BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring dengan perkembangan dan kemajuan teknologi keamanan jaringan komputer merupakan prioritas yang sangat penting untuk diperhatikan saat ini, banyak negara-negara yang membangun infrastruktur jaringan untuk mencegah konten negatif seperti sekolah, warnet, perusahaan, dan lembaga pemerintahan. Menurut badan Komunikasi dan Informatika dengan aplikasi TRUST+Positif, konten yang bermuatan negatif adalah konten yang mengandung unsur-unsur Pornografi, Radikalisme, Sara, Kekerasan, Penipuan, Perjudian, Keamanan, Hak Cipta, dan Narkoba. Pemblokiran konten yang bermuatan negatif sesuai dengan peraturan Menteri Komunikasi dan Informatika nomor 19 Tahun 2014, adalah upaya yang dilakukan agar situs internet bermuatan negatif tidak dapat diakses, tujuan ini dilakukan agar melindungi kepentingan umum dari konten *internet* yang berpotensi memberikan dampak negatif atau merugikan [1].

Metode penelitian dengan menggunakan DNS *server* sebagai *filtering* konten negatif menggunakan metode RPZ (Sani Muhlison, 2015) [2], dan implementasi *firewall* dengan menggunakan Mikrotik *RouterOS* (Muhammad Abdul Muin, Bambang Sugiantoro, 2017) [3], adalah dua metode *filtering* yang bekerja pada *application layer* model TCP/IP yang berfungsi untuk memfilter konten yang bermuatan negatif dan mengalihkan halaman *web* tersebut ke halaman pencarian yang bersih, akan tetapi kedua metode ini memiliki kelemahan pada tingkat *user* yang dapat melakukan *surfing* dengan menggunakan *tools*

tertentu agar dapat menembus sensor *filtering* yang berhasil dikembangkan oleh banyak aktivis, *programmer* dan sukarelawan, yang disebabkan oleh bertambahnya pemfilteran konten.

Metode *filtering* yang ada saat ini, sangat mungkin untuk dapat dihindari dengan menggunakan komputer perantara untuk mengakses layanan yang telah di blokir, proses ini sering disebut dengan *Censorship Circumvention* (menembus penyensoran), sedangkan komputer perantara disebut *Proxy*. *Server proxy* merupakan *server* yang berfungsi sebagai perantara antara komputer *client* dengan *server* lain [4]. *Server proxy* yang di kembangkan secara sukarela atau *non profit* tidak menyediakan *database* khusus sebagai *web filtering*, oleh sebab itu *proxy* jenis ini banyak digunakan oleh *user* dalam mengakses konten yang telah di blokir. Metode keamanan dengan menggunakan *squid proxy* sebagai *forward proxy* yang bekerja pada *Transport layer* dan *Aplication layer* model TCP/IP, diharapkan mampu mencegah pengalihan *web* ke eksternal *proxy* dan memblokir konten yang mengandung unsur-unsur konten negatif. Sistem yang dibangun adalah sistem yang bersifat independen.

Hal ini dilakukan karena *server* TRUST+Positi pusat tidak berfungsi sebagai *single gateway* ataupun *traffic relay* untuk koneksi internet seluruh Indonesia. Dan Kementerian Komunikasi dan Informatika tidak mengakomodir *traffic internet* bagi seluruh ISP ataupun organisasi penggunaan TRUST+Positif yang ada di Indonesia. Masing-masing pengguna akan menyediakan infrastruktur sesuai dengan kebutuhan yang ada pada zona masing-masing, dimana TRUST+Positif akan berfungsi sebagai referensi atau rujukan *database* URL

internet sehat [5].

Oleh sebab itu, penulis sangat tertarik untuk melakukan *research* tentang sistem pencegahan *user* melewati penyaringan konten negatif, menggunakan *proxy server* sebagai *forward proxy* atau *gateway* antara jaringan *local* dan jaringan *public*. Sistem ini menggunakan OS pfSense berbasis *(Open Source)* yang di *install* pada sebuah PC (*Personal Computer*).

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana merancang dan mengimplementasikan *firewall proxy server* sebagai *forward proxy* untuk mengamankan konten yang bermuatan negatif agar tidak dapat di akses oleh *user* dengan menggunakan *tools* yang dapat memotong aspek teknis penyaringan konten bermuatan negatif dan mengintegrasikan *packet database blacklist* ke dalam sistem yang dibangun.

1.3 Batasan Masalah

Pembahasan mengenai *firewall filtering* secara detail merupakan pembahasan yang luas dan memiliki pembagian-pembagian yang sangat kompleks. Namun dalam hal ini penulis membatasi pembahasan *firewall filtering* dalam cakupan mengamankan konten negatif agar tidak dapat diakses oleh *user* menggunakan *firewall proxy server*.

