BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Pada tahun 2013, Zohan Aris Pribadi melakukan penelitian tentang *firewall filtering* yang berjudul "Analisis dan Implementasi *Firewall* dengan Metode *Stateful Multilayer Inspection* Pada *Mikrotik Router OS*". Penelitian tersebut bertujuan untuk meneliti kelemahan apa saja yang terdapat pada implementasi *firewall filtering* menggunakan metode satu layer saja. Sehingga penelitian ini menghasilkan bahwa menggunakan metode baru yaitu metode *Stateful Multilayer Inspection* pada *Mikrotik Router OS* dapat berjalan secara efisien, mempermudah user untuk *manage firewall filtering* itu sendiri. Setelah mengimplementasikan metode tersebut, *firewall* yang telah dibuat cukup efisien untuk menyaring paket-paket data yang masuk lewat jaringan yang diteliti tersebut. (Pribadi, 2013)

Fatsyahrina Fitriastuti melaksanakan penelitian yang berjudul "Implementasi *Bandwidth Management* dan *Firewall System* Menggunakan Mikrotik OS 2.9.27" pada tahun 2014. Menurut penelitian mereka, *Firewall Filter Rules* dan *Firewall Mangle* memiliki perbedaan pada fungsinya. *Firewall Mangle* hanya melaksanakan tugasnya sebagai penanda paket dimana paket tersebut nanti yang akan dieksekusi oleh *Firewall Filter Rules* sehingga paket-paket tersebut nanti dapat diakses oleh pengguna internet. Selain itu, penelitian tersebut juga menghasilkan kesimpulan bahwa dengan menggunakan *Firewall Filter Rules* yang dikombinasikan dengan *Layer 7 Protocols* dapat menjadi pembatas akses paket-paket data yang telah disaring.(Fitriastuti & Utomo, 2014)

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

Penelitian berjudul "Implementasi *Blocking* Situs di Router Mikrotik RB 2011 Dengan Menggunakan *Web Proxy* Studi Kasus STIE-MUSI Rawas Lubuklinggau" pada tahun 2017 oleh Armanto menghasilkan penelitian bahwa penggunaan *web proxy* yang sudah tersedia di router Mikrotik cukup membantu dikarenakan tidak perlu membangun *web proxy* yang baru lagi. Penelitian tersebut juga mencapai hasil bahwa situs-situs yang bersifat negatif ataupun memiliki konten negatif didalamnya tidak dapat diakses oleh pengguna internet (dosen dan mahasiswa). Penelitian tersebut menyimpulkan bahwa fitur *firewall* pada Mikrotik router sangat efektif untuk melakukan pemblokiran pada situs yang memiliki konten negatif. (Armanto, 2017)

Gita Hersatya melakukan penelitian pada tahun 2013 yang berjudul "Implementasi *Filtering* Dengan *Layer 7 Protocol* Mikrotik RouterOS Pada Warnet Machnet" mengungkapkan bahwa *Layer 7 Protocol* dapat melakukan *filtering* pada kegiatan unduh atau *download* pada warnet Machnet. Penelitian tersebut melakukan implementasi pada perangkat lunak Utorrent dan Internet Download Manager. Dari hasil implementasi didapatkan bahwa kegiatan unduh melakukan kedua perangkat lunak tersebut tidak dapat diproses. *Download* yang dilakukan tidak berjalan sama sekali ataupun kecepatan *downloadnya* dikurangi. (Hersatya, 2013)

Faizal Eko Nugroho, dkk pada tahun 2015 menjelaskan dalam penelitiannya yang berjudul "Analisin Perbandingan Perfomansi *Deep Packet Inspection Firewall* Antara L7-Filter dan nDPI" keunggulan yang terdapat L-7 Filter adalah dapat mendeteksi trafik data aplikasi *peer-to-peer sharing* dikarenakan L-7 Filter cocok dengan protokol pada *application layer* pada OSI

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

model. Keunggulan L-7 Filter lainnya adalah dapat mengendalikan dan *manage bandwidth* tanpa ada perbedaan dengan layer lainnya. (Nugroho & Brotoharsono, 2015)

