Analisa Sistem Keamanan Jaringan Komputer *Firewall* Menggunakan *Shorewall* Pada PT. Indofarma Global Medika

Computer Network Security System Analysis Firewall Using Shorewall At PT. Indofarma Global Medika

Yeni Yanti[1,*], Rolan Effendi[2]
[1]Fakultas Teknik Program Studi Teknik Informatikan Universitas Serambi Mekkah, Jl. Teungku Imum Lueng Bata, Banda Aceh. Indonesia. 23245

*Email: yeniyanti@serambimekkah.ac.id

Tanggal Submisi: 01 Desember 2020, Tanggal Penerimaan: 09 Desember 2020

Abstrak

Kemajuan teknologi khususnya jaringan komputer sangat membantu di bidang informasi dan pengolahan data informasi yang diinginkan tanpa keterbatasan ruang dan waktu dengan menggunakan secara maksimal, sistem komputer dalam jaringan komputer yang terintegrasi akan didapatkan informasi data dengan cepat dan tepat. PT. Indofarma Global Medika (PT. IGM) memiliki jaringan distribusi, informasi-informasi atau integritas data yang penting untuk di lindungi. Untuk mencegah orang lain dalam mengakses informasi atau integritas data tersebut di perlukan suatu keamanan jaringan komputer bertujuan agar sistem informasi selalu aman. Pada penelitian ini melakukan pengujian *ACCEPT*, *DROP* dan *REJECT* menggunakan metode *firewall* dalam pengamatan jaringan komputer pada *shorewall* yang terdapat dikomputer *server*, guna untuk menjaga informasi atau integritas data yang ada dengan cara membatasi izin akses jaringan yang masuk pada komputer *server*. Adapun hasilnya dalam pengujian *DROP*, semua komputer *client* juga tidak bisa melakukan pengiriman paket *ping* ke *server* tetapi, setiap paket yang memiliki kebijakan *reject* ini *firewall* akan mengirimkan pesan *ICMP error* kepada si pengirim paket.

Kata Kunci: Jaringan Komputer, Keamanan Jaringan, *Linux*, *Firewall*, *Shorewall*

Abstract

Advances in technology, especially computer networks are very helpful in the field of information and processing of desired information data without limited space and time by using the maximum, computer systems in an integrated computer network will be obtained data information quickly and precisely. Pt. Indofarma Global Medika (PT. IGM) has a distribution network, information or data integrity that is important to protect. To prevent others from accessing the information or integrity of the data is necessary a computer network security aims to keep the information system always safe. In this study conducted ACCEPT, DROP and REJECT testing using firewall method in computer network observation on shorewall contained in server computer, in order to maintain information or integrity of existing data by limiting access permissions of incoming network on server computer. As for the results in drop testing, all client computers also can not send ping

packages to the server but, any package that has this reject firewall policy will send an ICMP error message to the sender of the package.

Keywords: Computer Networking, Network Security, Linux, Firewall, Shorewall

PENDAHULUAN

PT. Indofarma Global Medika (PT. IGM) merupakan anak perusahaan PT. Indofarma (Persero), merupakan bagian dari perusahaan BUMN yang bergerak di bidang farmasi, alat kesehatan, dan makanan sehat. Seiring dengan meningkatnya kebutuhan masyarakat terhadap pelayanan kesehatan dan seiring dengan era teknologi dalam bidang kesehatan di Indonesia yang semakin berkembang, PT. IGM yang didukung oleh Tim Sales dan Marketing yang profesional, IT dan teknologi yang mengikuti perkembangan zaman, serta didukung adanya jaringan distribusi di seluruh Indonesia yang dimiliki, PT. IGM siap menjadi Partner Handal di Industri Kesehatan (*Reliable Partner in Healthcare Industry*).

Semakin besarnya jaringan distribusi yang di buat oleh administrator jaringan PT. IGM, maka keamanan jaringan PT. IGM menjadi prioritas penting bagi administrator agar sistem informasi terlindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak dimana usaha tersebut bisa dilakukan baik dari dalam maupun dari luar sistem (Yanti et al., 2017). Salah satu metode yang baik untuk keamanan jaringan adalah membuat sebuah *firewall*.

