BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari hasil uraian bab-bab sebelumnya, dapat dikemukakan beberapa kesimpulan pokok dari hasil penelitian ini, yaitu:

1. Ancaman serangan *DDos* dan *deface* pada *web server* di DPRD Provinsi Jawa Barat, dapat diminimalkan dengan mengkombinasikan antara *firewall* dan *Intrusion Prevent System (IPS)* pada *Unified Threat Management (UTM) firewall* berbasis *Linux*.
2. Pengaksesan *database server illegal diikuti dengan* ancaman serangan seperti *PHP Injection*, *SQL Injection* dan eksekusi *query* tidak *valid* dapat diminimalkan dengan kombinasi *firewall* dan *Intrusion Prevent System (IPS)* pada *Unified Threat Management (UTM) firewall* berbasis *Linux*.
3. Ancaman yang bersifat *phising* dengan memafaatkan *content illegal* dapat dicegah dengan *conternt filtering* pada *Unified Threat Management (UTM) firewall* berbasis *Linux*.
4. Aktivitas yang mencurigakan seperti *virus* dan *spam* pada jaringan DPRD Provinsi Jawa Barat ini, dapat teratasi dengan mengkombinasikan sistem keamanan jaringan *antivirus* dan *content filtering* pada *Unified Threat Management (UTM) firewall* berbasis *Linux.*
5. Ancaman serangan *spoofing* dapat diatasi dengan penerapan aturan *firewall* dan *Intrusion Prevent Sysem (IPS)* pada *Unified Threat Management (UTM)* berbasis *firewall*.
6. *System control* keamanan yang masih terpisah – pisah dapat di sederhanakan dengan terpusat pada *Unified Threat Management (UTM) firewall* berbasis *Linux* sehinga Penanggung Jawab IT dengan cepat bisa mengevaluasi sebuah keamanan jaringan ini seperti *monitoring, file logs* dan *notification.*

5.2. Saran

Hasil-hasil penelitian ini akan lebih bermanfaat jika dilakukan studi lanjut untuk menyempurnakan hasil-hasil yang telah dicapai. Oleh karena itu disampaikan beberapa saran sebagai berikut:

1. Perlunya dilakukan pemantauan jaringan secara rutin dan menyeluruh terhadap kondisi jaringan internal DPRD Provinsi Jawa Barat untuk keamanan dan kelancaran jaringan yang berkelanjutan
2. Sebaiknya spesifikasi *hardware* tinggi digunakan untuk *server Unified Threat Management* (UTM) *Firewall* terhadap fungsi ketahanan dalam mendukung *performance*
3. Sebaiknya dalam melakukan audit sistem keamanan jaringan komputer DPRD Provinsi Jawa Barat ini dilakukan setiap bulan sekali. Hal ini dimaksudnya untuk mengevaluasi dengan cepet terdapat ancaman model baru.
4. Sebaiknya dilakukan analisis lebih lanjut antara *lisence commercial Unified Threat Management* (UTM) *Firewall* dengan *free Unified Threat Management* (UTM) *Firewall* untuk mengetahui unsur *reliability* yang terbaik.
5. Sebaikanya *access security* terhadap *server Unified Threat Management* (UTM) *Firewall* ini dilakukan dengan aturan yang sangat ketat
6. Sebaiknya *server Unified Threat Management* (UTM) *Firewall* melakukan *backup* dan *recovery* sistem setiap bulanya untuk mengantisipasi kejadian yang tidak terduga seperti *crash* pada *server.*
7. Sebaiknya Penanggung Jawab IT DPRD Provinsi Jawa Barat selalu melakukan *update* terhadapat database *virus, spyware* dan *snort*
8. Penambahan modul *Lan Card* pada server *Unified Threat Management* (UTM) *Firewall* sangat dibutuhkan ketika

9. Memeriksan halaman *web software Endian firewall Unified Threat Management* (UTM) di **http://www.endian.com** untuk melakukan *upgrade* pada sistem yang lebih baru telah di-*release*