

BAB II

KERANGKA TEORITIS

A. TINJAUAN PUSTAKA

Pada penelitian ini, sebelumnya ada beberapa referensi penelitian yang diambil sebagai bahan untuk penelitian yang diajukan, dari penelitian sebelumnya yang membahas permasalahan yang hampir sama. Berikut ini beberapa penelitian yang berhubungan dengan permasalahan yang hampir sama:

1. Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik (Imam Riadi, 2018)

Pada penelitian tersebut permasalahan yang dibahas adalah jaringan belum optimal sehingga Pengguna jaringan komputer harus mengeluarkan investasi yang tidak sedikit untuk mengakses Internet. Internet telah memberikan pengaruh yang sangat besar pada penyebaran informasi, sehingga semakin banyak orang yang mengakses data melalui Internet. Permasalahan tersebut dapat diatasi menggunakan MikroTik sebagai pengatur lalu lintas data Internet serta melakukan pemfilteran beberapa aplikasi yang dapat mengganggu konektivitas jaringan komputer sesuai dengan aturan yang telah ditetapkan. Penelitian ini dilakukan menggunakan beberapa tahapan antara lain : analisis proses untuk menentukan alur lalu lintas yang melewati proses pemfilteran menggunakan firewall, desain untuk mendapatkan cara yang paling efektif dan efisien mengimplementasikan router, implementasi serta pengujian yang dilakukan dengan metode stress test. Berdasarkan penelitian yang telah dilakukan aplikasi router menggunakan MikroTik yang di hasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna.

Perbedaan dengan yang diteliti yaitu : proses yang digunakan untuk menentukan alur lalu lintas dengan menggunakan firewall yang bertujuan untuk melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna.

1. IMPLEMENTASI DAN ANALISA PROXY SERVER SEBAGAI AUTENTIKASI PENGGUNAAN JARINGAN INTERNET DI SMK ROUDLOTUN NASYIIN

(Muhammad Misbahuddin, Mimin F Rohmah, Soffa Zahara, Universitas Islam Majapahit. 2019)

Tujuan dari penelitian ini adalah Mengimplementasikan Proxy Server sebagai Authentikasi jaringan internet di SMK Roudlotun Nasyiin dan Memanajemen Bandwidth berdasarkan User account. Metode penelitian yang digunakan adalah NDLC. Hasil penelitian adalah penggunaan Proxy Server sebagai autentikasi sangat berpengaruh besar atas kinerja jaringan internet pada SMK Roudlotun Nasyiin terutama saat melakukan proses downloading.

Simpulan dari penelitian ini yaitu *Proxy server* dapat berfungsi sebagai *gateway* yang membagi sumber daya dari internet, sehingga yang terhubung dalam jaringan lokal bisa mengakses internet secara bersamaan dalam satu waktu, *Proxy server* dapat diimplementasikan dengan membatasi penggunaan dalam satu jaringan dengan menggunakan proses Authentikasi dengan memberikan hak akses tertentu pada setiap *user* yang masuk, Optimalisasi penggunaan *bandwidth* menggunakan *Proxy Server* dapat berfungsi sebagai *filtering* dan *caching*, baik *filtering content*, pengguna serta waktu akses, *Proxy server* juga dapat diimplementasikan sebagai solusi manajemen *bandwidth* berdasarkan *User account* untuk membagi *bandwidth* secara adil pada setiap *User* dengan menggunakan konfigurasi *delay_pools*.

Bedanya dengan yang dilakukan ada pada metode penelitian yaitu pada penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC).

2. Implementasi firewall dan VPN menggunakan IPCop untuk keamanan data di Universitas Sangga Buana (Septiyahadi, Yosso, Universitas Komputer Indonesia. 2014)

Tujuan dari penelitian ini adalah Mengamankan *server mail*, *webserver*, dan jaringan *wireless* dengan menggunakan *firewall*, dan Melindungi data dengan menggunakan *Virtual Private Network* (VPN) agar dapat diakses diberbagai tempat dan tanpa terbatas oleh waktu. Pada penelitian ini menggunakan metode pengembangan sistem dengan PPDIOO. Kemudian hasil dari penelitian ini yaitu Firewall dan VPN telah membantu client di Universitas Sangga Buana YPKP dalam membantu kebutuhan kinerja pekerjaan mereka, Client Universitas Sangga Buana YPKP masih ragu-ragu dalam menggunakan firewall dan VPN untuk keamanan data, Client Universitas Sangga Buana YPKP setuju untuk menetapkan

firewall untuk mengatasi spam Dos, flooding, dan spoofing, Berdasarkan pengujian keamanan firewall dan VPN masih terdapat celah-celah sehingga tidak ada.

