BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Internet Service Provider (ISP) atau penyedia layanan internet di Indonesia, diwajibkan melakukan pemblokiran terhadap situs-situs yang terdapat dalam *TRUST*+Positif. Hal ini sesuai dengan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 19 Tahun 2014 Pasal 8 Ayat (1). Dengan adanya peraturan ini, diharapkan dapat menjauhkan masyarakat dari dampak negatif internet.

Dari hasil wawancara penelitian yang penulis lakukan di SMA Negeri 27 Bandung, disana sudah melakukan pemblokiran pada situs - situs yang terdapat pada *TRUST*+Positif melalui keamanan dari ISP yang mereka gunakan yaitu Indihome. Akan tetapi, disana tidak melakukan keamanan tambahan yang menyebabkan masih ada celah untuk melewati keamanan internet positif yang diberlakukan oleh ISP. Oleh karena itu, penulis memiliki ide untuk melakukan keamanan jaringan tambahan untuk mengoptimalisasikan pemblokiran terhadap situs berkonten negatif.

Dalam mencegah hal diatas dibuatlah sebuah mekanisme dalam upaya menjaga keamanan jaringan atau biasa disebut dengan *Firewall*. *Firewall* adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang tidak aman. Umumnya, sebuah *firewall* diimplementasikan dalam sebuah mesin terdefikasi, yaitu berjalan pada gerbang *(gateway)* antara jaringan lokal dan jaringan lainnya. *Firewall* umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar.

Keamanan yang akan penulis terapkan disana yaitu dari sisi DNS, Proxy, dan juga VPN. Keamanan dari sisi DNS menggunakan *Transparent DNS* yang dimana setiap paket data yang melewati *router* akan dikirim ke DNS ISP terlebih dahulu. Dengan begitu, walaupun *client* menganti DNS miliknya, paket data yang lewat akan dikirim ke DNS milik ISP terlebih dahulu. Ibaratnya seperti kita memaksa *client* untuk masuk ke DNS milik ISP.

Selain dari DNS, celah lain untuk melakukan *bypass* internet positif adalah dengan menggunakan *Proxy* dan juga VPN. Oleh karena itu, penulis juga akan mencoba menerapkan pemblokiran penggunaan *Proxy* serta VPN dengan menggunakan *firewall L7 Protocol* dari Mikrotik untuk mencegah *client* mengakses konten internet negatif.

Sesuai kesepakatan dengan kepala sekolah serta staff IT disana, mereka ingin bisa melihat akses apa saja yang dilakukan oleh siswa yang menggunakan internet di SMA Negeri 27 Bandung. Sehingga, jika masih ada yang terlihat menggunakan internet untuk hal yang tidak wajar, bisa ditindaklanjuti dengan hukuman seperti pemberhentian akses internet selama waktu yang ditentukan atau bisa ditegur oleh pihak yang terkait.

Berdasarkan latar belakang masalah diatas maka penulis bermaksud mengambil topik tugas akhir ini dengan judul "Penerapan Transparent DNS, Pencegahan Penggunaan Proxy dan VPN Dengan Firewall Metode Layer 7 Protocol Mikrotik Untuk Optimalisasi Filtering Konten Negatif Serta Implementasi di SMAN 27 Bandung".

1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang, maka dapat diidentifikasi masalah-masalah yang ada adalah sebagai berikut :

1. Siswa masih bisa membuka situs berkonten negatif dengan menggunakan DNS Eksternal
2. Siswa masih bisa menggunakan Proxy dan VPN sehingga tidak terkontrol lalu lintas datanya dan digunakan untuk membuka situs yang diblokir
3. Belum ada penindakan untuk siswa yang menggunakan internet di sekolah untuk hal yang tidak wajar.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah meningkatkan keamanan jaringan dari sisi *client* agar lebih optimal. Sedangkan tujuan dari dilakukannya penelitian ini adalah sebagai berikut :

1. Menerapkan *Transparent DNS* agar *client* tetap menggunakan *DNS* milik *ISP* meskipun mengganti pengaturannya
2. Memblokir situs-situs penyedia layanan *Proxy dan* VPN *Service* menggunakan *L7 Protocol* Mikrotik
3. Menerapkan pemutusan akses internet kepada *client* selama 1 menit jika masih mencoba menggunakan internet untuk membuka situs negatif.

1.4 Batasan Masalah

Adapun batasan-batasan masalah yang ada di dalam penelitian ini meliputi:

1. Konfigurasi diterapkan di *Routerboard Mikrotik RB951Ui-2HND*
2. Menggunakan *Firewall* metode *NAT Rule* untuk *Transparent DNS*
3. Menggunakan *Firewall* metode *Layer 7 Protocol* untuk pemblokiran akses *Proxy* dan VPN
4. ISP yang digunakan untuk konfigurasi adalah Indihome
5. Implementasi hasil konfigurasi dilakukan di SMAN 27 Bandung.

1.5 Metode Penelitian

Metode penelitian merupakan suatu proses yang digunakan untuk memecahkan suatu masalah yang logis, di mana memerlukan data-data untuk mendukung terlaksananya suatu penelitian. Metode penelitian yang digunakan adalah metode analisis deskriptif yang memiliki dua tahap yaitu pengumpulan data dan pengembangan jaringan.

