
ANALISIS KEAMANAN JARINGAN KOMPUTER MENGUNAKAN SISTEM FIREWALL UNTUK MENCEGAH SERANGAN JARINGAN INTERNET DENGAN METODE NETWORK DEVELOPMENT LIFE CYCLE (Studi Kasus : PT. Mitra Servisindo Utama)

Endang Puji Rahayu¹, Hadi Zakaria²

^{1,2}Prodi Teknik Informatika, Fakultas Teknik, Universitas Pamulang
e-mail : ¹endangpr00@gmail.com, ²dosen00274@unpam.ac.id

ABSTRAK

Sistem keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, terutama di era teknologi sekarang ini karena banyak instansi yang tidak terlalu memperdulikan adanya masalah keamanan ketika jaringan mendapat serangan dan terjadi kerusakan sistem, maka banyak biaya yang harus dikeluarkan untuk memperbaiki sistem. Terlebih saat komputer server terhubung ke jaringan internet, maka serangan akan semakin meningkat dan berbagai macam teknik serangan jaringan terus berkembang. Mengatasi ancaman serangan jaringan internet terdapat dua teknik yaitu bisa menggunakan firewall dan metode Network Development Life Cycle (NDLC) untuk membantu keamanan jaringan dan membantu perencanaan pengembangan jaringan komputer perusahaan. Dengan menggunakan firewall dan metode Network Development Life Cycle, maka terbentuk perencanaan pengembangan terstruktur terhadap sistem keamanan jaringan komputer, sehingga akses yang dari luar tidak langsung masuk kedalam komputer. Adanya firewall keamanan sangatlah penting karena mampu mendeteksi serta melindungi dari beberapa serangan virus, malware, spam dan jenis lainnya. Dapat dikatakan bahwa firewall merupakan perangkat keras ntuk mencegah akses yang dianggap ilegal atau tidak sah dari jaringan pribadi (private network). Dari hasil penelitian ini diharapkan pada sistem firewall dengan metode Network Development Life Cycle (NDLC) dapat menghasilkan keamanan yang optimal untuk menjaga data perusahaan dari berbagai serangan virus, malware, spam dan hacker.

Kata kunci: Keamanan Jaringan, Firewall, Ancaman Serangan, Jaringan Internet dan NDLC

1. PENDAHULUAN

Keamanan jaringan merupakan hal sangat penting untuk diperhatikan terutama di era teknologi sekarang ini, karena banyak instansi yang tidak terlalu memperdulikan adanya masalah keamanan jaringan. Ketika jaringan komputer mendapat serangan virus, spam dan malware maka akan terjadi kerusakan data dan kerusakan sistem yang dapat mengakibatkan kerugian pada perusahaan. Untuk itu sudah seharusnya perusahaan melakukan investasi dibidang keamanan jaringan untuk mencegah kerusakan dari ancaman serangan yang semakin beragam.

PT. Mitra Servisindo Utama merupakan perusahaan yang bergerak dibidang jasa dan penjualan produk Bandwitdh Management dengan wilayah penjualan dan pekerjaan yang mencakup di beberapa daerah dalam kota maupun luar kota. Perusahaan ini memiliki banyak data penting dan sistem yang harus dijaga karena rawan akan ancaman serangan jaringan internet, maka dari itu dibutuhkan suatu pengembangan jaringan terstruktur dengan menggunakan perangkat pendukung dan metode yang tepat membantu menjaga keamanan data perusahaan.

Terjadinya kehilangan data dan kerusakan sistem pada PT. Mitra Servisindo Utama diakibatkan karena kurangnya perlindungan keamanan jaringan. Untuk itu peran firewall adalah untuk melindungi, mengawasi dan membatasi akses ilegal yang akan masuk kedalam jaringan internal perusahaan. Untuk itu dalam penelitian ini penulis membuat judul “ANALISIS KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SISTEM FIREWALL UNTUK MENCEGAH SERANGAN JARINGAN INTERNET DENGAN METODE NETWORK (Studi Kasus : PT. Mitra Servisindo Utama)”.