Bedanya dengan yang dilakukan ada pada rumusan masalah penelitiannya, pada penelitian tersebut bertujuan mengimplementasikan firewall dan vpn, tetapi menggunakan sistem operasi yang sama yaitu IPCop.

3. Monitoring dan Filtering Situs Pornografi pada Proxy Server Berbasis Naïve Bayes Classifier dan JADE (Ramaditia Dwiyanaputra, Heri Wijayanto dan Misbahuddin, Universitas Mataram Nusa Tenggara Barat. 2014)

Pada penelitian ini bertujuan untuk memonitoring dan filtering situs atau konten negatif seperti pornografi. Hasil dari penelitian ini Keakuratan rata-rata klasifikasi dengan metode NBC dalam mengklasifikasi situs pornografi dan bukan pornografi mencapai 97,73% dengan keakuratan paling tinggi 98,3% dan paling rendah 96%. Pengaruh penggunaan tahap *preprocessing* (khusus penggunaan *stemming* dan *filtering*) dalam klasifikasi situs pornografi dan bukan pornografi yaitu penggunaan *stemming* dan *filtering* menghasilkan keakuratan yang paling baik. *Agent* dan *proxy server Squid* dapat digabungkan untuk melakukan *monitoring* dan *filtering* situs pornografi. *Agent* dan *proxy server Squid* akan saling berinteraksi dengan perantara log akses *proxy server Squid* dan *blocklist.txt* (daftar situs pornografi). Metode ini mempunyai kekurangan yaitu situs pornografi yang bisa disaring harus sudah pernah diakses sebelumnya.

Bedanya dengan yang dilakukan ada pada metode yang digunakan oleh peneliti tersebut yaitu menggunakan metode Naive Bayes Classifier.

4. TRAFFIC FILTERING DAN WEB CACHING DI SMA NEGERI KERJO (Regen Nopia Putri Cipto Haryono, Program Studi Informatika Fakultas Komunikasi dan Informatika, UNIVERSITAS MUHAMMADIYAH SURAKARTA, 2016)

Tujuan dari penelitian ini untuk memberikan solusi pada masalah yang ada di sekolah tersebut. Waktu yang digunakan untuk penelitian \pm 2 bulan di SMA Negeri Kerjo. Adapun alat yang digunakan dalam penelitian ini dibagi menjadi dua jenis yaitu perangkat keras dan lunak. Peralatan perangkat keras meliputi laptop 2 dan kabel UTP. Sedangkan peralatan perangkat lunak meliputi *IPCop* atau *Proxy* dan web browser.

Hasil dari penelitian yang dilakukan bertujuan untuk memonitoring trafik internet yang ada di SMA Negeri Kerjo. Oleh karena itu, perlu adanya rancangan jaringan di SMA Negeri Kerjo dengan menggunakan *router* dan *OS linux IPCop*

yang digunakan sebagai *server proxy* pada jaringan lokal dan internet bertujuan sebagai solusi keamanan trafik internet seperti *filtering*, *firewalling*, dan *caching* pada website yang meresahkan sertadapat menghemat menggunakan bandwidth yang ada. Penulis juga mengatur situs-situs yang terlarang agar tidak dapat diakses pada jam sekolah. Hal tersebut agar warga sekolah bisa fokus dalam mencari ilmu dari internet yang sudah tersedia dengan aman. Penelitian dilaksanakan di SMA Negeri Kerjo.

5. IMPLEMENTASI MANAJEMEN TRAFFIC DAN BANDWIDTH INTERNET DENGAN IPCOP (Tengku Ahmad Riza, Yon Sigit Eryzebuan, dan Umar Ali Ahmad Fakultas Elektro dan Komunikasi Institut Teknologi Telkom, Bandung, 2010)

Tujuan dari penelitian ini adalah Merancang dan melakukan implementasi pengaturan pengaksesan internet dan maksimal bandwidth/speed, Menerapkan IPCop untuk memonitor kondisi trafik dan penggunaan bandwidth, Memperoleh laporan pemakaian bandwidth yang digunakan oleh pengguna.