Firewall merupakan suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan. Paket data yang baik diperbolehkan untuk melewati jaringan dan paket data yang dianggap jahat tidak diperbolehkan melewati jaringan (Khoumsi et al., 2018). Dimana *Firewall* aplikasi *Linux* yang dibutuhkan untuk menjaga integritas data yang ada dari serangan-serangan *hacker* yang tidak bertanggung jawab dengan melakukan *filterisasi* terhadap paket-paket yang datang kepadanya (Gupta et al., 2004; Mustafa, 2016) . Dengan Sistem operasi *Linux* telah menyiapkan aplikasi untuk dijadikan sebuah *firewall* diantaranya *ipchains*, *iptables* dan *Shorewall* (Mhd. Dicky Syahputra Lubis & Allwine, 2018; Mustafa, 2016)

Penelitian oleh (Supendar et al., 2019), mendesain sebuah teknologi yang berbasis jaringan internet sebagai komunikasi antar cabang, teknologi atau yang disebut dengan *Voice Over Internet Protocol* (VoIP) yang merupakan sistem operasi open source dan firewall open source yang terdapat didalamnya Shorewall lalu dilakukan penginstallan dan pengetesan, firewall ini cukup handal dalam mengatasi suatu masalah yang terjadi oleh serangan jaringan. Untuk penelitian oleh (Mhd. Dicky Syahputra Lubis & Allwine, 2018), menggunakan sistem

operasi aplikasi Linux untuk digunakan firewall diantaranya ipchains, iptables dan Shorewall yang berfungsi untuk mengfilter paket data sudah dimasukkan dalam kernel dengan menggunakan protocol Telnex dalam proses pengiriman pesan ping.

Dalam penelitian ini akan di gunakan aplikasi *Shorewall* dari *Linux Debian Desktop*. *Shorewall* (*Shoreline Firewall*) merupakan salah satu *firewall* yang handal dan murah untuk digunakan di sistem operasi *Linux* selain *Ipchains* dan *Iptables*, *shorewall* juga mudah dikonfigurasi bagi penggunanya dan mengatur data yang diterima dan pengiriman data. Serta melakukan Ping pesan ICMP dalam proses Ping ACCEPT, DROP dan REJECT.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini dimulai dengan menelusuri teori-teori yang berkaitan dengan pemasalahan yang dibahas dalam penelitian ini melalui wawancara , diskusi terkait dengan keamanan jaringan komputer pada PT.IGM, buku, dan jurnal. Tahap kedua mendesai penelitian dengan merancang topologi jaringa ebuah komputer *server* menjadi *firewall* dengan menggunakkan *Shorewall*. lalu tahap ketiga melakukan perancangan (tiga) macam pengujian yaitu dengan pengiriman paket *ping ACCEPT, REJECT dan DROP* dengan menggunakan Internet Control Message Protocol (ICMP) yang kemudian dilakukan pengujian dengan menggunakan sistem operasi *Linux Debian* 10. Lalu ditahap melakukan proses analisis dari hasil pengujian dan yang terakhir mengumpulkan hasil keselurahan dalam sebuah laporan.

HASIL DAN PEMBAHASAN

Pada umumnya *firewall* menggunakan beberapa metode, pada penelitian ini metode yang penulis gunakan yaitu *packet filtering* alias penyaringan paket. *Packet filtering* ini melakukan pemeriksaan sederhana paket data. Kemudian, setelah itu informasi yang didapatkan seperti nomor *port*, alamat *ip* tujuan dan asal, juga informasi tingkat permukaan lainnya diperiksa tanpa membuka paket untuk memeriksa isinya. Langkah akhir adalah jika paket informasi tersebut setelah diperiksa tidak lulus inspeksi, maka paketnya akan dibuang terlihat pada Gambar.1.

