BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

DPRD Provinsi Jawa Barat merupakan lembaga perwakilan rakyat daerah dan berkedudukan di Jawa Barat sebagai unsur penyelenggaraan pemerintahan daerah, di samping Pemerintah. Disamping itu DPRD Provinsi Jawa Barat ini mempunyai insfrastrukur IT yaitu sistem informasi dan sistem jaringan komputer untuk membantu dalam melaksanakan fungsi dan tugasnya.

Namun dalam sistem keamanan jaringan yang diterapkan pada lembaga ini terdapat permasalahan yaitu ancaman penyerangan dari luar jaringan komputer maupun dalam jaringan komputer tersebut. Berdasarkan hasil wawancara dengan Bapak Ibnu Rubianto selaku staff Penanggung Jawab IT yang mengawasi insfrastruktur dan keamanan jaringan, terdapat beberapa permasalahan yang terjadi dalam keamanan jaringan DPRD Provinsi Jawa Barat.

Permasalahan yang terjadinya pada sistem keamanan jaringan komputer DPRD Provinsi Jawa Barat diantaranya pada tahun 2009 terjadi beberapa kali penyerangan *deface* tarhadap *home page* dan Fraksi dalam kurun waktu yang berdekatan. Selanjutnya pada tahun 2010 terjadi ancaman serangan *deface* pada bagian modul agenda dan ditahun yang sama terjadi juga terjadi penyerangan *PHP Injection* dan *SQL Injection* dimana pengeksekusian *illegal query* dengan *drop database* dengan masuk kedalam *database server.* Kemudian pada tahun 2011 terjadi ancaman serangan *illegal content, malware* dan *spam mail*. Pada tahun antara 2012 sampai 2014 terjadi lagi penyerangan *deface* terhadap *web server*. Kemudian yang terakhir pada tahun 2015 terjadi sebuah penyerangan *spoofing* untuk pengakses terhadap *database server*. Pada saat ini sistem *control monitoring* masih terpisah - pisah sehingga penanggung jawab IT membutuhkan waktu yang lebih dalam *maintenance* dan mengevaluasi keamanan jaringan komputer.

Dari permasalahan yang sudah dijelaskan sebelumnya, maka salah satu solusi sistem teknologi yang bisa mengatasi malasah tersebut adalah dengan menggunakan sistem keamanan jaringan *Unified Threat Management* (*UTM*) *Firewall* berbasis *Linux*. Pada sistem keamanan *Firewall* sebelumnya akan dengan cepat menjadi usang di dalam era *Internet* saat ini di mana banyak aplikasi mengirim atau menerima yang menyebabkan lalu lintas lebih sibuk dari *Port* yang biasanya diperbolehkan oleh *Traditional Firewall*.

Sistem keamanan jaringan *Unified Threat Management* (*UTM*) *Firewall* berbasis *Linux* ini, mempunyai keunggulan dimana tidak hanya bisa melakukan satu fungsi keamanan sebagai *Firewall* saja, tetapi memiliki lebih dari satu fungsi. Keamanan jaringan seperti *Instrucion Detection* atau *Prevention* Sistem*, Anti-spam Web filter, Anti-virus* dan *Virtual Private Network* (*VPN*) dengan *management control monitoring centralize system* yang sesuai dengan permasalahan keamanan jaringan yang terjadi pada DPRD Provinsi Jawa. Sistem keamana jaringan yang terpisah, dengan *Router Mikrotik* yang saat ini difungsikan salah satunya sebagai sistem keamanan jaringan, sehingga membebankan kinerja pada *Router Mikrotik* tersebut.

Berdasarkan permasalahan yang dihadapi, pada penelitian ini dilakukan analisis dan perencanaan prototype sistem keamanan jaringan menggunakan *Unified Threat Management (UTM) firewall* berbasisi *Linux* yang berguna untuk mengatasi ancaman serangan yang sudah dijelaskan sebelumnya

1.2. Identifikasi Masalah

Berikut ini adalah identifikasi masalah pada kasus yang sudah terjadi pada sistem keamanan DPRD Provinsi Jawa Barat.