2. LANDASAN TEORI

- a. Penelitian yang dilakukan (Mohd 2015:5) dengan judul “Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Komputer Menggunakan Firewall”. Aktivitas ilegal dalam jaringan semakin berkembang ketika jaringan internet terhubung ke komputer server sehingga pengguna mengalami kesulitan dalam menjaga keamanan data perusahaan, dalam kasus ini pengguna diharuskan untuk mendeteksi adanya permasalahan aktivitas ilegal yang masuk ke dalam jaringan. Pada penelitian ini dibutuhkan suatu akses keamanan untuk mendeteksi dan mencegah aktivitas ilegal yang mau masuk ke dalam jaringan dan membantu pengguna jaringan tidak khawatir dengan serangan tersebut.
- b. Penelitian yang dilakukan (Fauzi dan Suartana 2017) dengan judul “Analisa Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Firewall”. Serangan packet sniffing pada jaringan wireless sangat berbahaya karena dapat merekam dengan baik ketika user melakukan aktivitas internet menggunakan protokol HTTP, berbeda ketika user menggunakan HTTPS dimana data aktivitas yang terekam pada firewall akan terenkripsi. Firewall yang digunakan untuk menganalisa dan mendeteksi serangan apabila menggunakan aplikasi ketika ada kegiatan yang mencurigakan terutama packet sniffing dengan indikasi arp spoofing.
- c. Penelitian yang dilakukan (Riska, R., & Alamsyah, H. 2021) dengan judul “Penerapan Sistem Keamanan Web Menggunakan Metode Web Application Firewall”. Mengamankan aplikasi web dapat dilakukan dengan memasang firewall, anti virus, atau software sejenis pada komputer ataupun router yang terhubung langsung atau berada dalam satu jaringan dengan server aplikasi web tersebut. Web application firewall adalah suatu metode untuk pengamanan pada aplikasi web yang berupaya mencegah adanya ancaman dari attacker ataupun hacker, Web application firewall sudah dapat bekerja terlebih dahulu tanpa melakukan konfigurasi tambahan pada server web sehingga tidak perlu lagi dilakukan perubahan atas script default aplikasi. Dalam bentuk pengujian pertahanan, akan dicoba disimulasikan dengan teknik serangan yang paling sering terjadi. Dengan sistem pertahanan ini, diharapkan dapat memberikan rekomendasi untuk meningkatkan segi keamanan, sehingga aplikasi web yang dibangun tidak hanya mempunyai desain yang baik namun juga terjaga integritas datanya.

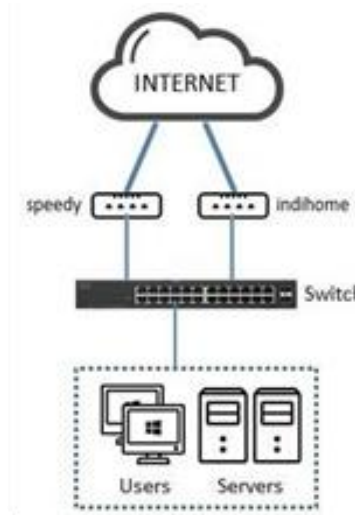
3. ANALISA SISTEM

Keamanan jaringan saat ini merupakan kewajiban dari suatu sistem yang harus dimiliki dan sangat penting untuk menjaga validitas dan integritas data bagi setiap penggunaannya. Sistem harus dilindungi dari segala macam ancaman serangan dan usaha peyusupan dari berbagai pihak yang tidak memiliki akses atau yang tidak memiliki otoritas. Proses analisa sistem pada jaringan sangat diperlukan untuk mensimulasikan tingkat keamanan pada suatu jaringan. Karena dengan analisa yang baik, maka diharapkan mampu mengidentifikasi celah keamanan sebaik mungkin. Dalam hal ini yang mendasari firewall sebagai alternatif dari sebuah sistem keamanan sekaligus sebagai media uji terhadap ancaman serangan. Perangkat firewall digunakan sebagai secondary sistem atau sistem yang berfungsi untuk melindungi sistem keamanan utama. Penelitian ini dilakukan menggunakan perangkat firewall dengan sistem operasi cOsCore dan Sistem Log yang

memiliki kemampuan untuk mencatat dan mendeteksi adanya penyusupan atau serangan terhadap jaringan.