Client saat mengirim paket data ke komputer *server(firewall)*, sistem *firewall* akan mencari komputer asal dan komputer tujuan, kemudian mencari aturan di *rules*, di cek *action*nya apakah *ACCEPT*, *DROP*, dan *REJECT*, lalu di tampilkan sesuai *action* yang ditemukan. Apabila tidak di temukan di *rules* maka sistem akan melakukan pencarian di *policy*. Adapun proses pengujian yang dilakukan dalam penelitian ini diantar

1. Pengujian Menggunakan Kebijakan *ACCEPT*

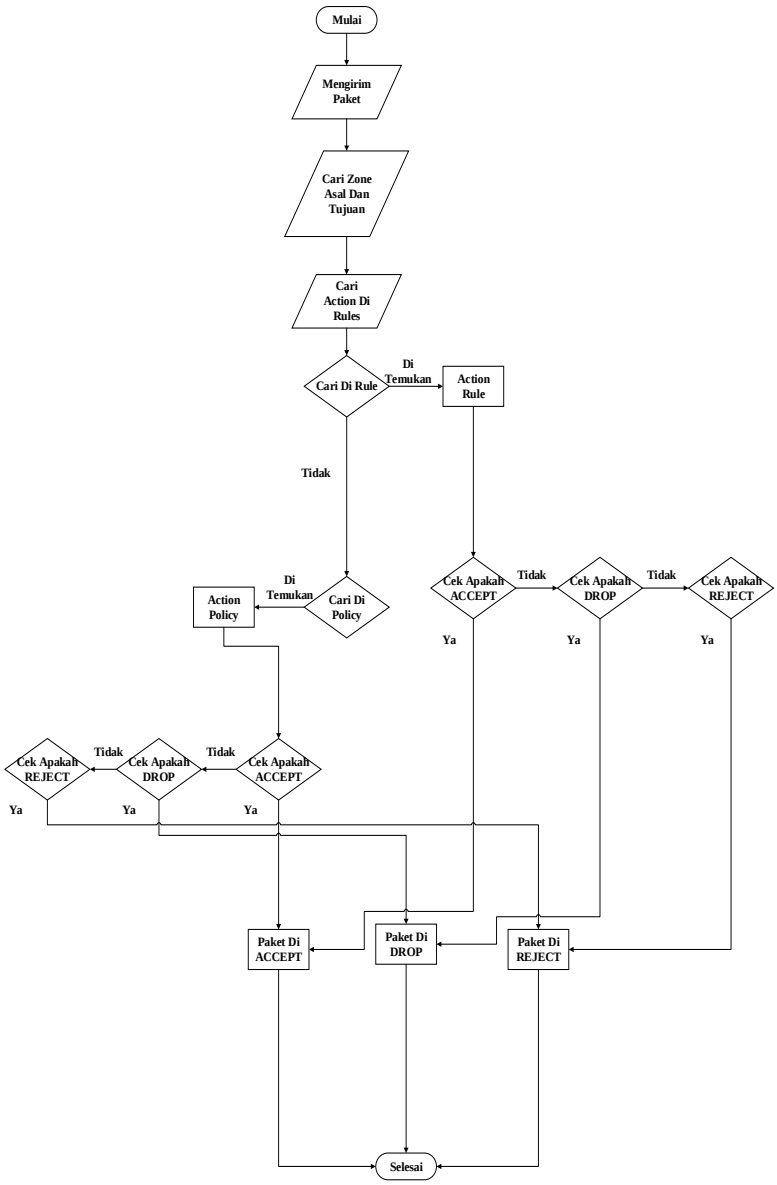
Pada kebijakan ini, semua komputer *client* melakukan pengiriman paket *ping* ke *server*, tapi setelah di konfigurasi pada *file rules* yaitu pada bagian ***Ping(ACCEPT) loc:192.168.43.77 $FW*** maka hanya komputer *client* yang memiliki *ip address* 192.168.43.77 yang bisa mengirim paket *ping* ke *server* (*Firewall*). Pada Gambar. 2, menunjukkan hasil pengujian *ACCEPT* pada komputer *client* yang memiliki *ip address* 192.168.43.77 mampu mengirimkan paket *ping* ke *server* (*Firewall*) dan untuk menambah komputer *client* yang diberi izin untuk mengirim paket *ping*, tinggal menambahkan di baris bawah konfigurasi sebelumnya pada *file rules* yaitu pada bagian ***Ping(ACCEPT) loc: $FW,*** untuk bagian *loc* masukkan *ip address* komputer *client* yang ingin di beri izin akses atau melakukan pengiriman paket *ping* terlihat pada Gambar 3.

