BAB 1. PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer adalah hubungan antara dua atau lebih komputer dengan perangkat lainnya seperti printer, modem, dan hard drive eksternal. Untuk membangun sebuah jaringan komputer diperlukan beberapa komponen dan alat yang digunakan untuk menghubungkan antar komputer seperti hub, access point, switch, router, dan perangkat-perangkat lainnya. Secara umum skala jaringan komputer terbagi menjadi empat klasifikasi yaitu *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Network* (WAN), dan *Internetwork* (Internet).

Dalam sebuah jaringan komputer dikenal beberapa potensi gangguan atau serangan dari *attackers* yang ingin mencuri dan merusak informasi dari sebuah sistem jaringan komputer. Menurut W. Stallings dalam buku Sofana (2012:307) ada beberapa kemungkinan serangan terhadap keamanan sistem informasi, yaitu *Interruption, Interception, Modification,* dan *Fabrication*. Berbagai potensi serangan yang mengancam keamanan jaringan dapat digolongkan seperti *virus*, *spyware*, *worm* dan serangan peretas (*hacker attacks*). Permasalahan tersebut terjadi melalui internet, *service* dari protokol atau port, dan lemahnya dasar keamanan dalam suatu jaringan komputer. Gangguan keamanan seperti *virus*, *spyware*, dan *worm* dapat masuk melalui port yang terbuka di jaringan komputer melalui situs-situs internet yang dibuka oleh komputer klien dan juga port-port terbuka di komputer yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses data dan informasi di komputer tersebut.

Keamanan jaringan (*Network security*) berkaitan dengan segala aktivitas yang dilakukan untuk mengamankan jaringan, khususnya untuk melindungi penggunaan (*usability*), tahan uji (*reliability*), ketangguhan (*integrity*), dan keamanan (*safety*) dari jaringan dan data. Target keamanan jaringan adalah bagaimana mencegah dan menghentikan berbagai potensi serangan (*threats*), agar tidak memasuki dan menyebar pada jaringan tertentu. Keamanan jaringan mencakup perangkat keras dan perangkat lunak. Pada studi kasus di perusahaan

PT. Eratex Djaja Tbk Probolinggo pengadaan keamanan jaringan dari sisi perangkat keras menggunakan router mikrotik. Router mikrotik digunakan sebagai pengatur protokol jaringan seperti telnet, smtp, ftp dan lain-lain. Sementara dari sisi perangkat lunak perusahaan terkait menggunakan dua program untuk mengamankan jaringan komputer. PDC (Primary Domain Controller) pada Windows 2000 server atau Windows 2008 server mampu memberikan dasar keamanan untuk akses ke jaringan komputer perusahaan. Squid digunakan sebagai *filtering* situs internet yang tidak diijinkan untuk diakses oleh klien. Dengan menggunakan router Cisco tiga tugas keamanan jaringan tersebut dapat dilaksanakan menggunakan metode Cisco ACL. Jadi hanya dengan router Cisco saja dapat mengganti ketiga metode sistem keamanan yang digunakan oleh perusahaan PT Eratex Djaja Tbk Probolinggo sehingga akan lebih mudah untuk mengadakan keamanan jaringan pada perusahaan tersebut.

Access Control List (ACL) adalah metode yang digunakan Cisco untuk mengatur keluar masuknya lalu lintas (*traffic*) kedalam maupun keluar router. Metode ini disebut dengan *packet filtering*. Daftar akses (*Access List*) ini berfungsi untuk membandingkan atau mencocokkan setiap paket yang diterima atau ditolak dengan aturan (*rules*) atau daftar akses yang diterapkan pada router.

1.2 Rumusan Masalah

Untuk memperjelas permasalahan yang akan diteliti, penulis merumuskan permasalahan kegiatan sebagai berikut :

a. Bagaimana cara menerapkan standard dan extended ACL (Access Control List) pada jaringan komputer?
b. Bagaimana mencegah *host* dalam suatu *network* mengakses situs-situs yang membebani bandwith?
c. Bagaimana cara menutup akses port yang terbuka pada jaringan komputer dan komputer klien?

1.3 Batasan Masalah

Agar kegiatan lebih terarah, terfokus dan tidak meluas, penulis membatasi kegiatan keamanan server pada jaringan lokal maupun internet terhadap satu atau dua pihak yang dianggap akan mencuri informasi yang ada di server.

a. Pengadaaan keamanan server dilakukan melalui perangkat-perangkat jaringan dari perusahaan Cisco yang dimiliki oleh Politeknik Negeri Jember seperti Cisco router dan Switch catalyst.
b. Kegiatan ini menggunakan tiga standar keamanan yang disediakan oleh perangkat jaringan Cisco seperti standard dan extended ACL (*Access Control List*) serta metode Firewall ACL – TCP (*Transmission Control Protocol*) *established and reflexive.*

1.4 Tujuan

Tujuan dari kegiatan ini adalah :

a. Memutus akses dari pihak yang tidak diinginkan untuk mengakses komputer server dan klien.
b. Menutup akses port yang terbuka dan tidak diperlukan untuk mencegah akses dari pihak eksternal.
c. Meningkatkan keamanan server pada jaringan lokal maupun internet.

1.5 Manfaat

Kegiatan ini diharapkan dapat memberi referensi dan jawaban dari permasalahan-permasalahan yang telah dirumuskan dan memberikan manfaat sebagai berikut :

a. Bagi mahasiswa

Kegiatan ini diharapkan menjadi sebuah referensi pembelajaran bagi mahasiswa lain dalam mendukung mata kuliah yang berhubungan dengan Cisco seperti CCNA (Cisco *Certified Network Academy*)

b. Bagi administrator jaringan

Melalui kegiatan ini, diharapkan administrator jaringan di PT Eratex Djaja Tbk mendapatkan referensi baru mengenai sistem keamanan menggunakan Cisco router. Sehingga akan lebih meningkatkan standar keamanan server di lembaga atau instansi tersebut.

c. Bagi peneliti lain

Dengan adanya kegiatan ini, penulis berharap akan bermunculan peneliti-peneliti lain yang akan membahas mengenai keamanan sever menggunakan perangkat jaringan Cisco yang terbaru.