a. Analisa Sistem Berjalan

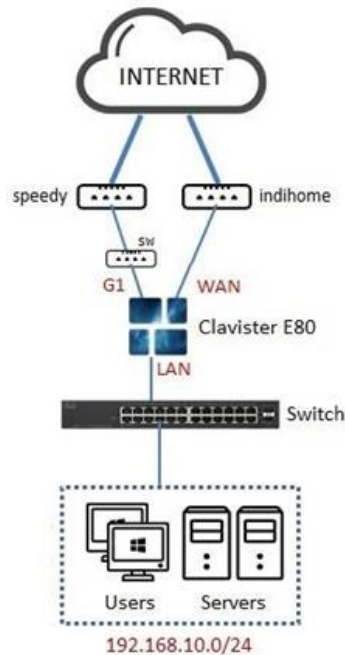
Proses simulasi jaringan, dari modem speedy dan indihome menyalurkan paket data ke switch untuk merubah jaringan public menjadi jaringan local dan di teruskan ke switch untuk menghubungkan dan menyebarkan paket data ke user.



Gambar 1. Skema Topologi Berjalan

b. Sistem Usulan

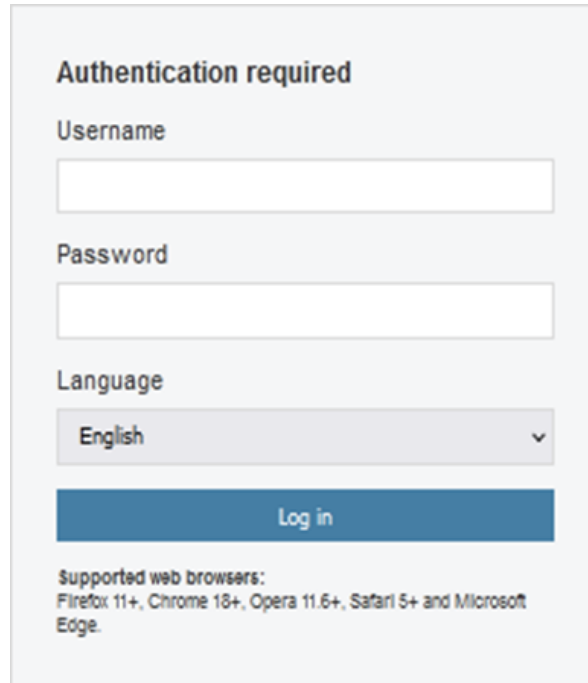
Proses simulasi jaringan, dari modem speedy dan indihome menyalurkan paket data ke firewall clavister untuk merubah jaringan public ke jaringan local dan di teruskan ke switch untuk menghubungkan dan menyebarkan paket data ke user dengan menggunakan keamanan khusus.



Gambar 2. Skema Topologi Berjalan

c. Perancangan Antarmuka (User Interface)

Dalam sistem keamanan jaringan ini diperlukan interface dalam penggunaannya, perancangan interface ini dilakukan untuk memberikan gambaran seperti tampilan sistem web gui pada calvsiter. Perancangan interface Tampilan Form Menu Login seperti gambar di bawah ini.



Authentication required

Username

Password

Language

English

Log in

Supported web browsers:
Firefox 11+, Chrome 18+, Opera 11.6+, Safari 5+ and Microsoft Edge.

Gambar 3. User Interface Login

Untuk Tampilan Menu Utama seperti gambar di bawah ini.



Gambar 4. User Interface Menu Utama

4. IMPLEMENTASI DAN PENGUJIAN

a. Spesifikasi Sistem

Spesifikasi sistem merupakan dokumen yang berfungsi menggambarkan fungsi dan kinerja sistem berbasis komputer yang akan di kembangkan, membatasi elemen – elemen sistem yang telah di alokasikan, serta memberi indikasi mengenai perangkat lunak dan konteks sistem keseluruhan dan informasi data control yang akan dimasukkan dan di keluarkan oleh sistem yang telah digambarkan dalam diagram aliran arsitektur.

b. Implementasi Antarmuka

Tahapan implemetasi adalah untuk menerapkan perancangan yang telah dilakukan terhadap sistem sehingga karyawan dapat melaporkan keluhan kerusakan software dan hardware. Implementasi antarmuka menggambarkan tampilan dari sistem yang sudah ada. Berikut ini adalah implementasi dari sistem web Grapichal User Interface (GUI) clavister. Tampilan Interface Address WAN & LAN seperti gambar di bawah ini.