Sedangkan keunggulan yang dimiliki *web proxy* pada Mikrotik dijelaskan secara rinci oleh Setya Wijayanta dan Muslihudin pada tahun 2013 dengan penelitian yang berjudul "Pembangunan *Web Proxy* Dengan Mikrotik Untuk Mendukung Internet Sehat di SMk Muhammadiyaah 1 Patuk Gunungkidul". Pada penelitian tersebut dapat ditarik kesimpulan bahwa *firewall filtering* pada Mikrotik tidak hanya dapat melakukan pemblokiran pada situs saja, namun dapat juga melakukan pemblokiran pada *keyword* atau kata kunci yang digunakan pada situs pencarian Google. Selain itu, pemblokiran dapat juga dilakukan dengan menggunakan pegnaturan waktu, sehingga ada waktu tertentu dimana pengguna internet dapat mengakses media sosial dan waktu tidak dapat mengaksesnya. (Setya Wijayanta, Muslihudin, 2013)

2.2 Landasan Teori

Pada pelaksanaan proyek ini terdapat teori yang penulis gunakan untuk memperkuat teori yang penulis paparkan. Teori yang telah dipilih dan diteliti oleh penulis sebagai referensi landasan teori adalah sebagai berikut:

2.2.1 Firewall

Menurut Fahlepi Roma Doni pada tahun 2010, *Firewall* merupakan sebuah sistem yang diaplikasikan baik pada *hardware*, *software* ataupun sistem dari sebuah perangkat dengan fungsi utama untuk melindungi, menyaring,

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

membatasi atau menolak kegiatan suatu sektor pada jaringan pribadi dengan jaringan luar. Sektor disini dapat berarti sebuah *workstation, server, router* atau *local area network* (LAN). (Doni, 2014)

Sedangkat menurut *National Institute of Standards and Technology* (NIST) pada tahun 2011 *Firewall* merupakan perangkat atau program yang mengendalikan arus lalu lintas jaringan antar jaringan atau *host* yang menggunakan tingkat keamanan yang berbeda. Publikasi ini memberikan gambaran umum tentang beberapa jenis teknologi *firewall* dan membahas kemampuan keamanan mereka dan keuntungan dan kekurangan relatifnya secara rinci. Ini juga membuat rekomendasi untuk menetapkan kebijakan *firewall* dan untuk memilih, mengkonfigurasi, menguji, menerapkan, dan mengelola solusi *firewall*.

2.2.2 Karateristik Firewall

Beberapa karakteristik yang dimiliki oleh *Firewall* menurut Ismi Mulyani adalah (Mulyani, 2017) :

1. *Firewall* memiliki keamanan yang kuat yang diharuskan kebal untuk menahan segala serangan yang disebabkan atau ditimbulkan dari luar sistem atau dari dalam sistem itu sendiri. Serangan dari dalam dapat berarti *virus* dan kelalaian dari pengguna jika dilihat dari sisi *firewall* yang terdapat pada sistem operasi. Jika dilihat dari sisi keamana jaringan *firewall* dapat menahan serangan peretas ataupun serangan DDOS (*Distributed Denial of Service*).
2. *Firewall* memiliki *rules* atau aturan dimana hanya aktivitas/kegiatan dan paket-paket data yang dikenalinya (yang sudah terdaftar pada daftar aturan

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

yang telah dikonfigurasi) yang dapat melewati penyaringan yang dilakukan oleh *Firewall*. Karakteristik ini dapat dilakukan dengan mengkonfigurasi *policy* yang terdapat keamanan lokal.

3. *Firewall* akan melakukan pemblokiran atau membatasi aktivitas/kegiatan dan paket-paket data yang telah disaring. Jika tidak terdaftar pada *rules* atau aturan yang telah dikonfigurasi, maka proses akan dihentikan dan tidak dapat diakses lagi. Sehingga segala hal yang masuk dari luar harus melewati *firewall* terlebih dahulu agar dapat terhubungan ke jaringan lokal.

