Pengembangan Rekayasa dan Teknologi, Vol 4, No. 2, November 2020, pp 87-97
p-ISSN: 1410-9840 & e-ISSN: 2580-8850
http://journals.usm.ac.id/index.php/jprt/index

APPLICATION GATEWAY DAN STATEFUL INSPECTION METHOD PADA IMPLEMENTASI *FIREWALL* UNTUK OPTIMASI KEAMANAN JARINGAN KOMPUTER

Vensy Vidya[1],Surono[2],Galih Setiarso[3]
[123]Jurusan Teknologi Informasi, Universitas Semarang
[1]vensyvidya@usm.ac.id,[2]surono@usm.ac.id,[3]galih@usm.ac.id

Abstaraksi

Firewall atau keamanan sangat di perlukan untuk jaringan internet pada saat ini dengan semakin berkembangnya teknologi internet dan semakin berkembangnya berbagai macam ancaman dari dunia maya entah itu virus maupun yang lainya firewall merupakan alat atau software keamana jaringan seperti pada hadware jaringan pada umumnya dan *firewall Application Gateway* ini sangat sesui diterapkan pada model jaringan internet dengan sekala menengah maupun sekala besar, suatu kampus dengan jaringan yang sangat luas dan besar sangat memerlukan *firewall* untuk keamana jaringan localnya.

Stateful pada *firewall* merupakan bagian penting untuk memfilter suatu paket ada yang di minta dan di kirim kepada penguna jaringan internet. Pada bagian ini sangat riskan terhadap serangan keamanan. Keamanan pada data di suatu instansi sangat di perlukan supaya mencegah kebocoran data kepada pihak pihak yang tidak bertanggung jawab serta penyalahgunaan data.

Serangan terhadap keamanan sistem informasi (*security attack*) dewasa ini seringkali terjadi. Kejahatan computer *(cyber crime*)pada dunia maya seringkali dilakukan oleh sekelompok orang yang ingin menenembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan

Kata kunci: *Firewall, Sistem Keamanan Jaringan, stateful, Application Gateway*

Abstract

Firewalls or security are very much needed for internet networks at this time with the development of internet technology and the development of various kinds of threats from cyberspace, whether viruses or others, firewalls are network security tools or software such as network hardware in general and this Application Gateway firewall. very suitable to be applied to the internet network model with medium scale or large scale, a campus with a very wide and large network really needs a firewall for the security of its local network. Stateful firewalls are an important part of filtering out a packet that is requested and sent to internet network users. This section is very risky for security attacks. Security in data in an agency is really needed in order to prevent data leakage to irresponsible parties and misuse of data.Attacks against information system security (security attacks) nowadays often occur. Cybercrime in cyberspace is often committed by a group of people who want to penetrate the security of a system. This activity aims to find, obtain, change, and even delete information on the system if it is really needed

Keywords: Firewall, Network Security System, stateful, Application Gateway

Pengembangan Rekayasa dan Teknologi, Vol 4, No. 2, November 2020, pp 87-97
p-ISSN: 1410-9840 & e-ISSN: 2580-8850
http://journals.usm.ac.id/index.php/jprt/index

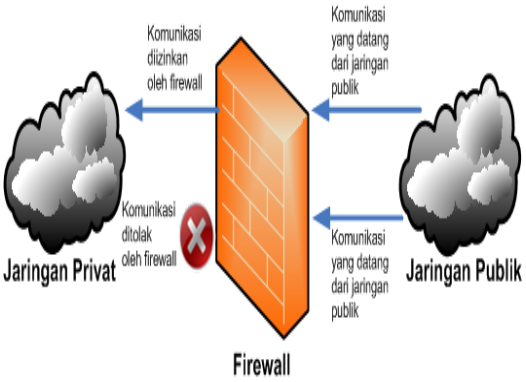
1. PENDAHULUAN

Firewall merupakan sebuah software maupun hadware yang diartikan sebagai sebuah perangkat lunak yang digunakan untuk memonitor dan membatasi akses antar jaringan internet , untuk membatasi hak akses dan keamnan di dalam dunia internet baik keamanan computer maupun keamanan jaringan yang dipenuhi oleh berbagai ancaan baik dalam maupun luar firewall merupakan solusi untuk mengatasi berbagai isu tersebut (Al-Shaer, 2014). Dengan suatu konfigurasi yang tepat pada firewall maka kemungkinan untuk mengamankan suatu data atau komputer pada jaringan menjadi jauh lebih aman (Hidayatulloh, 2014). Teknologi internet yang berkembang pesat saat ini merupakan suatu jaringan computer yang sangat besar ,raksasa,dan saling beriterakis di negara berkembang ataupun negara maju jaringan computer digunkan untuk memperlancar arus informasi di dalam pemerintahan maupun didalam swasta Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat. Ancaman dan serangan virus pun akan semakin gencar baik dari dalam maupun dari luar. Untuk mengurangi ancaman – ancaman tersebut perlu suatu konfigurasi firewall yang baik dan optimal(Adhi Purwaningrum, Purwanto, Agus Darmadi, Tri Mitra Karya Mandiri Blok Semper Jomin Baru, & -Karawang, 2018). Firewall sama dengan alat jaringan yang lainya yang berfungsi untuk mengkontrol akses antara jaringan internal dengan jaringan external (Pribadi, 2013).