2. Pengujian menggunakan *DROP*

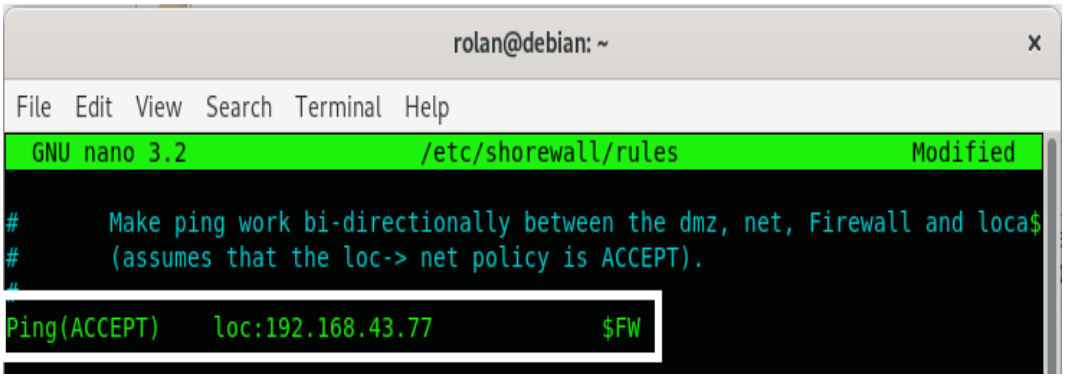
Pengujian DROP ip address 192.168.43.10 ini, hasilnya semua komputer *client* tidak bisa melakukan pengiriman paket *ping* ke *server*, karena *firewall* akan langsung ”membuang” setiap paket yang memiliki target ini tanpa mengirim pesan *error* kepada pengirim paket tersebut. Pada Gambar. 4, menunjukkan kebijakan *DROP*, yaitu pada pengujian ini semua komputer *client* tidak bisa mengirimkan paket *ping* ke *server* (*feriwall*). Terlihat pada Gambar.5.

3. Pengujian menggunakan *REJECT*

Sama dengan *DROP*, semua komputer *client* juga tidak bisa melakukan pengiriman paket *ping* ke *server* tetapi, setiap paket yang memiliki kebijakan *reject* ini *firewall* akan mengirimkan pesan *ICMP error* kepada si pengirim paket. Untuk melakukan konfigurasi *file rules* nya seperti pada Gambar.6, menunjukkan hasilnya pengujian *REJECT* ip address 192.168.43.118, yaitu sama seperti *DROP*, pengujian REJECT dikomputer *client* tidak bisa mengirimkan paket *ping* ke *server* (*firewall*), bedanya kalau kebijakan ini akan di kirimkan pesan *error* kepada komputer *client.* Secara *default, firewall* akan mengirimkan pesan *ICMP* berupa *port-unreachable* terlihat pada Gambar 7.