2.2.3 Fungsi Firewall

Jika dilihat dari sisi keamanan jaringan, menurut Aswin Dwiyono fungsi *firewall* terbagi tiga, yaitu diantaranya adalah (Dwiyono Aswin, 2008):

1. Melakukan modifikasi atau perubahan pada *header packet*. *Header packet* merupakan paket TCP yang bebentuk bit dimana paket ini muncul pada proses sebelum *routing* dilakukan.
2. Melakukan translasi pada alamat suatu *network* jika jaringan tersebut berasal dari jaringan publik. Dimana jaringan publik itu sendiri pada umumnya bersifat tidak aman. Proses translasi dapat dilakukan secara kebalikannya. Artinya *firewall* dapat melakukan translasi jaringan publik menjadi jaringan lokal ataupun sebaliknya.
3. Melakukan penyaringan paket data yang masuk ke jaringan. Jika paket data tersebut menurut *firewall* tidak aman maka proses masuknya data tersebut akan dihentikan dan akan dibatasi. Hasilnya dapat berbagai jenis seperti

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

dihapus, diblokir ataupun dibatasi aksesnya. Fungsi ini memastikan keamanan pengguna ketika sedang *surfing* di internet.

2.2.4 Jenis Firewall

Menurut Aswin Dwiyono, terdapat 5 jenis *firewall* diantaranya adalah (Dwiyono Aswin, 2008):

1. *Packet Filter*, jenis *firewall* yang dapat dibilang cukup *simple* dikarenakan fungsinya hanya sebagai penyaring paket-paket data yang keluar masuk dari jaringan komputer kita.
2. *Circuit Level Gateway*, jenis *firewall* yang terletak pada layer *session* atau layer kelima dalam layer OSI. Jenis ini biasanya memiliki komponen *proxy server* dan fungsinya lebih tinggi daripada jenis *firewall packet filter*. Namun jenis *firewall* ini hanya digunakan untuk menyembunyikan identitas asli pengguna internet.
3. *Application Level*, atau dapat juga disebut sebagai *Application Level Gateway* atau *Application Proxy*. Cara kerja *firewall* ini sama dengan *packet filter* namun *firewall* ini bekerja langsung pada layer paling atas, yaitu *application layer*. Jenis *firewall* ini yang penulis gunakan dalam proyek ini.
4. *Network Address Translation* (NAT), jenis *firewall* yang menyediakan proteksi secara otomatis dibalik sistem dari *firewall* itu sendiri. Fungsinya yaitu mentranslasikan jaringan internet atau lokal ke jaringan luar atau publik, begitupun sebaliknya.
5. *Stateful Firewall*, jenis *firewall* ini merupakan kombinasi antara *packet filter*, *proxy* dan *circuit level* yang fungsinya sebagai penyaring paket namun dilihat

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

dari karakteristik paketnya saja. Tugasnya hanya memastikan atau meyakinkan layer sesi bahwa paket-paket data tersebut aman dan dapat diizinkan masuk ke jaringan.

2.2.5 Jaringan Komputer

Jaringan komputer secara garis besar dapat disebut sebagai kumpulan komputer atau perangkat lain yang saling terhubung menggunakan media komunikasi. Informasi atau data yang ada dari setiap pengguna memungkinkan penggunaan jaringan untuk saling bertukar data atau menggunakan perangkat lunak maupun perangkat keras. Komputer dalam jaringan dapat saling berhubungan melalui kabel, jaringan telepon, gelombang radio, satelit ataupun sinar infra merah (Habibi & Arifin, 2013). Jika dilihat berdasarkan luas area yang dapat dijangkau jaringan komputer dibagi menjadi 3 jenis, yaitu :