Firewall atau keamanan sangat di perlukan untuk jaringan internet pada saat ini dengan semakin berkembangnya teknologi internet dan semakin berkembangnya berbagai macam ancaman dari dunia maya entah itu virus maupun yang lainya firewall merupakan alat atau software keamana jaringan yang sesui diterakan pada model jaringan internet dengan sekala menengah maupun sekala besar, suatu kampus dengan jaringan yang sangat luas dan besar sangat memerlukan firewall untuk keamana jaringan localnya

Dalam pengunaan jaringan perlu adanya sistem kontrol yang perlu di awasi supaya dalam maintance atau *upgrade software* dan *hardware* jaringan yang diperlukan tepat guna sistem gateway. *Gateway* bisa menjadikan jalan atau rute untuk menunjukan suatu tujuan dari suatu alamat pada jaringan internet dan gateway dapat berfungsi seperti atau layaknya router. Gateway juga dapat menghubungkan satu jaringan dengan jaringan lainnya meskipun setiap jaringan tersebut meniliki arsitektur dan pola topologi yang berbeda. Selain itu *gateway* dapat menghubungkan suatu jaringan komputer yang besar dengan jaringan yang besar lainnya, tidak hanya itu gateway juga bisa menghubungkan jaringan komputer yang besar dengan jaringan komputer yang lebih kecil. Istilah dari *gateway* biasanya tertuju kepada hardware atau software yang menghubungkan dua aplikasi atau jaringan yang tidak kompatibel, dan dapat mentransfer data yang berbeda beda. Contoh dari penggunaan gateway adalah email, dan email sendiri dapat mengirim data dengan sistem yang berbeda.

Serangan terhadap keamanan sistem informasi (*security attack*) dewasa ini seringkali terjadi. Kejahatan komputer (*cyber crime)*pada dunia maya seringkali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan(Sametinger, 2013) .



Gambar 1 .1 Komunikasi keamanan jaringan

Network Development Life Cycle (NDLC) digunakan sebagai metode dalam perancangan infrastruktur jaringan LAN karena sifatnya yang berkelanjutan. Tahapan NDLC yang digunakan yaitu *Analysis*, *Design* dan *Simulation Prototyping.* Metode ini selain untuk

sistem perangkat lunak akhir-akhir ini juga di di kembangan untuk pengembangan dalam pengunakan jaringan di sebuah instansi pemerintahan maupun instansi swasta(Ertie Nur Hartiwati, 2014). NDLC merupakan suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan. Metode ini mempunyai keuntungan yang bisa di kembangkan apabila di tengah jalan di rasa perlu untuk upgrade hardware maupun software yang di butuhkan. Dalam pengambangan suatu jaringan perlunya penghitungan yang tepat supaya dirasa segi budgeting maupun jumlah pengunaannya yang menjadi hal terpenting untuk transfer data dan pengamanan sistem dari serangan luar maupun dalam yang dapat kebocoran data maupun perusak sistem yang ada di dalamnya. Metode ini telah banyak di gunakan untuk beberapa topologi jaringan di pemerintahan maupun instansi pendidikan.

Stateful merupakan bagian metode dari filtering dalam firewall. Metode ini sangat sering di gunakan untuk memfilter paket data yang di minta dan di transfer dari sebuah router yang ada pada topologi jaringan internet yang tersedia. Selain untuk filtering paket data, *stateful* juga bisa di gunakan untuk melacak data yang di minta oleh seorang pengguna jaringan internet di suatu topologi jaringan(Lahmadi & Festor, 2009).

2. TINJAUAN PUSTAKA

Sebelum di laksanakannya penelitian ini, maka terdapat beberapa studi pustaka yang perlu di dalami secara lebih dalam untuk menambah pengetahuan dan informasi yang diperlukan. Beberapa pustaka tersebut meliputi keamanan jaringan, jenis serangan dan beberapa metode tentang firewall, dan penelitian terdahulu yang telah dilakukan mengenai pemantauan sumber daya *virtual server*.

2.1. Keamanan jaringan

Aspek penting dalam suatu jaringan internet bersekala besar ataupun berskala menegah adalah keaman, Keamanan jaringan sangat berperan dalam berlangsungnya suatu koneksi internet dlaam suatu jarngan local maupun interlocal, Akan tetapi masalah kemanan jaringan sering kali dia abaikan dalam suatu system informasi teknologi dan malahan tidak dianggap berperan dalam keperlangsungan suatu system informasi (Puspita et al., 2015). Terhubungnya suatu *Local Area Network* (LAN) atau komputer ke jaringan internet akan memberikan dampak membuka potensi adanya lubang keamanan yang tadinya bisa ditutup dengan mekanisme keamanan secara fisik. Jadi bisa kita asumsikan bahwa kemudahan mengakses suatu informasi berbanding terbalik dengan tingkay keamana sutu system itu sendiri. Keamanan informasi adalah bagaimana kita dapat mencegah penipuan atau mendeteksi adanya penipuan di sebuah sistem berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik (Wongkar et al., 2015). Keamanan jaringan menurut Mariusz Stawowski dalam jurnalnya "The principles of network security design", adalah Keamanan jaringan yang utama sebagai perlindungan sumber daya sistem terhadap ancaman yang berasal dari luar jaringan (Lin, Liu, Kuo, Chou, & Yang, 2008). Keamanan komputer digunakan untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Keamanan komputer yang dimaksud adalah keamanan sebuah komputer yang terhubung ke dalam sebuah jaringan (Internet).