Metode yang digunakan yaitu Quality of Service (QoS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis. QoS digunakan untuk mengukur sekumpulan atribut kinerja yang telah dispesifikasikan dan diasosiasikan dengan suatu servis. Hasil dari penelitian yaitu dapat disimpulkan bahwa IPCop telah berhasil untuk mengendalikan dan mengatur *bandwidth* yang didapat sampai ke tingkat *client*. Hal ini dapat dilihat pada gambar diatas, dimana telah berhasil menstabilkan *throughput* yang didapat di client dengan batasan 16 KBps saat mendownload satu *file* dan saat mendownload lebih dari satu *file* dapat mengendalikan *throughput* yang didapat *client* masih pada kisaran 16 KBps.

Dari sisi trafik juga menggambarkan bahwa ada penurunan trafik yang sangat besar ketika pengaturan *bandwidth* telah diterapkan. Tanpa adanya pengaturan *bandwidth* terlihat trafik *intranet* dan *internet* berada pada posisi lebih dari 200 KBps. Setelah menerapkan pengaturan *bandwidth* trafik mengalami penurunan yang sangat tajam menjadi dibawah 20 KBps. Hal ini sangat baik, karena dengan kecilnya trafik yang digunakan tiap *client* maka akan memberi kesempatan pada *client* yang lain untuk dapat menggunakan akses *internet*.

Bedanya yaitu ada pada metode penelitian yang digunakan yaitu Quality of Service (QoS).

6. PENGGUNAAN CONTENT FILTERING DAN DYNAMIC HOST CONFIGURATION PROTOCOL DALAM PROXY SERVER SQUID DI PT BANK INA PERDANA

(Achmad Fadillah, Raziv Herman Diputra, Binus University, 2013)

Tujuan penelitian ialah menganalisis dan merancang sebuah sistem yang secara otomatis akan membatasi hak pengguna dalam mengakses website dan jumlah perangkat yang digunakan untuk mengakses jaringan internet di PT Bank Ina Perdana. Hal ini bertujuan agar bandwidth akan lebih efisien dan network administrator di perusahaan akan lebih mudah melakukan monitoring jaringan. Metode penelitian yang digunakan meliputi studi kepustakaan mengenai topik yang dibahas dalam penelitian dan pengumpulan data menggunakan teknik wawancara dan teknik observasi.

Hasil yang dicapai ialah simulasi rancangan content filtering dengan metode Access Control List yang dapat melakukan filtering terhadap website yang ingin dikunjungi dan Dynamic Host Configuration Protocol (DHCP) dengan metode static allocation yang dapat membatasi jumlah perangkat yang digunakan untuk mengakses jaringan internet dalam proxy server squid. Simpulan dari penelitian ini adalah dengan digunakannya sistem content filtering dan DHCP maka karyawan di perusahaan tersebut hanya dapat mengakses website yang diizinkan oleh perusahaan dan menggunakan perangkat yang telah didaftarkan terlebih dahulu kepada network administrator.

Metode yang digunakan Access Control List (ACL) adalah sebuah metode yang dapat digunakan seorang *network administrator* untuk melakukan *packet filtering*. Dengan menerapkan ACL ini maka *network administrator* dapat menentukan paket-paket yang dapat dilalui melalui *proxy server*.

Bedanya penelitian ada pada masalah yang ada yaitu masalah bandwidth yang kurang efisien.

7. PERANCANGAN JARINGAN VIRTUAL *METAMETAROUTER* (Abdul Rozak dan Ahmad Susan Pardiansyah, STMIK Lombok, 2018)

Tujuan dari penelitian ini adalah Segi ekonomi, penghematan pembelian perangkat jaringan komputer pada SMK Bangun Bangsa, Segi koneksi jaringan komputer, perancangan jaringan MAN cukup menggunakan 1 (Satu) ISP *Internet Service Provider* pada SMK Bangun Bangsa, *MetaMetaRouter* dapat diimplementasikan pada SMK Bangun Bangsa setelah hasil uji terkoneksi 100 %.