1. *Local Area Network* (LAN), secara teoritis adalah jaringan milik personal atau privat di dalam suatu wilayah atau tempat yang berjarak hanya sampai beberapa kilometer saja tidak lebih dari 10 kilometer. Biasanya LAN berfungsi sebagai penghubung antar komputer dan atau perangkat keras di dalam wilayah baik itu kantor, perusahaan, sekolah, kampus, gedung pemerintahan ataupun pabrik agar perangkat-perangkat keras tersebut dapat digunakan bersama dan sebagai media bertukar informasi/data.
2. *Metropolitan Area Network* (MAN), dengan fungsi dan teknologi yang digunakan pada LAN, MAN memiliki perbedaan pada jangkauan wilayahnya. Jangkauan MAN dapat mencapai jarak hingga 50 kilometer. MAN secara harfiah merupakan kumpulan dari beberapa LAN. Sehingga MAN berfungsi

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

sebagai jaringan yang menghubungkan antar perkantoran, antar gedung pemerintahan, antar kampus atau sekolah yang meiliki *bandwidth* yang tinggi karena pertukaran data pada jaringan MAN membutuhkan kecepatan transfer data yang tinggi.

3. *Wide Area Network* (WAN), biasanya digunakan untuk menghubungkan jaringan-jaringan LAN atau MAN ke internet. Jarak jangkauan WAN dapat mencapai ribuan kilometer atau bahkan satu dunia. Dikarenakan jaringan WAN menggunakan satelit sebagai pemancar sinyal dan penghantar informasi/data yang dikirim. WAN memiliki fungsi yang lebih kompleks karena menghubungkan sesama jaringan LAN atau MAN ataupun jaringan LAN dengan MAN dan *vice versa*.

2.2.6 Topologi

Topologi atau dapat disebut juga sebagai *blueprint* dari jaringan komputer merupakan gambaran atau skema koneksi antar perangkat jaringan dalam suatu sistem jaringan komputer yang berfungsi untuk mengidentifikasi seberapa tinggi tingkat efektivitas kinerja jaringan komputer itu sendiri. (Nirsal & Ali, 2017). Ada empat bentuk dasar jaringan, yaitu :

1. Topologi *Bus*, menggunakan tipe kabel *backbone* dan menggunakan konektor *T-Connector* pada setiap kabelnya. Sehingga setiap perangkat harus memilik *port* untuk jenis konektor tersebut. Kelemahan dari topologi ini adalah adanya kemungkinan untuk tabrakan data saat antar komputer melakukan komunikasi atau *transfer* data. Kelemahan lainnya adalah jika terjadi gangguan pada satu titik, maka keseleruhan topologi akan terkena dampaknya.

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

2. Topologi *Star*, berbeda dari topologi *Bus* topologi ini lebih memposisikan jaringan yang berbentuk sentralisasi. Sehingga semua perangkat diletakkan seolah-olah mengelilingi perangkat yang menjadi sentral dari topologi tersebut. Biasanya perangkat yang bertugas menjadi sentralitas dari topologi adalah *switch* dan atau *hub*.
3. Topologi *Ring*, memiliki bentuk topologi yang sama dengan topologi *star*. Perbedaannya terletak pada sentralitasnya. Pada topologi *ring* tidak terdapat perangkat yang berperan sebagai sentralitas topologi, melainkan setiap perangkat terhubung antar satu sama lain tanpa adanya perangkat sentralitas tersebut. Sehingga bentuk topologi *ring* benar-benar membentu sebuah cincin dan jika terjadi suatu gangguan atau masalah pada satu perangkat maka semua komunikasi atau aktivitas *transfer* data pada topologi terganggu,
4. Topologi *Mesh*, memiliki keunggulan saat komunikasi antar perangkat terjadi. Jika perangkat A ingin melakukan komunikasi dengan perangkat B maka komunikasi dapat langsung terjadi dan terhubung ke perangkat yang dituju. Sehingga kemungkinan terjadinya masalah cukup minim.
5. Topologi *Tree*, topologi ini menggunakan media kabel yang terdapat pada topologi *bus* dan menggunakan teknologi yang diterapkan pada topologi *star*. Sehingga perangkat yang berperan sebagai sentralitas topologi akan dihubungkan ke perangkat sentralitas lainnya dengan kabel *backbone*.