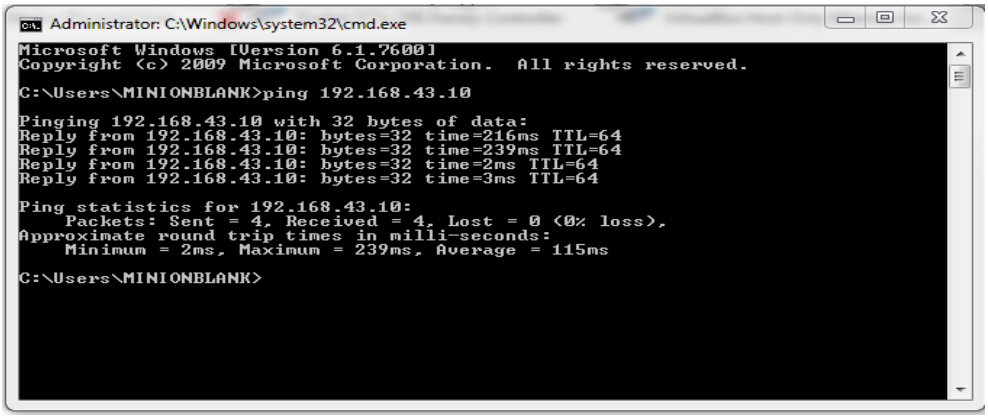


Gambar 1. *Flowchart Filtering Packet*

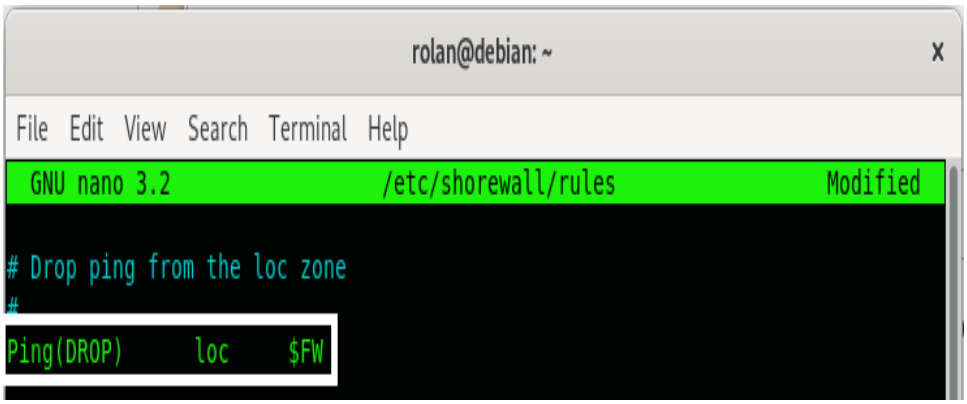


Gambar 2. Script Ping *ACCEPT*

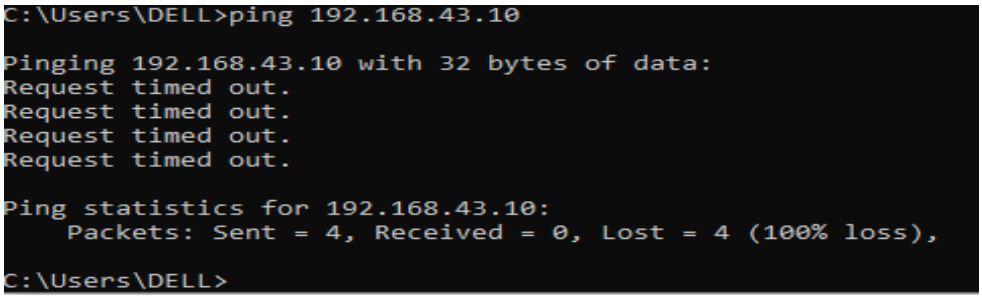
 e-ISSN 2723-6528



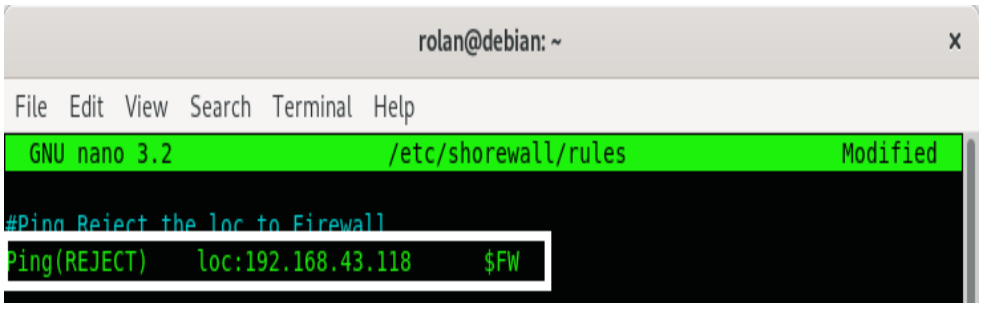
Gambar 3. Hasil Pengiriman Paket Ping *ACEEPT*



