BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Peran jaringan komputer pada saat ini tidak dapat diabaikan dan tidak dapat dipungkiri bahwa jaringan komputer memiliki peran yang signifikan. Perkembangan jaringan komputer dimulai dari kebutuhan untuk berbagi data, perangkat lunak, dan akses ke jalur komunikasi (internet). Fungsi praktis dari jaringan komputer ini sangat relevan dalam berbagai sektor seperti agama, sosial budaya, bisnis, pertahanan, kesehatan, pemerintah, dan agama. Semua sektor tersebut memanfaatkan jaringan komputer sebagai sarana pendukung dalam menjalankan aktivitas mereka. Namun demikian dengan meningkatnya jumlah pengguna dan kebutuhan yang semakin kompleks, timbul pula masalah berkaitan dengan keamanannya[1].

Sebagai bagian dari upaya untuk meningkatkan keamanan terhadap serangan eksternal dalam lingkungan jaringan perusahaan, diperlukan upaya untuk meningkatkan tingkat keamanan infrastruktur tersebut. Salah satu cara untuk mencapai hal ini adalah dengan menganalisis data dan sistem informasi yang menjadi aset penting bagi perusahaan, sehingga dapat dilindungi dengan baik. Selain itu, perlindungan jalur komunikasi yang mengandung informasi rahasia juga merupakan hal penting. Implementasi protokol keamanan jaringan harus dipilih sesuai dengan kebutuhan dan persyaratan organisasi. akan membantu menjaga kerahasiaan dan integritas data dalam jaringannya[2].

Keamanan jaringan *wireless* merupakan bagian yang sangat penting dalam menjaga integritas data. Jika tidak dikelola dengan baik, para peretas atau *hacker* dapat dengan mudah memanfaatkan kemampuan mereka untuk mengeksploitasi jaringan tersebut, yang pada akhirnya akan menyebabkan kerugian bagi pengguna. Oleh karena itu, perlindungan terhadap keamanan jaringan *wireless* harus menjadi prioritas utama guna mencegah potensi ancaman dan risiko yang mungkin timbul[3].

Virtual Local Area Network (*VLAN*) adalah tipe jaringan yang terhubung dalam satu jaringan, meskipun berada di lokasi yang berbeda. Konfigurasi *VLAN* dilakukan melalui metode *trunking* pada *switch* untuk menghubungkan dan memisahkan jaringan-jaringan tersebut. Dengan menggunakan teknologi ini, pengguna dapat membuat kelompok-kelompok jaringan *virtual* yang terisolasi secara logika tanpa harus bergantung pada letak fisiknya[4]. *VLAN* memiliki kemampuan untuk membagi *LAN* menjadi beberapa segmen *broadcast*. Dengan keunggulannya, *VLAN* merupakan fitur yang dapat diimplementasikan tanpa perubahan fisik pada jaringan, namun memberikan berbagai manfaat tambahan bagi teknologi jaringan[5].

Spanning Tree Protocol (*STP*) adalah protokol yang terdapat pada *switch* jaringan, yang memfasilitasi komunikasi antara semua perangkat secara efisien dan mencegah terjadinya perulangan tak diinginkan dalam jaringan. Jika terjadi ketidakmampuan akses pada salah satu segmen jaringan dalam *STP*, algoritma *spanning tree* akan melakukan konfigurasi ulang dan membangun kembali *link* dengan mengaktifkan jalur cadangan[3].

Firewall adalah langkah perlindungan yang diterapkan dalam perangkat lunak maupun perangkat keras yang berfungsi melindungi *segmen-segmen* jaringan dengan cara menyaring atau membatasi lalu lintasnya[3]. Metode yang digunakan untuk mengelola lalu lintas IP yang masuk ke jaringan dan menyaring paket *data* saat melewati *router*, digunakan pengaturan pada pintu masuk jaringan dengan metode *filtering* menggunakan *Access Control List* (*ACL*)[6].

ACL bisa sangat berguna ketika perlu mengontrol trafik jaringan *Access Control List* menjadi pilihan yang dominan dalam pengambilan keputusan dalam situasi tersebut. Secara sederhana *ACL* digunakan untuk memperbolehkan atau menghalangi paket-paket dari sebuah komputer menuju tujuan tertentu. *ACL* terdiri dari aturan-aturan dan kondisi-kondisi yang menentukan lalu lintas jaringan dan memutuskan apakah paket akan diteruskan atau tidak oleh *router*[7]. *Router* memiliki peran yang sangat penting dalam menentukan siapa saja yang bisa mengakses jaringan. *Router* akan melaksanakan semua aturan yang telah dibuat dan mengontrol akses terhadap siapa saja yang dapat terhubung ke jaringan tersebut.

Ketika ada pengguna dari luar yang mencoba masuk, *router* secara otomatis akan menolak koneksi tersebut[8].