2.2.7 Server

Server umumnya berwujud seperti komputer yang digunakan oleh pengguna atau *client*. Perbedaannya terletak pada spesifikasi dan performa pada

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

server. Karena sesuai dengan namanya *server* bertindak sebagai penyedia layanan baik itu layanan dalam internet ataupun layanan yang dibutuhkan *client* untuk menunjang proses pekerjaan saat menggunakan komputer (Bawafie & Muslihudin, 2013).

2.2.8 IP Address

IP address memiliki kepanjangan kata yaitu *Internet Protocol Address* yang memiliki didefinisikan sebagai identitas setiap perangkat seperti komputer, laptop, perangkat jaringan, bahkan *smartphone*. Identitas tersebut umumnya berbentuk kumpulan angka unik yang khusus dialokasi untuk setiap perangkat. Sehingga setiap perangkat memiliki angka yang berbeda dan menghindari terjadinya duplikasi identitas. *IP address* ini sendiri memiliki beberapa variasi, diantaranya adalah:

1. *Static IP* adalah *IP address* yang diisi secara manual oleh pengguna komputer ataupun administrator.
2. *Dynamic IP* adalah *IP address* yang didapatkan secara otomatis melalui *DHCP server* ketika perangkat terhubung ke jaringan yang memiliki layanan tersebut.
3. *Public IP* adalah *IP address* yang digunakan ketika komputer atau perangakat jaringan lainnya terhubung ke jaringan Internet.
4. *Private IP* adalah *IP address* yang hanya bisa digunakan pada jaringan local pada sesama komputer untuk dapat saling terkoneksi.

Untuk mempermudah pembagian dan pendistribusiannya, alamat IP dikelompokkan dalam beberapa kelas berdasarkan jangkauan jaringan dan jumlah

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

ip yang dapat ditampung dalam jaringan tersebut. *IP address* terbagi menjadi 5 kelas, 3 kelas diantaranya adalah kelas yang dipakai untuk umum sedangkan 2 kelas lainnya hanya digunakan untuk kepentingan pemerintahan dan penelitian. Ketiga kelas tersebut adalah:

1. *IP address* kelas A tersusun atas angka kombinasi dimana 8 bit pertama dialokasikan sebagai *network ID* dan 24 bit lainnya dialokasikan sebagai *host ID*, Dikarenakan jumlah *host ID* yang besar maka *IP address* kelas A memiliki jumlah *host* yang terbanyak dari semua kelas. Rentang dari *IP* address kelas A dimulai dari 1.xxx.xxx.xxx hingga 126.xxx.xxx.xxx.
2. *IP address* kelas B memiliki pembagian yang merata untuk *network ID* dan *host ID*. *Network ID* dan *host ID* masing-masing memiliki 16 bit. Sehingga penggunaan *IP address* kelas B umumnya digunakan pada jumlah *host* yang sedang. Rentang *IP address* untuk kelas B dimulai dari 128.0.xxx.xxx hingga 191.255.xxx.xxx.
3. *IP* address kelas C memiliki 24 bit pada *network ID* dan 8 bit lainnya untuk *host ID*. Karena memiliki jumlah *host ID* yang sedikit *IP address* kelas C umumnya digunakan untuk jaringan yang berskala kecil, contohnya seperti jaringan LAN. Rentang *IP address* kelas C dimulai dari 192.0.0.xxx hingga 223.255.255.xxx

2.2.9 Subnetting

Subnetting adalah teknik yang umum digunakan pada jaringan komputer untuk memecah jaringan yang besar menjadi beberapa jaringan yang lebih kecil. *Subnet* juga bisa diartikan sebagai pembagian suatu alamat IP dalam suatu

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

jaringan menjadi banyak alamat IP atau banyak *subnet* yang memiliki alamat jaringan tersendiri. Pada dasarnya perhitunggan *subnetting* dipergunakan untuk mencari tahu ataupun menentukan *Network ID*, Alamat *broadcast*, *Subnetmask*, Jumlah *host* dan *Gateway*.