2.2. Jenis Serangan Pada Komputer

Pada dasarnya, menurut jenisnya, serangan terhadap suatu data dalam suatu jaringan dapat dikategorikan menjadi 2, yaitu :

a. Serangan Pasif (Passive Attacks)

Serangan pasif adalah serangan pada sistem autentikasi yang tidak menyisipkan data pada aliran data (data stream), tetapi hanya mengamati atau memonitor pengiriman informasi ke tujuan. Informasi ini dapat digunakan di lain waktu oleh pihak yang tidak bertanggung jawab. Serangan pasif yang mengambil suatu unit data dan kemudian menggunakanya untuk memasuki sesi autentikasi dengan berpura-pura menjadi user autentik/ asli disebut dengan replay attack. Beberapa informasi autentikasi seperti password atau data biometric yang dikirim melalui transmisi elektronik dapat direkam dan kemudian

digunakan untuk memalsukan data yang sebenarnya. Serangan pasif ini sulit untuk dideteksi karena penyerang tidak melakukan perubahan data. Oleh sebab itu untuk mengatasi serangan pasif ini lebih ditekankan pada pencegahan daripada pendeteksiannya.

b. Serangan Aktif (Active Attacks)

Serangan aktif adalah serangan yang mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket-paket data yang salah ke data stream atau dengan memodifikasi paket-paket yang melewati data stream. Kebalikan dari serangan pasif, serangan aktif sulit untuk dicegah karena untuk melakukannya dibutuhkan perlindungan fisik untuk semua fasilitas komunikasi dan jalur-jalurnya setiap saat. Yang dapat dilakukan adalah mendeteksi dan memulihkan keadaan yang disebabkan oleh serangan ini.

2.3. **Model Osi**

Pengunaan model OSI terdapat 7 lapis proses standar untuk menjaga interoperabilitas antara peralatan yang dibuat oleh perusahan yang berbeda beda. model OSI ditetapkan oleh sebuah badan standar internasional yang bernama International Standards Organization (ISO) pada tahun 1947. Adapun ke 7 Lapis tersebut : Application layer, Presentation layer, Session layer, Transport layer, Network layer, Datalink layer dan Physical layer

2.4. **Protokol**

Protokol adalah sebuah standar aturan yang mengatur alat-alat dalam jaringan komputer sehingga dapat saling berkomunikasi satu sama lain, dapat berhubungan satu sama lain dan dapat melakukan perpindahan data satu sama lain. Protokol dapat diterapkan pada perangkat keras (hardware), perangkat lunak (software) dan kombinasi keduanya. Protokol adalah sebuah standar aturan yang mengatur alat-alat dalam jaringan komputer sehingga dapat saling berkomunikasi satu sama lain, dapat berhubungan satu sama lain dan dapat melakukan perpindahan data satu sama lain. Protokol dapat diterapkan pada perangkat keras (hardware), perangkat lunak (software) dan kombinasi keduanya

2.5. **Defisini firewall**

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan lingkupnya (Adhi Purwaningrum et al., 2018). Segmen tersebut dapat merupakan sebuah *workstation*, *server*, *router*, atau *Local Area Network* (LAN)

2.6. **Fungsi dan karateristik firewall**

Berdasarkan definisi diatas maka fungsi secara umum firewall sebagai berikut :

a. Mengatur dan mengontrol lalu lintas jaringan
b. Melakukan autentikasi terhadap akses
c. Melindungi sumber daya dalam jaringan privat
d. Mencatat semua kejadian, dan melaporkan kepada administrator

Selain mempunyai fungsi, pada dasarnya Firewall juga memiliki karateristik dalam pengunaannya atau dalam melakukan berkomunikasi. Karakteristik Firewall sebagai berikut (Adhi Purwaningrum et al., 2018):

a. Seluruh hubungan/kegiatan dari dalam ke luar, harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
b. Hanya kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat di lakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat di pilih sekaligus berbagai jenis policy yang di tawarkan.
c. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. Hal ini berarti penggunaan sistem yang

dapat dipercaya dan dengan sistem yang relatif aman.

2.7. Gateway dan fungsinya

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer yang protokolnya berbeda. Gateway merupakan sebuah teknik untuk mengontrol sebuah komunikasi jaringan antar penguna yang di batasi oleh sesuatu cara atau metode yang bisa banyak, biasa juga di sebut dengan gerbang jaringan.