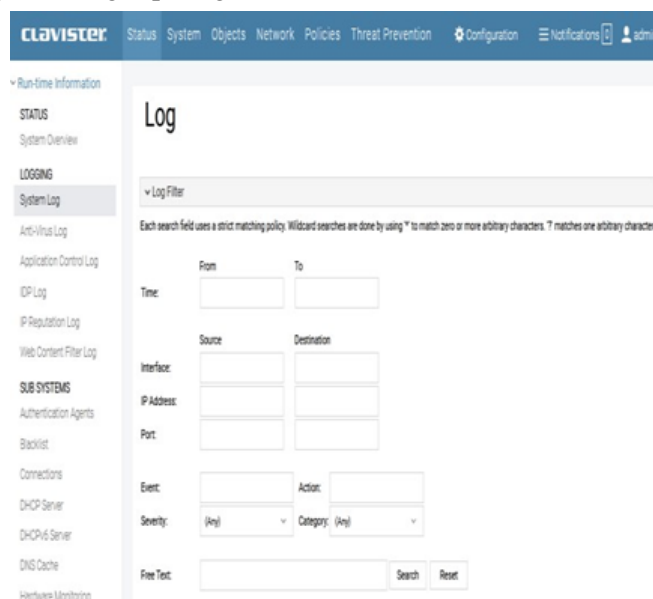


The screenshot shows a web interface titled "InterfaceAddresses" with a table listing network configurations. The table has columns for ID, Name, Address, Use Auth Group, and Comments. It lists configurations for WAN and LAN interfaces, including IP addresses, netmasks, default gateways, and DHCP server addresses.

ID	Name	Address	Use Auth Group	Comments
1	WAN_L1	192.168.30.2		IP address of interface WAN
2	WAN_M1	192.168.30.0/24		Netmask of interface WAN
3	WAN_G1	192.168.30.1		Default gateway for interface WAN
4	WAN_S1	8.8.8.8		Primary DNS server for interface WAN
5	WAN_S2	8.4.3.1		Secondary DNS server for interface WAN
6	LAN_L1	192.168.10.1		IP address of interface LAN
7	LAN_M1	192.168.10.0/24		Netmask of interface LAN
8	LAN_DHCP1	192.168.10.100-192.168.10.200		IP address pool for DHCP server on interface LAN

Gambar 5. Interface Address

Tampilan System Log seperti gambar di bawah ini.



Gambar 6. System Log

5. KESIMPULAN

Kesimpulan dari penelitian ini yaitu keamanan data perusahaan menjadi lebih aman dari berbagai ancaman serangan dan keamanan sistem perusahaan menjadi lebih optimal sehingga tidak mudah terserang virus maupun malware. Berdasarkan hasil responden, yang merupakan pihak perusahaan yang telah di berikan kuesioner tentang penggunaan sistem firewall sebagai keamanan data dan sistem perusahaan, dapat hasil bahwa 82% responden setuju, keamanan ini menggunakan firewall yang dapat melindungi, membatasi, ngawasi dan memblock akses yang di anggap ilegal.

DAFTAR PUSTAKA

- Giyono. (2016). Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada Pt Guna Karya Indonesia. *CKI On Spot*. 9(1). 2-4. <https://scholar.google.co.id>. Diakses 05 Februari 2020
- Husain, M.A. (2016). Analisis dan Pengembangan Sistem Keamana Jaringan LAN. Studi Kasus: SMPN 3 Baebunta. Skripsi Tidak Diterbitkan. Palopo : FTKOM-UNCP
- Krisianto, A. (2014). Internet untuk Pemula. Elex Media Komputindo. Jakarta
- Watchguard Firebox Pada Pt Guna Karya Indonesia. *CKI On Spot*. 9(1). 2-4. <https://scholar.google.co.id>. Diakses 05 Februari 2020
- Zakaria, Hadi., Sewaka., Udin Zailani, Achmad. (2020). Pengantar Teknologi Informasi. Tangerang Selatan: Unpam Press
- Zakaria, Hadi., Sewaka., Udin Zailani, Ahmad. (2021). Interaksi Manusia Dengan Komputer. Tangerang Selatan: Unpam Press