BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil penelitian yang dilakukan penulis, mulai dari tahap perancangan *Hardware* dan implementasi, sampai pada tahap pengujian konektifitas, kesimpulan yang dapat diambil dari pelaksanan penelitian ini adalah sebagai berikut :

1. Metode penelitian yang digunakan dalam penelitian ini adalah metode non *transparent proxy* sebagai metode pencegahan pengalihan *web*
2. Metode ini menggunakan konfigurasi WPAD (*Web Proxy Auto Discovery*) adalah metode pengalihan *web* ke *server proxy* dan *server proxy* hanya meneruskan *packet* yang menuju kepadanya.
3. Sistem ini harus menginputkan *packet database blacklist* sebagai *web filtering*
4. Metode non *transparent proxy* dapat menggunakan *Web Proxy Auto Discovery*, agar setiap *user* tidak perluh melakukan penginputan IP *address* dan port *proxy* pada setiap *web browser*.
5. Penggunaan *tools* byapssing *content filtering*, adalah proses pengalihan *web* dari ISP ke *server proxy* lain, hal ini terjadi pada port 80 (HTTP) dan port 443(HTTPS) yang harus di blokir.

AMIKOM RESOURCE CENTER YOGYAKARTA

5.2 Saran

Untuk pengembangan dan penyempurnaan sistem dalam melakukan tugas *filtering* terdapat saran-saran sebagai berikut :

1. Penambahan RAM (*Random Access Memory*) harus diperhatikan dalam penelitian dan pengembangan selanjutnya. Terutama dalam melakukan konfigurasi *firewall filtering*.
2. Memilih perangkat untuk pengupgradetan, harus diperhatikan dengan spesifikasi versi OS pfSense.
3. Pencegahan *user* melewati penyaringan konten negatif, dapat dicegah dengan memahami proses TCP/IP dan membuat *rules protocol* sesaui dengan kebutuhan sistem
4. Perancangan PC router untuk jumah *client* yang banyak dapat disesuaikan dengan spesifikasi komputer yang tinggi untuk *proxy server*.
5. Penerapan keamanan jaringan dengan packet aplikasi yang berbeda diharapkan tidak dilakukan dalam 1 PC *router* karena selain memberatkan sistem, sistem akan menjadi *crash* karena harus melakukan proses yang banyak
6. *Packet database blacklist* yang digunakan adalah bersifat *free*, untuk pemblokiran konten bermuatan negatif agar lebih optimal dapat menggunakan *packet database commercial*.
7. Pengupgradetan NIC *interface* untuk mendapatkan *speed* dan *duplex*

harus sama, karena kecepatan tidak dapat dipaksakan. Ketidak cocokan / *duplex* akan menghasilkan kesalahan dan konektifitas yang terdegradasi. Kesalahan akan menghasilkan kesalahan *In / Out* dan *Collisions*.

8. Dalam *instalasi* packet *firewall filtering* harus diperhatikan aturan *instalasi*.
9. Dalam penelitian ini penulis masih mendapatkan beberapah *domain*, URL *web proxy* dan konten pornografi yang masih lolos sensor *filtering*. Agar sistem ini lebih sempurnah peneliti menganjurkan untuk melakukan pengupgradetan *database Blacklist Commercial* (Berbayar).
10. Metode pencegahan penggunaan *tools server proxy* dan VPN serta metode *filtering web*, tidak dapat di filter dalam satu konfigurasi saja. Hal ini harus dibedahkan dalam setiap langkah-langkah yang ingin kita terapkan.
11. Kategori konten bermuatan negatif dapat di filter sesuaikan dengan kebutuhan di lapangan, hal ini disebabkan setiap instansi memiliki pandangan yang berbedah-bedah mengenai konten bermuatan negatif.
12. *Rules protocol* dapat di sesuaikan dengan kebutuhan dalam setiap konfigurasi, baik menambahkan atau mengurang aturan tersebut.
13. Pengembangan dapat di tingkatkan dengan menggunakan pfBlockerg sebagai *web filtering* dalam satu *server proxy* tetapi harus meningkatkan jumlah RAM.

14. Pengembangan dapat di tingkatkan dengan metode *safe search* berbasis DNS.
15. Untuk metode *redirect web* berbasis HTTPS (443) harus menggunakan *Certificate* berbayar agar proses dapat dilakukan.
16. Untuk konfigurasi WPAD dapat di konfigurasi sesuai kebutuhan sistem.
17. Metode *transparent proxy* adalah metode dimana *user* tidak perluh menginputkan IP *address* dan port *proxy*, hal ini karena semua request di dengarkan oleh port 80 (HTTP) sebagai pengalihan *web* (WWW) dan menuju port *proxy*. Hal ini dapat menyaring konten bermuatan negatif tetapi tidak dapat menyaring penggunaan *tools* yang melewati konten *filtering*.
18. Metode *transparent proxy* tidak dapat menyaring *web*site berbasis HTTPS (port 443), kecuali membuat *Certivficate Authority* (CAs).