Dari pengertian di atas Gateway sendiri mempunyai fungsinya tersendiri yaitu:

a. Sebagai pintu masuk jaringan satu dengan jaringan lainnya.
   Sesuai dengan definisinya adalah pintu gerbang (gateway) gateway merupakan perangkat keras atau *hardware* yang memiliki fungsi sebagai pintu masuk antara jaringan satu dengan jaringan yang lainnya.
b. Menghubungkan dua atau lebih suatu jaringan satu dengan yang lain.
   Tidak semua jaringan memiliki arsitektur, pola, atau juga topologi yang sama. Ketika berkomunikasi antar jaringan tentunya akan memiliki kesulitan-kesulitan kompabilitas . Gateway ini lah yang akan membantu menghubungkan komunikasi antara jaringan tersebut meskipun mempunyai perbedaan arsitektur.
c. Menghubungkan suatu jaringan komputer besar dengan jaringan komputer besar yang lain.
   Selain menghubungkan antara topologi jaringan yang satu dengan yang lain, gateway juga mempunyai fungsi lain untuk pengabungan antara jaringan besar satu dengan jaringan besar yang lainnya. Atau menggabungkan antara jaringan topologi kecil dengan jaringan yang bertopologi besar dan sebaliknya.

2.8. Stateful

Metode ini merupakan bagian dari firewall (Cuppens, Cuppens-Boulahia, Garcia-Alfaro, Moataz, & Rimasson, 2012), pada metode ini merupakan bagian dari filtering paket data. Metode stateful mempunyai keunggulan untuk jenis firewall yang satu ini dikenal sebagai sebuah firewall dengan fungsinya dalam menggabungkan berbagai keunggulan yang biasanya ditawarkan oleh firewall berjenis packet filtering, proxy dan circuit level dalam suatu system. Firewall jenis ini dapat melakukan filtering pada lalu lintas atas dasar karakteristik paket, sebagaimana halnya filtering berjenis packet filtering serta memiliki pengecekan pada sesi koneksi guna meyakinkan kalau sesi koneksi tersebut diizinkan (Lahmadi & Festor, 2009).

2.9. Penelitian Sebelumnya

Dalam sebuah instansi maupun perusahan yang mempunyai jaringan internet perlunya sistem keamanan jaringan untuk melindungi data-data yang ada perusahaan tersebut. Maka dari itu aspek keamanan jaringan di rasa sangat perlu untuk perlindungan data yang sangat perlu dalam suatu jaringan internet.

Pada penelitian Alfin Hikmaturokhman tahun 2010(Hikmaturokhman et al., 2010), melakukan penelitian analisa topologi jaringan internet mengunakan *firewall* dan *traffic filtering*. Dalam penelitian tersebut mengunakan fungsi router Cisco Router seri 1721. Cisco Router adalah perangkat keras utama yang telah banyak digunakan pada Jaringan Area Luas atau Wide Area Network (WAN). Dalam pengunaan perangkat keras cisco tersebut mengatur paket filtering yang berguna untuk menyaring data yang lewat pada cisco router. Paket-paket data yang datang ke router difilter (disaring) untuk menentukan paket data mana yang akan ditolak dan paket data mana yang akan diteruskan ke suatu alamat jaringan (network address) atau ke suatu alamat komputer (host address) tertentu. Dalam metode paket filtering mengunakan fungsi daftar akses. Dalam fungsinya tahapannya adalah setiap pakaet data yang di terima oleh router akan di cocokan dengan dengan daftar isi akses yang yang diterapkan pada *router interface* baris perbaris. Apabila suatu baris yang cocok maka paket tersebut di teruskan atau di tolak ketika ada baris yang tidak cocok sesuai dengan baris tersebut.

Pengembangan Rekayasa dan Teknologi, Vol 4, No. 2, November 2020, pp 87-97
p-ISSN: 1410-9840 & e-ISSN: 2580-8850
http://journals.usm.ac.id/index.php/jprt/index

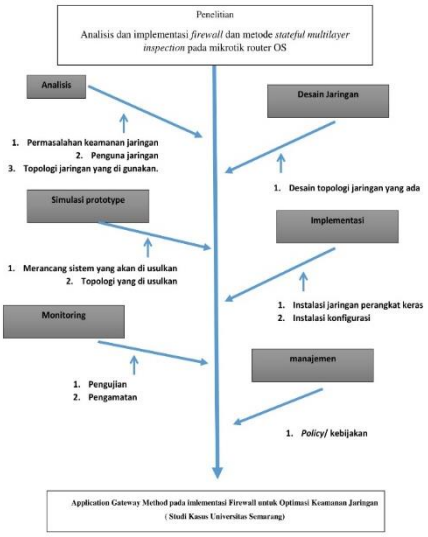
Pada tahun 2015 Yanuar Dwi Jatmiko Wismoaji dan Imam Riadi melakukan penelitian untuk laboratorium komputer(Wismoaji & Riadi, 2015). Pada penelitian tersebut mengunakan metode filtering untuk memblokir situs-situs yang tidak berhubungan dengan kegiatan praktikum serta membatasi *download* file yang besar dalam laboratorium tersebut. Dalam tahapannya melakukan perancangan arsitektur firewall yang di gunakan untuk memfilter paket data dengan firewall dan manajemen bandwidth internet dengan menerapkan layanan *Quality Of Service* (QoS) untuk menetapkan tipe lalu lintas yang terdapat pada jaringan tersebut. dalam penelitian tersebut mendapatkan uji kelayakan sebesar sangat setuju = 20 %, setuju = 78 %, dan kurang setuju = 2 %.