1. *Network ID* merupakan indentitas pada suatu jaringan, yang menyatakan bahwa semua IP dalam satu jaringan/*broadcast domain* yang sama. *IP Network ID* adalah IP pertama yang ada di jaringannya.
2. *Broadcast* merupakan IP yang digunakan untuk menyebarkan pengiriman paket ke semua IP atau pengiriman data jika terjadi perubahan ataupun *request* dari satu *host* ke seluruh *host* yang ada pada jaringan tersebut. *IP Broadcast* adalah IP terakhir yang ada pada jaringannya.
3. *Subnetmask* merupakan angka biner yang terdiri dari 32 bit yang digunakan untuk membedakan *Network ID* dengan *Host ID*, serta menentukan berapa banyak IP yang berada dalam satu jaringan tersebut.
4. Jumlah *host* adalah jumlah *IP Address* yang bisa diset atau digunakan pada perangkat yang terhubung kejaringan yang menggunakan *protocol TCP/IP*.
5. *Gateway* merupakan alamat IP yang digunakan untuk terhubung dengan jaringan lain berbeda, *IP Gateway* adalah IP yang dipilih dari salah satu IP Jumlah *host* dan di set pada perangkat router.

Konsep perhitungan *subnetting* menggunakan rumus $2^{(32-n)}$ dimana nilai n merupakan *prefix subnet*, dan nilai n pada rumus di tambah 8 sesuai dengan pengeseran garis pemisah antara bagian *network* dan bagian *host* dari suatu alamat IP. Misalnya alamat ip 192.168.1.10/25 maka nilai n adalah 25. Sehingga $2^{(32-25)} = 2^7 = 128$ maka untuk menentukan blok IP pada jaringan tersebut menggunakan

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

kelipatan 128 dan nilai dikurangi 1 untuk mendapatkan IP broadcast, seperti yang terlihat di Tabel 1.

Tabel 1

Net ID dan Broadcast Kelas C

Net ID	Broadcast
0	127
128	255
256	

Jadi, berdasarkan soal diatas 192.168.1.10/25 berada pada *range* 0 - 127 yaitu 192.168.1.0 -192.168.1.127, maka:

Network ID :192.168.1.0 (IP pertama pada jaringan ini)

Broadcast : 192.168.1.127 (IP terakhir pada jaringan ini)

Subnetmask : 255. 255. 255.128

IP Host : 192. 168. 1. 2-192. 168. 1. 126

Gateway : 192. 168. 1. 1

Contoh lain dengan alamat IP 172.20.10.10/22 dikarenakan *prefix* pada alamat IP tersebut merupakan IP kelas B maka nilai n ditambah 8 menjadi 30. Sehingga $2^{(32-(22+8)} = 2^2 = 4$ maka untuk menentukan blok IP pada jaringan tersebut menggunakan kelipatan 4 seperti yang terlihat di Tabel 2.

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

Tabel 2

Net ID dan Broadcast Kelas B

Net ID	Broadcast
0	3
4	7
8	11
...	...

Jadi berdasarkan soal diatas 172.20.10.10 berada pada range 8-11 yaitu 172.20.8.0 - 172.20.11.255, maka:

Network ID :172.20.8.0 (IP pertama pada jaringan ini)

Broadcast : 172.20.11.255 (IP terakhir pada jaringan ini)

Subnetmask : 255. 255. 252.0

IP Host : 172.20.8.2 - 172.20.11.254

Gateway : 172.20.8.1

2.2.10 OSI Layer

OSI Layer adalah singkatan dari *Open System Interconnection* yang merupakan sebuah model arsitektural atau protokol interkoneksi jaringan yang dibuat oleh *International Organization for Standardization (ISO).* Model OSI menerapkan konsep yang dikenal dengan enkapsulasi. Enkapsulasi adalah metode membungkuskan data dari satu lapisan model OSI dalam struktur data baru sehingga setiap lapisan model OSI hanya akan melihat dan berurusan dengan

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

formasi yang dibutuhkan untuk dengan benar menangani dan memberikan data pada jaringan komputer (Sujana, 2014).

