

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi Informasi merupakan ilmu pengetahuan yang sekarang ini sedang berkembang dengan pesat. Seiring dengan perkembangan zaman, TI memberikan pengaruh yang luar biasa bagi kemajuan ilmu pengetahuan yang bisa dimanfaatkan bagi setiap orang. Teknologi informasi yang sedang berkembang saat ini, telah mendorong di berbagai bidang. Secara langsung ataupun tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Karena banyak kemudahan yang ditawarkan, teknologi informasi hampir tidak dapat dilepaskan dari berbagai aspek kehidupan manusia. Seseorang dapat dengan mudah mendapatkan informasi, referensi, pengetahuan, wawasan dan lain-lain yang di dapat melalui TI [1].

Dengan perkembangan teknologi informasi tersebut memungkinkan suatu informasi diakses dimana saja, dan kapan saja, sehingga sangat membantu mobilitas. Apalagi dengan kemajuan teknologi *wireless* yang sangat menunjang mobilitas pengguna. Dengan *hotspot* pengguna jaringan bisa menikmati akses internet dimanapun berada selama di area *hotspot* tanpa harus menggunakan kabel [1].

Dengan mudah dan bebasnya pengaksesan terhadap teknologi informasi tersebut tidak menutup kemungkinan akses internet bisa disalahgunakan untuk hal-hal yang negatif seperti pengaksesan *website* yang mengandung konten-konten negatif, seperti pornografi, judi dan sebagainya. Sehingga suatu sistem

keamanan jaringan khususnya metode *filtering* menjadi salah satu aspek yang sangat penting untuk diterapkan di jaringan internet [2].

Dari permasalahan tersebut maka diperlukan sistem yang dapat menjadi *firewall* yang handal dalam mengamankan jaringan internet. *PfSense* adalah distribusi dari *FreeBSD* yang bersifat *open-source* dan dirancang khusus sebagai *firewall* dan *router* yang sepenuhnya dikelola melalui antarmuka web [2]. *PfBlockerNG* adalah sebuah paket yang dapat di-*install* pada sistem operasi *pfSense* yang berfungsi sebagai *firewall filtering*. *PfBlockerNG* mempunyai salah satu fitur DNSBL (*Domain Name System-based Blackhole List*), yang bekerja sebagai *firewall filtering* untuk mengatasi permasalahan tersebut.

Tujuan utama dari penelitian ini yaitu dapat memblokir situs-situs yang mengandung konten-konten negatif seperti pornografi, judi dan sebagainya menggunakan *pfBlockerNG* dengan metode DNSBL (*Domain Name System-based Blackhole List*).

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka dapat dirumuskan suatu masalah yaitu bagaimana menerapkan keamanan jaringan berbasis *pfBlockerNG* menggunakan metode DNSBL (*Domain Name System-based Blackhole List*) sebagai pembatasan akses *website* yang dianggap negatif?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini dipaparkan sebagai berikut:

1. Spesifikasi PC *router low end*, disesuaikan dengan kebutuhan dan implementasi.
2. Perakitan PC *router* tidak dibahas pada penelitian ini.
3. *Firewall* yang digunakan adalah *pfSense* distribusi dari *freeBSD*.
4. Konfigurasi dilakukan secara GUI (*Graphical User Interface*) bukan CLI (*Command-Line Interface*).
5. Menggunakan *package pfBlockerNG* dari *pfSense* untuk *filtering*.
6. Menggunakan fitur DNSBL dari *pfBlockerNG* untuk URL *filtering* konten-konten negatif seperti, pornografi, judi dan sebagainya.
7. Tidak membahas tentang *bypassing filtering website*.

1.4 Maksud Penelitian

Maksud dari penelitian dengan judul "Implementasi DNSBL (*Domain Name System-based Blackhole List*) sebagai *Filtering* Konten Negatif menggunakan *Firewall pfBlockerNG*," untuk memenuhi persyaratan dalam mencapai gelar sarjana pada program studi S1 Informatika di Universitas AMIKOM Yogyakarta.

1.5 Tujuan Penelitian

Berdasarkan uraian dari latar belakang masalah maka penelitian memiliki tujuan penelitian yaitu:

1. Mampu merancang dan mengimplementasikan PC (*Personal Computer*) sebagai *firewall filtering* untuk membatasi hak akses situs-situs tertentu menggunakan *pfSense*.
2. Untuk meningkatkan layanan internet yang sehat dan aman dalam melakukan *browsing*.