Okta Puspita Dwi Anggorowati dkk pada tahun 2015(Puspita, Anggorowati, Kurniawan, & H, 2015), melakukan penelitian desain arsitektur jaringan di PDII-Lipi mengunakan *Network Development Life Cycle* (NDLC). Metode ini di rancang untuk memantau kinerja jaringan yang di bangun. Penelitian ini digunakan untuk mengetahui prototype yang di gunakan pada jaringan tersebut serta mengukur sebaran sinyal yang di hasilkan access point yang di yang di pasang pada lokasi tertentu. Hal ini di lakukan untuk menunjang kinerja dalam organisasi tersebut. Dalam penelitian tersebut menganalisa jaringan yang sudah tersedia. Analisa jaringan itu menjadi acuan dalam membangun topologi yang diusulkan supaya tidak ada jaringan yang *redundant* dalam membagi jaringan yang ada pada lokasi terseebut. Pengukuran jaringan yang tersedia mengunakan *Quality Of Service* (QoS). Dimana hasil tersebut menjadi acuan untuk usulan topologi jaringan peneliti.

3. METODE

3.1. Bagan Penelitian

Bagan penelitian dalam bentuk fishbone dapat di lihat pada gambar ini:



Gambar 1.1 Bagan Fishbone

3.2. Jenis Data

Ada 2 jenis data dalam penelitian ini yang digunakan :

1. Data Primer, data yang diperoleh secara lansung ,peneliti melakukan observasi configurasi dalam implementasi firewall jaringan komputer
2. Data Sekunder, yaitu data-data yang diperoleh peneliti dari literatur, buku referensi,ataupun dari browsing internet. Dalam penelitian ini ada beberapa tahapan gunakan untuk membangun konfigurasi firewall didapat dengan beberapa tahapan

3.3. Pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah :

1. Observasi: Melakukan Mengamati dalam proses implemetasi application Gateway firewall
2. Studi Pustaka : Mengumpulan literatur, buku referensi ataupun dari browsing internet.

3.4. Metode Penelitian

Dalam penelitian ini peneliti akan membangun firewall dengan metode *Application gateway* menggunakan NDLC (*Network Development Life Cycle*), NDLC adalah salah

satu metode yang dilakukan dalam pengembangan metode dalam jaringan.

Ada 6 tahapan dalam metode NDLC tahapan – tahapan tersebut adalah sebagai berikut :

1. Analysis,

   Analysis dilakuikan peneliti meliputi analisa permasalahan,analisa user, dan analisa topologi jaringan ;

2. Design,

   Desain dalam tahapan ini di buat untuk mengambarkan skema jaringan yang sedang berjalan dan diterapkan;

3. Simulation Prototyping,

   Tahapan ketiga yang peneliti lakukan, dimana pada tahapan simulasi ini akan membangun Sistem yang diusullkan.

4. Implementation,

   Dalam tahapan Implementasi peneliti akan dilakukan spesifikasi rancangan yang akan dijalankan meliputi instalasi konfigurasi jaringan, instalasi jaringan perangkat keras (*hadware*)

5. Monitoring,

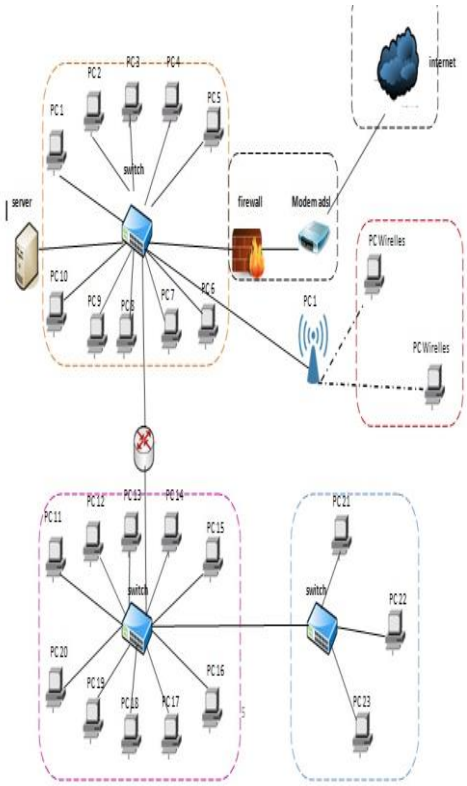
   Tahapan ini peneliti melakukan pengujian terhadap infrastruktur jaringan yang telah diterapkan/diimplementasikan

6. Management,

   adalah tahapan keenam yang peneliti lakukan, dimana pada tahapan managemen ini mengatur masalah policy kebijakan agar system yang sudah dibangun dapat terjaga.

4. HASIL DAN PEMBAHASAN

Hasil dan pembahasan yang dicapai merupakan hasil dari implementasi dari metode yang telah direncanakan diawali dengan tahapan persiapan dengan merancang topologi dari sebuah jaringan dengan metode *NDLC.*