1. Terjadinya ancaman serangan *Deface* dan *Distributed Denial of Service DDos* pada *Web Server.*
2. Terjadinya ancaman serangan dari luar dan dalam jaringan DPRD Provinsi Jawa Barat seperti *PHP Injection* dan *SQL Injection* terhadap *database server* dengan eksekusi *query* tidak *valid* dengan mengakses *database server.*

3. Sistem keamanan jaringan untuk *web content filtering* yang berjalan saat ini memiliki celah terhadap *content illegal*.
4. Terjadinya aktivitas yang mencurigakan seperti *virus* dan *spam mail*
5. Terjadinya ancaman serangan *spoofing* dari dalam pada jaringan DPRD Provinsi Jawa Barat.
6. sistem keamanan yang bersifat terpisah – pisah dalam hal *monitoring* dan *control management* untuk Penanggung jawab IT DPRD Provinsi Jawa Barat terhadap *maintenance* pada jaringan DPRD Provinsi Jawa Barat.

1.3. Maksud dan Tujuan

Dalam melakukan penelitian ini adapun maksud dan tujuan penulis yang diterangkan sebagai berikut:

1.3.1. Maksud

Adapun maksud dari penelitian ini adalah analisis dan implementasikan sistem keamanan jaringan *Unified Threat Management* (UTM) *firewall* di lembaga Dewan Perwakilan Rakyat Daerah (DPRD) Provinsi Jawa Barat.

1.3.2. Tujuan

Adapun tujuan akhir yang ingin dicapai dalam penelitan ini adalah sebagai berikut.

1. Dengan menggunakan sistem keamanan jaringan *Unified Threat Management* (*UTM*) *firewall* berbasis *Linux* ini, dapat meminalkan dalam mengatasi ancaman serangan *DDos* dan *deface* pada *web server* DPRD Provinsi Jawa Barat ini.
2. Dengan menggunakan sistem keamanan jaringan *Unified Threat Management* (*UTM*) *firewall* berbasis *Linux* ini, diharapkan administrator jaringan dapat meminalkan dalam mengatasi dan meminimalkan ancaman serangan dari luar dan dalam terhadap jaringan di DPRD Provinsi Jawa Barat dengan mengakses *database server* seperti ancaman serangan *PHP Injection*, *SQL Injection* dan eksekusi *query* tidak *valid*.

3. Dengan menggunakan sistem keamanan jaringan *Unified Threat Management* (*UTM*) *firewall* berbasis *Linux* ini, dapat mencegah *content* yang bersifat *phishing.*
4. Dengan menggunakan sistem keamanan jaringan *Unified Threat Management* (*UTM*) *firewall* berbasis *Linux* ini, Pendeteksian aktivitas yang mencurigakan seperti *virus* dan *spam* pada jaringan DPRD Provinsi Jawa Barat ini dapat teratasi.
5. Dengan menggunakan sistem keamanan jaringan *Unified Threat Management* (*UTM*) *firewall* berbasis *Linux* ini, dapat meminalkan dalam mengatasi ancaman serangan *Spoofing.*
6. Dengan menggunakan sistem keamanan jaringan *Unified Threat Management* (*UTM*) *firewall* berbasis *Linux* ini, dapat menyederhanakan kontrol terpusat sehingga Penanggung Jawab IT dengan cepat bisa mengevaluasi sebuah keamanan jaringan ini.