Hasil dari pada penelitian adalah Hasil penelitian pada SMK Bangun Bangsa sebelum penerapan jaringan virtual *metarouter* membutuhkan biaya mahal

untuk pembelian router dari segi estimasi ekonomi, setelah peneliti mengimplementasikan jaringan virtual metarouter pada SMK Bangun Bangsa estimasi ekonomi lebih hemat Rp. 2.330.000 dibandingkan sebelum menerapkan virtual *Metarouter* sebesar Rp.5.930.000 dan Hasil kinerja penerapan dan ujicoba virtual *Metarouter* pada SMK Bangun Bangsa, terkoneksi 100 % dengan menggunakan *routerboard* CSR125- 24G-1S-1N dengan implementasi 2 (Dua) *Metarouter* pada satu perangkat, berdasarkan hasil implementasi.

Bedanya dengan yang dilakukan ada pada metode penelitiannya yaitu metode desain PPDIOO.

Dari beberapa tinjauan pustaka yang telah di uraikan dapat di simpulkan yaitu teknologi dan teori yang di gunakan dalam penelitian sebelumnya berbeda dengan teori dan teknologi yang di gunakan oleh penyusun, dalam penelitian ini penyusun menerapkan metode ACL (Access Control List) untuk fitering konten pada jaringan yang menggunakan IPCop, sehingga proses filter di harapkan menjadi lebih efektif.

B. LANDASAN TEORI

1. Jaringan Komputer

Menurut Thomas G. Robertazzi (2011) pada buku yang berjudul Basics of Computer Networking yaitu Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut peladen (*server*). Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Dari definisi diatas dapat diketahui bahwa sebuah LAN dibatasi oleh lokasi secara fisik. Adapun penggunaan LAN itu sendiri mengakibatkan semua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Kerjasama ini semakin berkembang dari hanya pertukaran data hingga penggunaan peralatan secara bersama.

Pada penelitian ini menggunakan topologi jaringan jenis Star, yaitu topologi jaringan berbentuk bintang dimana pada umumnya memakai hub atau switch untuk koneksi antar client. Topologi jaringan komputer ini paling sering digunakan saat ini karena memiliki banyak kelebihan.

2. Access Control List (ACL)

Menurut buku yang berjudul *Security Configuration Guide: Access Control Lists*, Cisco IOS XE Release 3S yang dikeluarkan oleh Americas Headquarters Cisco Systems, Inc. (2015). (Sumber : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-16-12/sec-data-acl-xe-16-12-book.html).

Access Control List (ACL) yaitu melakukan pemfilteran paket untuk mengontrol pergerakan paket melalui jaringan. Penyaringan paket memberikan keamanan dengan membatasi akses lalu lintas ke jaringan, membatasi pengguna dan perangkat akses ke jaringan, dan mencegah lalu lintas meninggalkan jaringan. Daftar akses IP mengurangi kemungkinan spoofing dan serangan penolakan layanan, dan memungkinkan akses pengguna sementara yang dinamis melalui firewall. Daftar akses IP juga dapat digunakan untuk tujuan selain keamanan, seperti untuk mengontrol bandwidth, membatasi konten pembaruan perutean, mendistribusikan kembali rute, memicu panggilan dial-on-demand (DDR), membatasi output debug, dan mengidentifikasi atau mengklasifikasikan lalu lintas untuk fitur kualitas layanan (QoS). *Access List* adalah daftar berurutan yang terdiri dari setidaknya satu pernyataan izin dan mungkin satu atau lebih penolakan pernyataan. Dalam hal daftar akses IP, pernyataan ini dapat berlaku untuk alamat IP, protokol IP lapisan atas, atau bidang lain dalam paket IP. Daftar akses diidentifikasi dan dirujuk oleh nama atau nomor. Daftar akses bertindak sebagai filter paket, penyaringan paket berdasarkan kriteria yang ditentukan dalam setiap daftar akses. Setelah Anda mengkonfigurasi daftar akses, agar daftar akses berlaku, Anda harus menerapkan daftar akses tersebut ke antarmuka (dengan menggunakan perintah *ip access-group*), vty (dengan menggunakan perintah kelas akses), atau referensi daftar akses dengan perintah apa pun yang menerima daftar akses. Beberapa perintah dapat merujuk akses yang sama daftar.