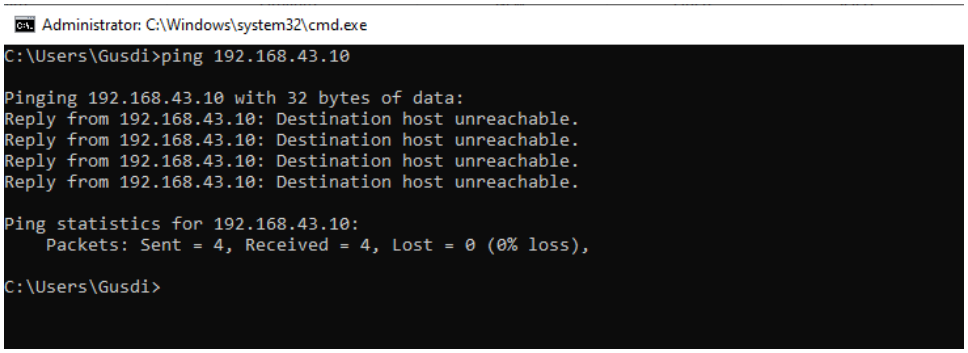
Gambar 4. Script ping drop



Gambar 5. Hasil Pengiriman Paket Ping *Drop*



Gambar 6. Script Ping *REJECT*



Gambar 7. Hasil Pengiriman Paket Ping *REJECT*

KESIMPULAN

Berdasarkan hasil penelitian diatas diperoleh kesimpulan semua komputer *client* juga tidak bisa melakukan pengiriman paket *ping* ke *server* tetapi, setiap paket yang memiliki kebijakan *reject* ini *firewall* akan mengirimkan pesan *ICMP error* kepada si pengirim paket dalam proses pengujian DROP.

SARAN

Dari hasil penelitian dan pengamatan sebelumnya, maka penulis mengemukakan pendapat yang dapat dimanfaatkan dan diteruskan oleh peneliti-peneliti selanjutnya yaitu Sesudah melakukan konfigurasi pada *file rules*, *shorewall* harus di *restart* terlebih dahulu agar konfigurasi tersebut dapat berjalan dengan baik sesuai dengan kebutuhan sistem. Selanjutnya perancangan *firewall* menggunakan *shorewall* ini semoga dapat terus di manfaatkan dan di kembangkan sehingga membawa hasil yang lebih baik kedepan.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada rekan-rekan yang telah mendukung akhirnya penelitian ini selesai dan tidak pula penulis mengucapkan terima kasih kepada PT. Indofarma Global Medika telah meberikan kesempatan penulis melakukan penelitian di perusahaan tersebut.

DAFTAR PUSTAKA

Gupta, V., Goswami, S., Ashok Kumar, A. K., & Singh, M. (2004). Networking and Security Measures. *DESIDOC Bulletin of Information Technology*, *24*(2), 9–16. https://doi.org/10.14429/dbit.24.2.3621

Khoumsi, A., Erradi, M., & Krombi, W. (2018). A formal basis for the design and analysis of firewall security policies. *Journal of King Saud University - Computer and Information*

Sciences, *30*(1), 51–66. https://doi.org/10.1016/j.jksuci.2016.11.008

Mhd. Dicky Syahputra Lubis, & Allwine. (2018). Membangun PCrouter Dengan UbuntuServer dan Keamanan Jaringan Dengan Shorewall. *Jurnal Armada Informatika*, *2*(1), 46–55. http://jurnal.stmikmethodistbinjai.ac.id

Supendar, H., Handrianto, Y., & Setiawan, S. (2019). Kualitas Pelayanan Dalam Voice Over Internet Protokol Berbasis Shorewall. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, *7*(2), 123–132. https://doi.org/10.33558/piksel.v7i2.1815

Yanti, Y., Arif, T. Y., & Munadi, R. (2017). Perancangan dan Penerapan Algoritme 4DES (Studi Kasus Pada Keamanan Berkas Rekam Medis). *Jurnal Rekayasa Elektrika*, *12*(3), 73. https://doi.org/10.17529/jre.v12i3.3271