Gambar 2 Topologi jaringan

4.1. Metode NDLC (*Network Development Life Cycle*)

Dalam desain jaringan di atas firewall sebelum di bagikan ke penguna internet di kampus, akan di lakukan filtering firewall. Untuk Firewall perangkat lunak adalah perangkat lunak terprogram yang berjalan di atas lapisan aplikasi komputer, sebagai pembatas eksternal untuk mencoba mendapatkan hak istimewa dalam menggunakan komputer dalam hal ini koneksi internet. Dalam konfigurasi middlebox, OSI dan jaringan TCP / IP, model mengoperasikan firewall di lapisan perangkat keras tingkat rendah, Informasi header paket digunakan untuk menentukan keaslian otorisasi paket. Secara khusus, aturan filter firewall diterapkan pada alamat IP sumber, tujuan Alamat IP, dan alamat port, misalnya, nomor port dari antarmuka protokol TCP atau UDP dan IP. Ini Metode penyaringan dikenal sebagai firewall. Firewall inspeksi stateful juga disebut sebagai firewall dinamis yang terus-menerus memeriksa informasi keadaan koneksi jaringan aktif dan menggunakannya untuk memutuskan apakah

akan mengizinkan atau menolak paket melalui firewall. Router dan switch generasi saat ini dibangun dan memprogram tabel penerusan mereka secara lokal, yang memaksa perangkat lokal untuk membuat keputusan penerusan secara internal. mendukung administrator jaringan untuk mempertahankan status jaringan untuk proses alokasi sumber daya otomatis

4.2. Metode Stateful

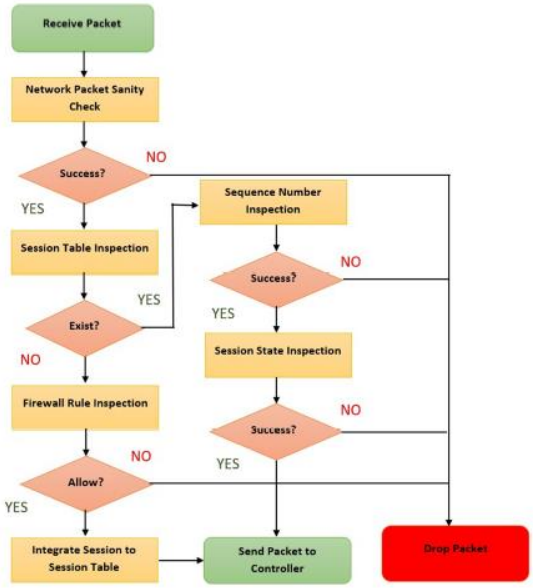
Algoritma firewall inspeksi stateful yang diusulkan menerima dan menganalisis header paket yang masuk untuk mengizinkan atau menolak paket. Sementara itu, kebijakan firewall stateful dikonfigurasi untuk mengelola firewall tabel aturan, tabel sesi untuk menjaga informasi arus lalu lintas. Kontroler adalah diprogram dengan aplikasi firewall stateful sebagai modul. Langkah-langkah dijelaskan sebagai berikut.

Algorithm 1: Stateful Inspection Firewall Algorithm
Input: ST states Session Table, SNC states Sequence Number Check, RT states Firewall Rule Table, and SS states Session State status.
Step 1: START
Step 2: Receive Packet;
Step 3: Perform Network Sanity Check ←mac = phdr.find (mac);
Step 4: If (mac.find() = = 0:0:0:0) then:
Step 5: Drop the packet;
Step 6: Else
Step 7: Examine socket in Session Table ←socket = ST.find (socket);
Step 8: Examine flag in Session Table ←flag = ST.find (flag);
Step 9: If (pkt.find() = = socket && flag) then;
Step 10: pkt.send (SNC) ;
Step 11: Else
Step 12: Apply Firewall Filtering Policy ←rule = RT.match (rule);
Step 13: If (rule.match() = = allow) then;
Step 14: pkt.send (ST);
Step 15: Else
Step 16: Drop the packet;
Step 17: Endif
Step 18: Endif
Step 19: Examine Sequence Number ←SNC = phdr.find (SNC);
Step 20: If (pkt.find() = = SNC) then;
Step 21: pkt.send (SS);
Step 22: Else
Step 23: Drop the packet;
Step 24: Endif
Step 25: Examine Session State ←SS = ST.find (active);
Step 26: If (pkt.find() = = SS) then;
Step 27: pkt.send (Cp);
Step 28: Else
Step 29: Drop the packet;
Step 30: Endif
Step 31: Endif
Step 32: END

Langkah 1 hingga 6: Paket masuk diterima dan menjalani pemeriksaan kesehatan jaringan awal. Pemeriksaan ini dilakukan untuk memberikan keamanan tingkat awal dan untuk mengurangi beban lalu lintas firewall. Jika paket melewati pemeriksaan kewarasan, itu diperbolehkan ke dalam proses penyaringan firewall; jika tidak, paket akan dibuang.
Langkah 7 hingga 11: Header paket diperiksa, dan operasi pencarian dilakukan berdasarkan soket dan bendera informasi untuk menemukan entri aktif dalam tabel sesi. Jika kecocokan ditemukan, maka paket dikirim ke sequence nomor check submodule, atau jika tidak ada entri yang tersedia di tabel sesi, maka paket tersebut dikenakan kebijakan firewall.
Langkah 12 hingga 16: Header paket diperiksa dan menjalani inspeksi kebijakan firewall untuk menerapkan izin atau tolak aturan dari tabel aturan. Jika paket diijinkan, maka entri sesi baru ditambahkan dalam tabel sesi; jika tidak, paket dijatuhkan.
Langkah 17 hingga 21: Sekali lagi, header paket diperiksa untuk mencari dan menemukan nomor urut yang cocok dalam tabel sesi. Jika kecocokan ditemukan, kemudian paket tersebut diteruskan ke submodul status sesi pencarian atau paket tersebut dijatuhkan.
Langkah 22 hingga 28: Status status sesi divalidasi dengan menemukan status status aktif di tabel sesi. Jika sesi menyatakan dari paket yang ditemukan aktif, maka aliran paket tertentu diteruskan ke pengontrol utama untuk keputusan kontrol, atau paket dijatuhkan.

