ABSTRAKSI

Saat ini teknologi *Internet* yang berbasis protokol TCP/IP telah dipakai secara luas pada kehidupan rutin sehari-hari. Terhubungnya LAN atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Menurut G. J. Simons keamanan informasi adalah bagaimana mencegah penipuan (*cheating*) atau paling tidak, mendeteksi adanya pelanggaran kebijakan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.Sehingga dibutuhkan suatu sistem keamanan yang dapat mendeteksi,menganalisa dan bereaksi terhadap serangan tanpa mengurangi performansi servis yang disediakan.

Firewall adalah suatu cara untuk membatasi informasi yang dibolehkan masuk dan keluar dari jaringan lokal. Umumnya *host* terhubung ke Internet dan LAN lokal, dan akses LAN ke Internet hanya melalui *firewall*. Dengan demikian *firewall* dapat mengendalikan apa yang diterima dan dikirim dari Internet dan LAN.

Pada tugas akhir ini keamanan jaringan dirancang dan diimplementasikan dengan menggunakan metode *AIRIDS. AIRIDS (Automated Intelligently Reactive Intrusion Detection System)* merupakan suatu metode keamanan jaringan yang bertujuan untuk membentuk suatu arsitektur sistem keamanan yang terintegrasi antara *Intrusion Detection System (IDS)* , *Firewall* System, *Database System* dan *Monitoring System*.. Sistem keamanan ini bertujuan melindungi jaringan dengan kemampuan merespon secara cerdas sesuai dengan kebijakan keamanan dengan menggunakan prinsip prinsip *Artificial Intelligent (AI)* dalam pengambilan keputusan .Keputusan yang diambil digunakan oleh Adaptive Firewall sebagai kebijakan untuk menentukan apakah suatu paket akan di blok atau diteruskan ke jaringan .

Implementasi keamanan jaringan menggunakan *AIRIDS* dan *Adaptive Firewall* menunjukkan peningkatan performansi dalam pengamanan jaringan.