |  |  |  |
| --- | --- | --- | --- |
| Percobaan  Firewall | Komputer Asal | Komputer Tujuan | Keterangan |
| Lantai 2A | Server 0 | Server 1 | Bisa |
| Server 2 | Bisa |
| Laptop 1 | Server 0 | Bisa |
| Lantai 2B | Laptop 9 | Server 0 | Tidak |
| Lantai 1 | Laptop 19 | Server 0 | Tidak |
| Lantai 2B | Server 1 | Server 0 | Bisa |
| Server 2 | Bisa |
| Laptop 10 | Server 1 | Bisa |
| Lantai 2A | Laptop 2 | Server 1 | Tidak |
| Lantai 1 | Laptop 19 | Server 1 | Tidak |
| Lantai 1 | Server 2 | Server 0 | Bisa |
| Server 1 | Bisa |
| Laptop 19 | Server 2 | Bisa |
| Lantai 2A | Laptop 3 | Server 2 | Tidak |
| Lantai 2B | Laptop 11 | Server 2 | Tidak |

Penjelasan dari tabel IV.3 dimana pada simulasi keamanan *firewall* ini dilakukan dengan tes *ping*. Dari pengujian *firewall* yang mempunyai akses untuk masuk ke *server* diberikan keterangan “Bisa”, sedangkan yang tidak mempunyai akses diberikan keterangan “Tidak”. *Server* yang ada di lantai 1 dan lantai 2 saling terhubung agar dapat melakukan pertukaran dan penyimpanan data, kemudian *server* mengamankan data-data tersebut dari pengguna lain dan pihak luar. Laptop yang ada di lantai masing-masing hanya bisa terhubung ke *server* di lantai tersebut dan tidak bisa terhubung dengan *server* luar.



Gambar 13 Hasil Pengiriman Email

Gambar 13 adalah tampilan kita melakukan uji coba pengiriman *mail* dari setiap pengguna, seperti gambar diatas mencoba mengirimkan pesan dari *user* 2 ke *user* 1. Langkah pertama pilih menu *Compose* dan mengisi *email* penerima, subjek, pesan, dan tekan tombol *send* jika ingin mengirim pesan. Pesan yang sudah terkirim akan mendapatkan keterangan dibawah yaitu *Send Success*.

# KESIMPULAN

Berdasarkan penelitian yang telah dilakukan maka didapat hasil dari pembuatan rancangan jaringan dan keamanan *Firewall Packet Filtering* menggunakan metode *Top-Down* di Asrama J.C Oeavaang Oearay dapat diambil kesimpulan sebagai berikut:

1. Jaringan baru yang didesain dan dirancang ini dapat membantu dengan baik sebagai salah satu kebutuhan di asrama.
2. Penerapan jaringan ini dapat memberikan informasi yang cepat, pengolahan data yang akurat, dan juga keamanan yang cukup terjaga.
3. Rancangan ini sudah cukup bagus untuk diimplementasikan, dapat dilihat dari berbagai hasil pengujian.
4. Jaringan masih bisa terhubung ketika satu kabel ada yang terputus koneksinya dengan menggunakan *router* *backup*.

# SARAN

Setelah melakukan penelitian pembuatan rancangan jaringan dan keamanan *Firewall Packet Filtering* menggunakan metode *Top-Down* di Asrama J.C Oeavaang Oearay Kalimantan Barat, terdapat beberapa saran seperti berikut ini:

1. Diharapkan rancangan jaringan ini dapat diimplementasikan di Asrama Mahasiswa J.C Oeavaang Oearay Kalimantan Barat.
2. Diharapkan pada penelitian selanjutnya dapat menggunakan pengujian pengiriman paket secara berlebihan (*spamming*).
3. Penelitian selanjutnya dapat menyederhanakan rancangan yang dibuat supaya tidak membutuhkan banyak biaya ketika diimplementasikan di Asrama Mahasiswa J.C Oeavaang Oearay Kalimantan Barat.
4. Penelitan selanjutnya diharapkan pengujian *tracert* dalam pengiriman paket dapat memilih jalur terdekat atau tercepat agar bisa sampai ke tujuan.

# DAFTAR PUSTAKA

|  |  |
| --- | --- |
| [1] | M. Syahrizal, Pengantar Jaringan Komputer, Yogyakarta: C.V. ANDI OFFSET, 2020. |
| [2] | G. T. Irawan, M. Djaohar and M. F. Duskarnaen, "Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan Web Proxy Berbasis Mikrotik di SMA Negeri 1 Kota Sukabumi," *PINTER: Jurnal Pendidikan Teknik Informatika dan Komputer,* pp. 27-32, 2018. |
| [3] | A. Darmianto, Yanto and Kartono, "PERANCANGAN SECURITY HAK AKSES DAN FIREWALL PADA TOPOLOGI JARINGAN," *INTEKSIS,* pp. 66-73, 2017. |
| [4] | R. Ocanitra and M. Ryansyah, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen," *JUSTIN (Jurnal Sistem dan Teknologi Informasi),* pp. 52-59, 2019. |
| [5] | Y. Yanti and R. Effendi, "Analisa Sistem Keamanan Jaringan Komputer Firewall Menggunakan Shorewall Pada PT. Indofarma Global Medika," *Jurnal TEKSAGRO,* pp. 14-21, 2020. |