Batasan masalah yang akan dijadikan pedoman dalam pelaksanaan penelitian yaitu:

1. Spesifikasi PC *router low end*, disesuaikan dengan kebutuhan dan implementasi.
2. Perakitan alat PC *router* tidak dibahas pada penelitian.
3. Penelitian difokuskan pada permasalahan yang diteliti yaitu (sistem pencegahan user melewati penyaringan konten negatif).
4. Peneliti tidak fokus pada kecepatan proses *request cache*, karena berbeda masalah yang diteliti.
5. *Filtering* konten negatif dibahas dalam penelitian, karena sebagai hasil pengujian *system* (*output*). Dan beberapa *domain* yang diblok oleh penulis yang tidak ada dalam *packet database SquidGuard*.
6. Kategori konten negatif di blokir berdasarkan kata kunci TRUST+Positif.
7. *Domain* penyedia layanan *web proxy* diblokir oleh penulis.

1.4 Maksud dan Tujuan Penelitian

Maksud dari penelitian adalah :

1. Mengembangkan ilmu yang dimiliki oleh penulis tentang jaringan komputer.
2. Mengembangkan dan mengimplementasikan ilmu yang dimiliki oleh penulis selama mempelajari pfSense.
3. Bagaimana memanfaatkan OS (*Operating System*) *Open Source* sebagai *firewall*.
4. Membuat teori karya ilmu sebagai ilmu pengembangan dan pengetahuan dalam bidang informatika.

5. Memanfaatkan komputer sebagai *router proxy server*.

Tujuan dari penelitian ini adalah :

1. Merancang dan mengimplementasikan PC (*Personal Computer*) sebagai *forward proxy* untuk jaringan *internet* dalam membatasi hak akses konten yang bermuatan negatif.
2. Meminimalisir hak akses konten yang bersifat privasi.
3. Untuk meningkatkan *internet* sehat dan aman dalam melakukan *surfing*

1.5 Manfaat Penelitian

1. Bagi peneliti
   a. Memanfaatkan ilmu yang didapat dari referensi
   b. Dapat mengetahuhi kelemahan dan kelebihan *proxy server* yang telah ada (sesuai dengan komfigurasi yang diterapkan)
   c. Menambah wawasan bagi penulis dalam melakukan penelitian *firewall filtering*.
   d. Penelitian yang didapat, dapat dikembangkan dan digunakan dalam dunia kerja.
   e. Dapat di implementasikan bagi masyarakat yang membutuhkannya.
2. Bagi ilmu pengetahuan
   a. Dapat menjadi referensi bahan pembelajaran tentang fungsi *Squid proxy*.

b. Dapat menjadi pertibangan dan kebutuhan sesuai dengan kebutuhan dalam merancang dan membangun sebuah jaringan.

1.6 Metode Penelitian

Sebagai usaha dalam memperoleh data yang relevan dan terarah sesuai dengan permasalahan yang telah dihadapi, maka perlu adanya suatu metode yang tepat untuk mencapai tujuan dalam penelitian, untuk itu penulis menggunakan beberapa metode dalam penelitian skripsi ini, yaitu:

1.6.1 Mengumpulkan Data

1. Studi Literatur

   Mengumpulkan data-data dengan membaca buku dan membuka situs-situs *internet* yang mendukung dan menunjang dalam penelitian ini.

2. Studi Kasus

   Dalam melakukan penelitian ini, penulis melakukan pengujian langsung dan mengamati sisi keamanan *firewall* pada Universitas Amikom Yogyakarta dengan memanfatkan akses *internet* jaringan *local* (*Wired* dan *Wireless*).

3. Diskusi (*sharing*)

   Metode ini dilakukan dengan melakukan diskusi langsung terhadap *user* yang melakuan koneksi yang bersifat privasi dalam mengakses konten negatif.

4. Metode kuesioner

   Metode ini digunakan untuk mendapatkan jawaban atau *tools* yang digunakan oleh setiap *user* untuk melewati akses penyaringan konten negatif.

1.6.2 Analisis

Pada tahap ini, penulis melakukan identifikasi masalah menggunakan metode *Grounded Theory*, selain itu juga terdapat analisis kebutuhan fungsional dan kebutuhan non-fungsional.

1.6.3 Perancangan

Metode perancangan yang dilakukan oleh penulis adalah dengan melalui tahap pembuatan *flowchart* yang dibuat sesuai dengan cara kerja sistem.

1.6.4 *Testing* (Pengujian Sistem)

Untuk mengetahui ke akuratan dan kesempurnaan sistem, agar dapat digunakan. Penulis melakukan pengujian pada sisi *user* dengan melakukan (*Bypassing Filtering Content Negative*).

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan penulis dalam menulis laporan penelitian ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, maksud penelitian, tujuan penelitian, dan metode untuk melakukan penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi kajian pustaka dan uraian teori-teori yang mendasari pembahasan yang berhubungan dengan penelitian.

BAB III ANALISIS DAN PERANCANGAN

Bab ini berisi hasil penelitian, mulai dari tahapan analisis, dan perancangan yang akan menjadi *ouput* dari penelitian ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang instalasi dan konfigurasi sistem, serta pengujian sistem, hasil pengujian dan tampilan hasil akhir.

BAB V PENUTUP

Bab ini berisi uraian kesimpulan dan saran yang diambil dari pembahasan yang telah dibuat.