1.6 Manfaat Penelitian

1.6.1 Bagi Penulis

Hasil penelitian ini oleh peneliti diharapkan bermanfaat untuk:

1. Memperoleh gelar Sarjana Komputer pada Universitas AMIKOM Yogyakarta.
2. Memanfaatkan ilmu yang didapat dari referensi.
3. Meningkatkan pemahaman dan pengetahuan dalam keamanan jaringan khususnya *filtering*.
4. Mengetahui lebih detail dan fungsi dari *pfSense* sebagai keamanan jaringan khususnya *filtering*.
5. Sebagai bekal untuk memasuki dunia kerja yang saat ini telah menggunakan teknologi tersebut.
6. Dapat di implementasikan bagi masyarakat yang membutuhkan.

1.6.2 Bagi Universitas

1. Mengetahui kemampuan mahasiswa dalam menguasai materi yang telah diterima selama di perkuliahan.
2. Mengetahui kemampuan mahasiswa dalam menerapkan ilmu-ilmunya dan sebagai bahan evaluasi.

1.6.3 Bagi Pembaca

1. Sebagai informasi mengenai keamanan jaringan khususnya *filtering*.
2. Sebagai tolak ukur bagi peneliti selanjutnya untuk dapat menyempurnakan sistem keamanan ini.

1.7 Metode Penelitian

Dalam menyusun penelitian skripsi ini ada beberapa metode yang digunakan, antara lain:

1.7.1 Metode Pengumpulan Data

Untuk mendapatkan data yang benar dan relevan sesuai topik yang dibuat, maka diperlukan metode yang tepat untuk mencapai maksud dan tujuan penelitian. Adapun sumber-sumber data untuk keperluan penelitian ini menggunakan metode-metode berikut ini:

1. Studi Literatur

Untuk menambah referensi yang relevan akan teori-teori yang diperlukan, penulis melakukan studi literatur dengan membaca dan mempelajari secara literatur yang mendukung penelitian ini. Referensi

ini dapat dicari dari buku, jurnal, artikel, laporan penelitian, dan situs-situs di internet yang berhubungan dengan materi skripsi ini.

2. Metode Eksperimen

Metode ini melakukan percobaan teknik DNSBL (*Domain Name System-Based Blackhole List*) sebagai *filtering* konten negatif menggunakan *firewall pfBlockerNG*.

1.7.2 Metode Analisis Perancangan

Pada tahap ini penulis akan menganalisis, mengumpulkan data dan mempersiapkan kebutuhan alat, menggunakan metode NDLC (*Network Development Life Cycle*), untuk mendapat perancangan dari konfigurasi yang akan di implementasikan.

1.7.3 Metode Implementasi

Pada tahap ini, penulis melakukan implementasi rancangan yang telah di buat dan akan melakukan analisa terhadap kehandalan dari sistem yang telah dibuat.

1.7.4 Metode Pengujian

Pada metode pengujian ini dilakukan untuk mengetahui ke akuratan dan kesempurnaan sistem, agar dapat digunakan. Penulis melakukan pengujian pada sisi *user* dengan mencoba mengakses situs yang berkonten negatif.

1.8 Sistematika Penulisan

Penulis skripsi yang berjudul “Implementasi DNSBL (*Domain Name System-based Blackhole List*) sebagai *Filtering* Konten Negatif menggunakan *Firewall pfBlockerNG*” mempunyai sistematika penulisan sebagai berikut:

BAB I

PENDAHULUAN

Bab ini merupakan pendahuluan yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II

LANDASAN TEORI

Bab ini menjelaskan landasan-landasan teori yang digunakan sehubungan dengan Implementasi DNSBL (*Domain Name System-based Blackhole List*) sebagai *Filtering* Konten Negatif menggunakan *Firewall pfBlockerNG*.

BAB III

METODE PENELITIAN

Berikutnya dalam bab ini akan diuraikan mengenai hasil analisa dan perancangan yang hasilnya akan menjadi implementasi.

BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini akan membahas tentang hasil perancangan yang telah di implementasikan dan pembahasan hasil implementasi.

BAB V**PENUTUP**

Pada bab ini berisi kesimpulan dan saran dari perumusan masalah yang telah disampaikan.