Pengembangan Rekayasa dan Teknologi, Vol 4, No. 2, November 2020, pp 87-97
p-ISSN: 1410-9840 & e-ISSN: 2580-8850
http://journals.usm.ac.id/index.php/jprt/index

Berikut flowchat dari metode stateful

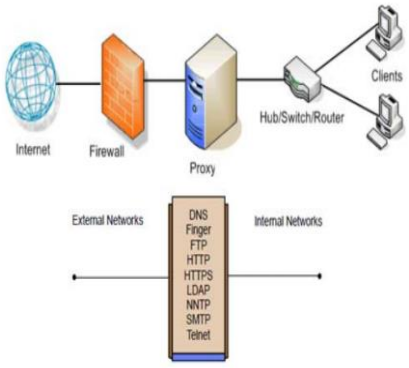


Gambar 3 Flowchart Metode stateful

4.3. Aplication Proxy Gateway

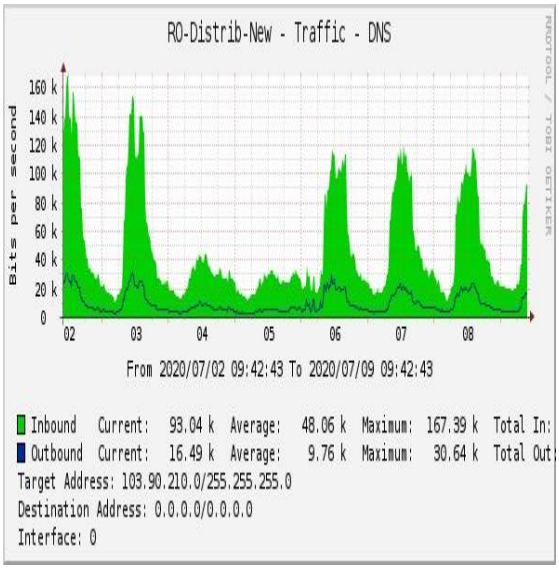
Server proxy atau gateway firewall aplikasi berada di antara aplikasi klien dan server dan bertindak sebagai perantara antara dua host yang berkomunikasi. *Firewall proxy* berfungsi dengan mencegat permintaan dari host klien di internal jaringan dan kemudian meneruskannya ke tujuannya.

Adakalanya server yang ada pada jaringan yang di akses dari jaringan publik. Contohnya karena ada karyawan yang bersifat mobile dan harus bisa mengakses data yang ada di server tersebut, yang di butuhkan adalah IP public statis lebih rekomendasi. Memasang ip public ke server, maka server tersebut sudah bisa di akses dari internet. Agar server bisa di akses dari internet mengkonfigurasi forwarding di router miktrotik dengan fitur firewall NAT. forwarding ini akan membelokkan traffic menuju ip public yang terpasang di router menuju ke ip local server. Dengan begitu seolah-olah client di internet berkomunikasi dengan server meminjam IP public router microtic



Gambar 4 Application Gateway firewall

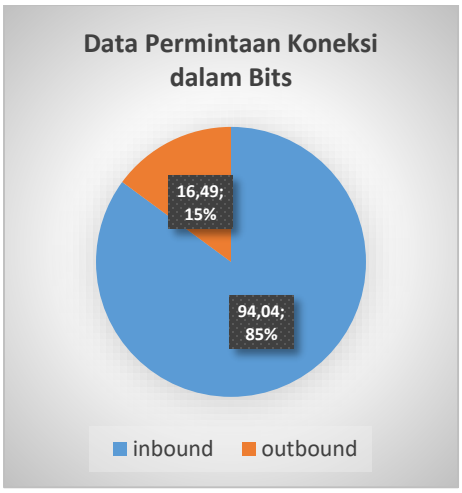
4.4. Hasil Perbandingan Metode Stateful Dan Application Gateway



Gambar 5. Perbandingan Metode Stateful Dan Application Gateway

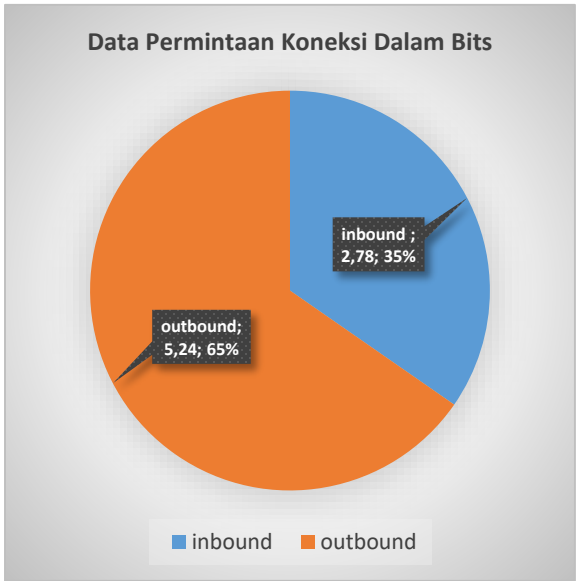
Ini merupakan hasil dari implementasi metode stateful dan applicaton gateway. Pada gambar 5 adalah hasil pengunaan metode stateful yang di gunakan. Dari paket permintaan jaringan yang di lakukan oleh penguna. Dari data pada gambar 5 ketahui nilai inbond 94,04 bits dan outbond 16,49 bits. Dari nilai tersebut 77,55 paket yang di drop atau di tolak dalam permintaan jaringan komputer yang mengunakan metode stateful. Dengan metode ini permintaan data yang di tolak sebesar 70% dari total keseluruhan.