Beberapa permasalahan dalam jaringan *VLAN* termasuk redundansi jaringan, keterbatasan pembagian hak akses bagi pengguna, dan kurangnya keamanan atau pemantauan pada penggunaan server. Seperti yang sudah diketahui, penggunaan *VLAN* dalam jaringan memiliki beberapa kelemahan. Untuk mengatasi masalah tersebut, penulis berusaha memberikan solusi dengan menerapkan *extended ACL* pada jaringan *VLAN* menggunakan *simulator V-NG* agar dapat mengontrol hak akses pengguna untuk setiap layanan.

Berdasarkan uraian latar belakang di atas, penulis melakukan penelitian dengan judul "ANALISIS PENERAPAN *ACCESS CONTROL LIST* (*ACL*) SEBAGAI PEMBATASAN HAK AKSES PADA JARINGAN *VLAN SPANNING TREE PROTOCOL* (*STP*)".

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini ialah:

1. Bagaimana merancang jaringan *Virtual Local Area Network* (*VLAN*) menggunakan *Spanning Tree Protocol* (*STP*) dengan penerapan *Access Control List* (*ACL*).
2. Bagaimana implementasi *extended ACL* dapat digunakan untuk mengatur hak akses setiap jaringan *VLAN* dengan cara membatasi alamat jaringan yang diizinkan untuk mengakses server.
3. Bagaimana penggunaan protokol *HTTP* untuk membatasi akses ke *web server* dan penggunaan protokol *ICMP* untuk membatasi *ping* ke *server*
4. Bagaimana konsep *Inter-VLAN* memungkinkan komunikasi antara pengguna di *VLAN* yang berbeda melalui penggunaan perangkat jaringan *router*.
5. Bagaimana *QOS* sebelum dan sesudah pengimplementasian sebelum dan sesudah *Extended ACL* dalam membatasi konektivitas antara jaringan *VLAN* dan server.

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1. Sistem keamanan ini dibuat pada jaringan *Virtual Local Area Network* (*VLAN*).
2. Perancangan *VLAN* menggunakan *Spanning Tree Protocol* (*STP*).
3. Penelitian akan menggunakan *V-NG* sebagai *simulator* untuk perancangan jaringan.
4. Server akan menggunakan *OS Ubuntu*.
5. *Web browser* yang digunakan adalah *Apache Browser*.
6. Pembatasan hak akses dalam keamanan jaringan akan menggunakan metode *Extended Access Control List* (*ACL*).
7. Membatasi *protocol HTTP* dan *icmp* untuk mengakses server.
8. Melakukan pengujian pada *IP address* dan akses terhadap *web server* yang telah di batasi.
9. *Quality of Service* (*QoS*) yang di ukur *throughput* dan *packet loss*.

1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1. Menganalisis perancangan jaringan *Virtual Local Area Network* (*VLAN*) berbasis *Spanning Tree Protocol* (*STP*) dengan keamanan *Access Control List* (*ACL*).
2. Menganalisis *extended ACL* untuk mengatur hak akses setiap jaringan *VLAN* dengan cara membatasi alamat jaringan yang diizinkan untuk mengakses server.
3. Menganalisis penggunaan protokol *HTTP* untuk membatasi akses ke *web server* dan penggunaan protokol *ICMP* untuk membatasi *ping* ke *server*.
4. Menganalisis komunikasi antara pengguna di *VLAN* yang berbeda melalui penggunaan perangkat jaringan *router*.
5. Menganalisis *QOS* sebelum dan sesudah pengimplementasian sebelum dan sesudah *Extended ACL* dalam membatasi konektivitas antara jaringan *VLAN* dan server.

1.5 MANFAAT

Penelitian ini diharapkan dapat memberikan manfaat berikut:

a. Bagi pengguna

   Dengan menerapkan *Access Control List* sebagai langkah keamanan jaringan, hal tersebut dapat memberikan kepuasan kepada pengguna jaringan dengan sistem yang lebih aman.

b. Bagi penulis

   Pentingnya bagi penulis untuk mendapatkan pemahaman yang lebih mendalam tentang keamanan jaringan komputer dan keterampilan praktis dalam menerapkan *Extended Access Control List* (*ACL*) sebagai langkah untuk meningkatkan keamanan jaringan komputer.

1.6 SISTEMATIKA LAPORAN

Penelitian ini terstruktur dalam beberapa bagian. Bab 1 mencakup tinjauan awal tentang masalah penelitian, perumusan masalah, tujuan penelitian, serta manfaatnya dalam pengembangan ilmu pengetahuan. Bab 2 akan membahas tinjauan pustaka berdasarkan buku referensi dan jurnal-jurnal yang relevan tentang topik-topik terkait jaringan komputer, seperti *VLAN* (*Virtual Local Area Network*) dan *ACL* (*Access Control List*). Pada Bab 3, akan dijelaskan mengenai alur penelitian, skenario, dan topologi jaringan yang digunakan dalam penelitian. Selanjutnya, Bab 4 akan menganalisis data hasil penelitian yang telah diperoleh sebelumnya dan melakukan diskusi mendalam tentang penelitian tersebut. Akhirnya, pada Bab 5 kesimpulan dan saran sebagai penunjang untuk penelitian selanjutnya.