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penulisan skripsi ini sebagai berikut:

1. Studi Literatur

   Mempelajari buku, artikel dan paper yang berkaitan dengan topik tugas akhir.
2. Perancangan Sistem

   Perancangan yang dilakukan antara lain perancangan topologi jaringan, mempersiapkan kebutuhan perangkat, dan pemasangan sistem operasi dan

aplikasi yang digunakan untuk melakukan optimalisasi sehingga dapat berjalan dengan baik pada sistem.

3. Implementasi

   Implementasi yang dilakukan yaitu berupa implementasi sistem dan konfigurasi *Transparent DNS,* Pemblokiran *Proxy* dan *VPN* untuk mengoptimalkan filtering konten negatif yang diberlakukan *ISP*

4. Pengujian

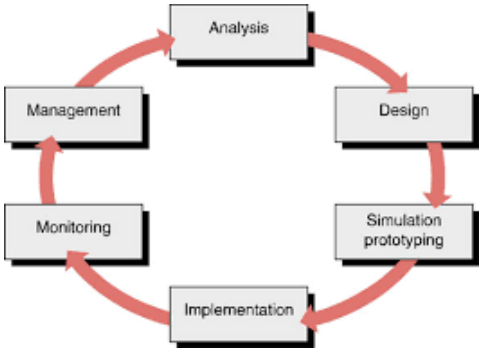
   Pengujian dilakukan dengan melakukan penggunaan DNS *default* yang diberikan oleh ISP, menggunakan DNS Eksternal, serta menggunakan *Proxy* dan *VPN*

5. Analisa dan Kesimpulan

   Setelah melakukan pengujian pada DNS, *Proxy,* dan VPN dapat diambil kesimpulan.

1.5.2 Metode Pengembangan Jaringan

Metode yang digunakan pada penelitian ini adalah model NDLC. *Network Development Life Cycle* (NDLC) merupakan sebuah model yang bergantung pada proses model siklus hidup jaringan dengan konsep NDLC yaitu, Analisis Kebutuhan (*Analysis),* Perancangan *(Design),* Simulasi *(Simulation Prototype),* Implementasi *(Implementation), Monitoring,* dan *Management*. Jika pengimplementasian teknologi jaringan dilaksanakan dengan efektif, maka akan memberikan sistem informasi yang akan memenuhi tujuan. Berikut ini adalah tahapan dari NDLC [1]



Gambar 1.1 Network Development Life Cycle (NDLC)

Sumber: https://pojokteknologi.com

Adapun penerapan dari setiap tahap NDLC adalah sebagai berikut:

1. Analisis Kebutuhan *(Analysis)*

Tahap ini dibutuhkan analisis permasalahan yang muncul, analisis keinginan *user* serta kebutuhan *hardware* yang akan digunakan dan analisis topologi jaringan yang sudah ada saat ini.

2. Perancangan *(Design)*

Design atau perancangan bisa berupa struktur topologi, *design* akses data, *design* tata *layout* perkabelan dan sebagainya yang akan memberikan gambaran jelas tentang *project* yang akan dibangun.

3. Simulasi *(Simulation Prototype)*

Pada tahap simulasi penulis membangun sebuah jaringan sederhana pada *project* yang akan dibangun menggunakan semua alat yang nantinya akan digunakan pada penerapan.

4. Implementasi (*Implementatiton)*

Pada tahap implementasi penulis akan mengkonfigurasi sebuah jaringan LAN dan juga *Wireless*. Implementasi ini diawali dengan pengaturan dasar

5. *Monitoring*

Model pengawasan sistem jaringan NDLC mengkategorikan proses pengujian pada tahap monitoring. Hal ini dikarenakan pengawasan sistem yang sudah dibangun atau dikembangkan. Proses pengujian yaitu untuk menjamin apakah sistem yang dibangun atau dikembangkan dapat berjalan dan sesuai dengan keinginan. Pada tahap ini penulis memantau *user* menggunakan Mikrotik. Langkah dilakukan dengan tujuan memastikan jaringan berjalan dengan baik.

6. *Management*

Selanjutnya adalah *management* atau pengelolaan. Fase ini meliputi aktifitas dan pemeliharaan dari seluruh sistem yang sudah dibangun. Tahap *management* ini akan dilakukan setelah sistem ini berjalan dengan baik pada jaringan yang telah dibangun. Pada tahap *management* penulis akan melakukan beberapa langkah pengelolaan agar sistem yang telah dibangun dapat berjalan sesuai dengan yag diharapkan.

1.6 Sistematika Penulisan

Sistematika penulisan ini disusun untuk memberikan gambaran umum tentang penulisan tugas akhir yang akan dilakukan. Sistematika penulisan tugas akhir ini adalah sebagai berikut.

BAB 1 PENDAHULUAN

Berisi pendahuluan yang menjelaskan tentang latar belakang, tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Membahas tentang teori yang berhubungan dengan topik dalam tugas akhir seperti: jaringan komputer, Internet, topologi dan hardware jaringan, protokol jaringan, alamat IP, sistem operasi dan aplikasi yang digunakan dalam perancangan *Transparent* DNS dan juga pemblokiran *Proxy* dan VPN.

BAB 3 PERANCANGAN SISTEM

Berisi tentang topologi perancangan sistem, kebutuhan perangkat, instalasi sistem dan konfigurasi *Transparent* DNS dan juga pemblokiran *Proxy* dan VPN.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Membahas pengujian proses optimalisasi yang dilakukan pada DNS, *Proxy*, dan VPN.

BAB 5 KESIMPULAN DAN SARAN

Berisi kesimpulan dari seluruh pembahasan skripsi ini dan saran untuk pengembangan lebih lanjut.