Pengembangan Rekayasa dan Teknologi, Vol 4, No. 2, November 2020, pp 87-97
p-ISSN: 1410-9840 & e-ISSN: 2580-8850
http://journals.usm.ac.id/index.php/jprt/index

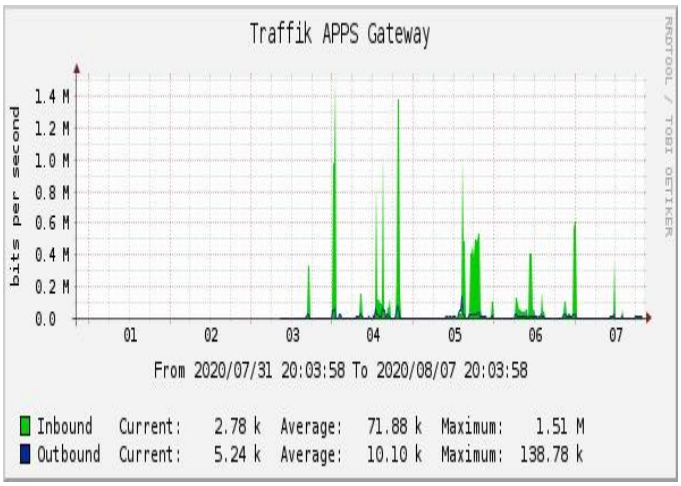


Gambar 6. Diagram permintaan paket dengan metode stateful

Dari data pada gambar 6 ketahui nilai inbond 2,78 bits dan outbond 5,24 bits. Dari nilai tersebut 77,55 paket yang lolos dari sistem keamanan jaringan sebanyak 30%. Maka metode stateful firewall lebih baik daripada metode gateway.
dsad



Tabel 1 diagram permintaan paket dengan metode gateway



Gambar 7. Trafik APPS Gateway

5. Kesimpulan

Kami menganggap makalah kami sebagai langkah pertama dalam mendesain dan menganalisis firewall stateful. Kontribusi kami dalam hal ini. Pertama, kami mengusulkan model pertama untuk menentukan firewall stateful, yang selanjutnya membuka pintu untuk penelitian baru tentang firewall stateful. Model stateful kami firewall memiliki beberapa sifat yang menguntungkan. Ini sederhana tetapi dapat mengekspresikan berbagai fungsi pelacakan status. Itu memungkinkan kami mewarisi hasil yang kaya dalam desain firewall tanpa negara dan analisis. Selain itu, ini memberikan kompatibilitas ke belakang sedemikian rupa sehingga firewall stateless juga dapat ditentukan menggunakan kami model. Kedua, kami menyajikan metode untuk menganalisis stateful firewall yang ditentukan menggunakan model kami. Kami menguraikan metode untuk memverifikasi apakah firewall benar-benar stateful.

Beberapa masalah yang terkait dengan model firewall stateful kami adalah berangkat untuk pekerjaan masa depan, misalnya, bagaimana menerapkan secara efisien model ini dan cara menggunakannya untuk menganalisis properti lain firewall stateful.

6. Daftar pustaka

Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru, P., & -Karawang, C. (2018). *Optimalisasi Jaringan Menggunakan Firewall*. *2*(3), 17–23.

Al-Shaer, E. (2014). Automated firewall analytics: Design, configuration and optimization. In *Automated Firewall Analytics: Design, Configuration and Optimization*. https://doi.org/10.1007/978-3-319-10371-6

Cuppens, F., Cuppens-Boulahia, N., Garcia-Alfaro, J., Moataz, T., & Rimasson, X. (2012). Handling stateful firewall anomalies. *IFIP Advances in Information and Communication Technology*, *376 AICT*,174–186. https://doi.org/10.1007/978-3-642-30436-1_15

Ertie Nur Hartiwati. (2014). Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet. *Jurnal Ilmiah Informatika Komputer Universitas Gunadarma*, 27–33.

Hidayatulloh, S. (2014). Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol Ipsec. *Jurnal Informatika*, *1*(2), 93–104. https://doi.org/10.31311/ji.v1i2.47

Hikmaturokhman, A., Purwanto, A., Munadi, R., Batu, T. B., Telkom, A., Putra, S., … Router, P. C. (2010). *Analisis Perancangan Dan Implementasi Firewall Dan*. *2010*(semnasIF), 1–8.

Lahmadi, A., & Festor, O. (2009). SecSip: A stateful firewall for SIP-based networks. *2009 IFIP/IEEE International Symposium on*