3. Firewall

Menurut John E. Canavan (2001) pada buku yang berjudul *Fundamentals of Network Security* firewall adalah suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internal. Tembok api bekerja dengan cara melacak dan mengendalikan jalannya data serta memutuskan aksi untuk melewatkan (pass), menjatuhkan (drop), menolak (reject), mengenkripsi atau melakukan pencatatan aktivitas (log) data. Firewall menjamin agar data sesuai dengan aturan (rule) yang terdapat di dalam kebijakan keamanannya (security policy) yaitu seperangkat aturan yang telah didefinisikan di dalam keamanan jaringan internal.

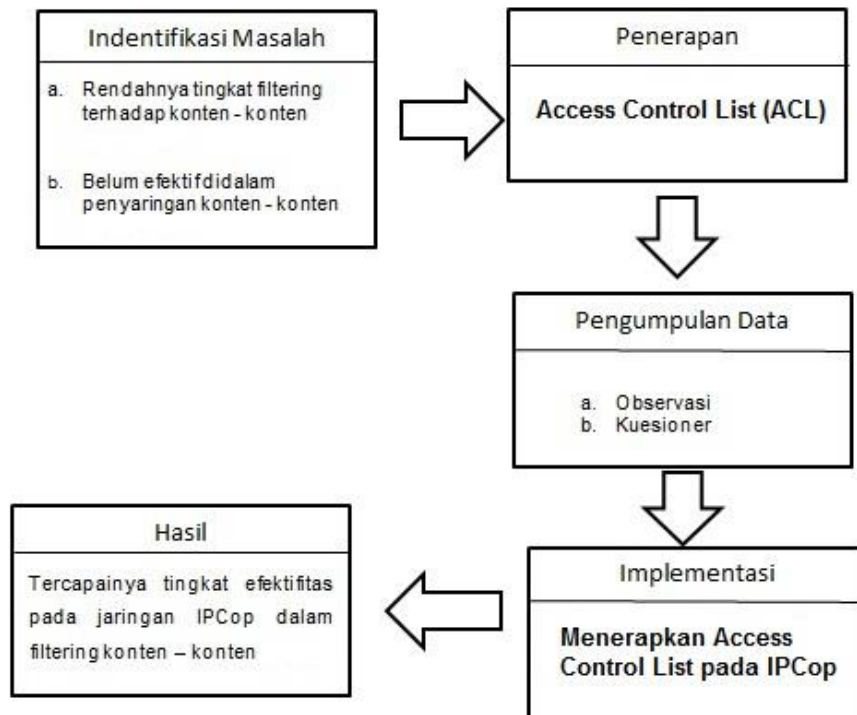
4. IPCop

Menurut Barrie Dempster dan James Eaton-Lee (2006) pada buku yang berjudul *Configuring IPCop Firewalls*, IPCOP adalah suatu distribusi Linux yang menyediakan fitur simple-to-manage firewall appliance berbasis perangkat keras PC. IPCOP juga merupakan suatu stateful firewall dibuat berdasarkan pada Linux netfilter framework. IPCOP sangat simple, dan memiliki fitur user-managed untuk mekanisme update security-nya. Bahkan cenderung mudah dipahami untuk yang para pemula, dan handal untuk yang sudah berpengalaman.

5. PPDIOO

Menurut Marwan Al-shawi dan André Laurent (2017), pada buku yang berjudul *Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide*, PPDIOO merupakan metode perancangan jaringan yang biasa disebut sebagai siklus hidup layanan jaringan Cisco yang dirancang untuk mendukung berkembangnya jaringan. PPDIOO terdiri dari *Prepare, Plan, Design, Implement, Operate, dan Optimize*. Dengan kebutuhan layanan jaringan yang semakin kompleks, maka diperlukan suatu metodologi yang mendukung perancangan arsitektur dan disain jaringan.

C. KERANGKA PEMIKIRAN



Penjelasan tentang kerangka pemikiran pada penelitian ini adalah :

1. Identifikasi masalah untuk menetapkan tujuan penelitian .
2. Melakukan penerapan metode Access Control List untuk meningkatkan efektifitas dalam filtering .
3. Melakukan pengumpulan data berdasarkan kebutuhan setiap pengguna.
4. Melakukan pengembangan melalui tahap perancangan, tahap implementasi, dan tahap pengujian.
5. Melakukan evaluasi terhadap software Filtering yang dikembangkan.

D. Hipotesis

Hipotesis dalam penelitian ini yaitu dengan penerapan metode Access Control List diduga dapat melakukan filtering yang lebih efektif dari sebelumnya dalam penggunaan internet di PT Argha Karya Prima Industry.