Model OSI dibagi menjadi tujuh lapisan yang masing-masing mempunyai tugas sendiri yang saling berkaitan satu sama lain, yaitu:

1. *Application Layer*, merupakan lapisan ketujuh yang berada paling atas pada model OSI, layer ini berfungsi sebagai antarmuka dengan aplikasi dengan menyediakan akses jaringan untuk program aplikasi
2. *Presentation Layer*, berfungsi untuk memastikan data yang akan di transmisikan oleh aplikasi telah dikonversi ke dalam format yang dapat ditransmisi dan dimengerti oleh proses lapisan aplikasi melalui jaringan.
3. *Session Layer*, berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau memutuskan komunikasi antar aplikasi atau proses yang berjalan di jaringan.
4. *Transport Layer*, berfungsi untuk mengirimkan packet data dari sumber pengirim ke alamat tujuan dan memastikan packet diterima dengan sukses dan keutuhan data.
5. *Network Layer*, berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan *routing* melalui jaringan dengan menggunakan perangkat seperti *Router* dan *Switch* layer-3 *(Switch Manage).*
6. *DataLink Layer*, Spesifikasi *IEEE 802* membagi Layer ini menjadi dua Layer anak, yaitu lapisan *Logical Link Control (LLC)* dan lapisan *Media Access Control (MAC)* befungsi untuk menentukan bagaimana *bit-bit* data dikelompokkan menjadi format yang disebut sebagai *frame.*

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

7. *Physical Layer*, berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi *bit*, arsitektur jaringan, topologi jaringan dan pengabelan.

Dari ke Tujuh layer tersebuat mempunyai 2 (dua) Tingkatan *Layer*, yaitu:

1. *Lower Layer* yang meliputi, *Physical Layer*, *DataLink Layer*, dan *Network Layer*. Bagaimana data mengalir pada *network* ditangani oleh layer ini dalam bentuk *hardware* maupun *software.*
2. *Upper Layer* yang meliputi *Transport Layer, Session Layer, Presentation Layer* dan *Application Layer*.Segala sesuatu yang berkaitan dengan *user interface*, data *formatting* dan *communicationsessions* ditangani pada layer ini.

2.2.11 Firewall Layer 7

Layer 7 atau biasa disebut juga layer aplikasi dari OSI Layer model memiliki dukungan aplikasi *end-user* seperti contohnya adalah HTTP dan SMTP. Oleh karena itu, jika layer ini diserang oleh *hacker* atau *virus* maka akan berakibat fatal, seperti penyusupan keamanan sistem ataupun pencurian data (jika yang diserang adalah perusahaan besar). Sehingga layer 7 menyediakan *firewall* yang dapat membantu menyaring atau melakukan *filtering* pada data-data yang masuk melewati layer 7 ini. Jika dibandingkan dengan *firewall* tradisional, kemampuan *filtering* pada *firewall* layer 7 lebih mumpuni. *Firewall* layer 7 melakukan penyaringan lebih baik daripada *firewall* tradisional. *Firewall* tradisional disini merujuk pada *firewall* yang ada pada layer 3 atau *session* layer. *Firewall* layer 7 juga mampu menganalisa data paket yang akan masuk sehingga *firewall* ini dapat membuat keputusan sendiri apakah paket data tersebut dapat diizinkan memasuki

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018

jaringan lokal. Contohnya *firewall* layer 7 dapat mengizinkan atau menolak Telnet dari pengguna lain ataupun pengguna tertentu sehingga hak akses pengguna tersebut dibatasi. Oleh karena *firewall* layer 7 dipilih oleh penulis karena fungsi dan kemampuan dari *firewall* itu sendiri sehingga jaringan lokal yang ada dapat dilindungi dengan maksimal ataupun dapat dilakukan pencegahan secara cepat dan tanggap.

Febrison Yohaness, Perancangan dan Implementasi Policy Management Layer 7 di Batam Tourism Polytechnic, 2018
UIB Repository©2018