1.4. Batasan Masalah

Adapun batasan - batasan masalah pada penelitian ini sehingga tidak melebar dari permasalahan yang ada adalah sebagai berikut:

1. Ruang lingkup penelitian ini adalah lembaga negera Dewan Perwakilan Rakyat Dearah (DPRD) Provinsi Jawa Barat.
2. Pengalamatan *IP Address* menggunakan *IPv4* pada jaringan internalnya.
3. Dalam pengalamatan *IP Adrees* tidak dibahas lebih dalam tentang *subnetting.*
4. Sistem operasi yang dijadikan sebagai *server Unified Threat Management firewall* adalah *Linux Endian Firewall.*
5. Sistem yang digunakan untuk memonitoring kontrol terpusat pada keamanan jaringan ini berbasis *web application.*
6. Sistem ini hanya digunakan hanya untuk Penanggun Jawab IT.
7. Tidak membahas teknologi jaringan *nirkabel (wireless)*.
8. Dalam penerapan sistem keamanan jaringan ini menggunakan *PC Desktop* sebagai *server*.

9. *Server Unified Threat Management* (UTM) *firewall* berbasis *Linux* hanya menggunakan dua modul *LAN Card*.
10. *Virtual Private Network* (VPN) digunakan untuk oleh Penanggung Jawab IT sebagai akses diluar jaringan komputer.

1.5. Metode Penelitian

Adapun penulis untuk tahapan – tahapan metodologi penelitian yang dilakukan oleh dalam penelitian ini adalah sebagai berikut:

1.5.1. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut:

a. Studi Literatur

   Pengumpulan data dengan cara mengumpulkan literatur, jurnal, dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

b. Observasi

   Pengumpulan data dengan mengadakan peninjauan langsung terhadap permasalahan yang diambil.

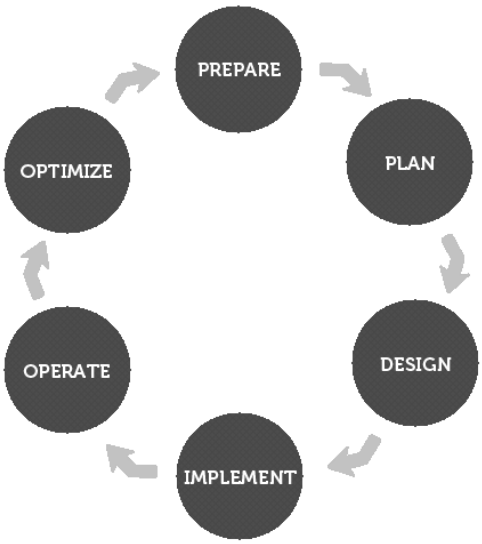
c. Wawancara

   Pengumpulan data dengan melakukan tanya jawab kepada staff Penanggung Jawab IT DRPRD Provinsi Jawa Barat yang selama ini terlibat dalam penentuan kebijakan - kebijakan dan pengelolaan jaringan dan keamanan komputer.

1.5.2. Metode Pengembangan Sistem

Metode yang dipakai pada perancangan sistem keamananini adalah *Cisco Lifecycle Services* atau *PPDIOO* yang merupakan singkatan dari *Prepare, Plan, Design, Implement, Operate, and Optimize.Cisco Lifecycle Services* adalah pendekatan dengan enam fase. Setiap fase mendefinisikan aktifitas yang dibutuhkan untuk mensukseskan penyebaran dan pengoperasian teknologi jaringan. Fase-fase ini juga mendefinisikan bagaimana mengoptimalkan kinerja di

seluruh siklus hidup suatu jaringan. *Cisco Lifecycle Services* juga biasa disebut dengan metode *PPDIOO* yang merupakan singkatan dari huruf pertama pada setiap fase yang dilalui [1].



Gambar 1. 1 *PPDIOO*

(*Sumber: http://www.ccexpert.us/network-design/images/7896_51_44.jpg)*

Berdasarkan penjelasan pada gambar 1.1 metode yang digunakan dalam proses penelitian dilakukan dengan mempersiapkan teknologi keamanan jaringan yang akan dibangun, merencanakan seperti apa jaringan yang akan dibangun, mendesain jaringan sesuai dengan yang direncanakan, mengimplementasikan desain yang sudah dibuat, pengoperasian sehari-hari untuk membantu mencapai skalabilitas maksimum, ketersediaan, keamanan dan pengelolaan jaringan yang dibuat dengan mengoptimalkan jaringan yang bertujuan untuk meningkatkan kinerja jaringan dan kehandalan dengan mengidentifikasi dan mengatasi masalah jaringan sebelum terjadi kerusakan. Metode ini dirancang untuk mendukung perkembangan sistem jaringan komputer. Adapun keuntungan dari metode ini adalah menurunkan total biaya dengan melakukan validasi terhadap kebutuhan teknologi yang akan diterapkan serta perencanaannya dan meningkatkan *availability* dari jaringan. Meningkatkan fleksibilitas, disamping itu metode ini mempercepat akses ke aplikasi dan layanan dengan meningkatkan ketersediaan, kehandalan, keamanan, skalabilitas, dan kinerja dari jaringan [1].

a. *Prepare*

Dalam model pengembangan sistem *PPDIOO*, fase pertama adalah *Prepare*. Pada fase ini dilakukan proses identifikasi masalah, mengidentifikasi konsep dari sistem yang akan diimplementasikan, jenis dan tipe penerapannya, serta komponen pendukung yang akan dikonfigurasi.

b. *Planning*

Dalam fase ini, mulai dibuat perencanaan dari hasil identifikasi masalah, seperti komponen yang dibutuhkan dalam implementasi sistem keamanan *Unified Threat Management (UTM) Firewall*, jenis *server* yang mendukung dalam implementasi. Selain itu kebutuhan user akan di analisa dalam fase ini.

d. *Design*

Dalam fase ini, dirancang topologi jaringan yang baik dalam implementasi *Unified Threat Management (UTM) Firewall* berbasis *Linux*.

e. *Implement*

Dalam fase ini, dilakukan penerapan atas semua yang telah direncanakan. Tahap implement, mencangkup instalasi sistem operasi dan *device*s yang akan digunakan sesuai dengan topologi yang sudah dirancang, konfigurasi dan pengujian pada *Unified Threat Management (UTM) Firewall* berbasis *Linux* yang diimplementasikan.

e. *Operate*

Dalam fase ini, hasil implementasi mulai dioperasikan, untuk menyesesuaikan dengan analisa awal dengan implementasi dan menentukan aktor yang terlibat dalam pengoperasian *Unified Threat Management (UTM) Firewall* berbasis *Linux*. Disamping itu tindakan *monitoring* dan *maintenance* berada dalam fase ini.

f. *Optimize*

Fase yang terakir adalah *optimize* dimana dalam fase ini Penanggung Jawab IT berhak membuat kebijakan khusus dalam penambahan performasi dalam sistem yang telah diimplementasikan. Sebagai contoh penambahan sistem kontrol

monitoring terpusat untuk monitoring dan evaluasi keamanan sistem jaringan di DPRD Provinsi Jawa Barat.

1.6. Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini disusun untuk memberikan gambaran umum tentang tugas akhir yang dijalankan. Sistematika penulisan laporan tugas akhir ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini berisi latar belakang, identifikasi masalah, maksud dan tujuan, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi profil singkat perusahaan dan landasan teori yang berkaitan dengan permasalahan yang dikaji.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi analisis sistem keamanan jaringan komputer menggunakan *Unified Threat Management (UTM) Firewall* berbasis *Linux* yang sesuai dengan metode pembangunan jaringan yang digunakan.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi hasil implementasi seperti tahapan instalasi dan konfigurasi terhadap system keamanan jaringan komputer *Unified Threat Management* (*UTM*) *Firewall* berbasis *Linux* yang diimplementasikan dalam bab ini dan juga berisi hasil-hasil pengujian.

BAB 5 KESIMPULAN DAN SARAN

Bab ini merupakan penutup penyusunan laporan yang berisi kesimpulan yang didapatkan dari hasil implementasi dan pengujian, serta bab ini juga berisi saran perbaikan yang diusulkan untuk dapat dilakukan di waktu yang akan datang.