ABSTRAK

Moh. Furqon

Teknik Elektro

Analisis Kinerja Jaringan IPSec Berbasis Protokol IKEv2 Menggunakan Algoritma Key Exchange MODP dan ECP

Dewasa ini, internet telah digunakan secara meluas dan *massive*, penggunaannya mulai dari berselancar sederhana hingga transaksi yang penting membuatnya sangat rentan terhadap serangan keamanan dan dapat menimbulkan kerugian. Salah satu sistem keamanan yang baik digunakan pada jaringan internet adalah IP *Security* (IPSec). IPSec merupakan rangkaian protokol yang menyediakan kemanan untuk komunikasi internet pada *network layer*. IPSec sangat bisa diandalkan baik itu pada skema *site-to-site*, *host-to-host* maupun *end-to-end*. Protokol IPSec akan sangat efisien apabila menggunakan sebuah subprotokol bernama *Internet Key Exchange Version* 2 (IKEv2). Satu hal yang kurang diperhatikan pada penggunaan IKEv2 adalah penggunaan algoritma *key exchange*, padahal pengguaan algoritma *key exchange* yang tepat akan membuat pengguaan IPSec akan lebih efisien. Pada penelitian ini, IPSec diimplementasikan pada dua *host* dengan skema jaringan *host-to-host* dan dihubungkan melalui jaringan internet. Mekanisme otentikasi yang dipakai adalah dengan *public key* dan dinegosiasi dengan protokol IKEv2. Pengujian dilakukan dengan menggunakan algoritma *key exchange* yang berbeda yaitu modp1024, modp3072 dan ecp384 dengan analisa performa pada kecepatan *key exchange generation*, waktu delay IKE SA *established* dan performa jaringan dari ketiga algoritma tersebut. Hasil yang didiperoleh dari pengujian tersebut adalah IPSec dengan menggunakan algoritma *key exchange* ecp384 mendapatkan performa yang paling baik.

Kata kunci: IPSec, IKEv2, kriptografi, algoritma *key exchange*.

ABSTRACT

Moh. Furqon

Electrical Engineering

Performance Analysis of IPSec Based on IKEv2 Protokol Using MODP and ECP Key Exchange Algorithm

Recently, the Internet has been used extensively and massively, its use from simple surfing to important transactions makes it extremely vulnerable to security attacks and can cause losses. One of the best security systems used on internet networks is IP Security (IPSec). IPSec is a protocol suite that provides security for Internet communication on the network layer. IPSec is reliable in both site-to-host, host-to-host and end-to-end schemas. The IPSec protocol will be very efficient when using a subprotocol called IKEv2. One thing that is less attention to the use of IKEv2 is the use of key exchange algorithm, whereas the use of appropriate key exchange algorithm will make more efficient IPSec use. In this study, IPSec is implemented on two hosts with host-to-host network schemes and connected via the internet network. The authentication mechanism used is public key and negotiated with IKEv2 protocol. Experiments were performed using different key exchange algorithms, namely modp1024, modp3072 and ecp384, followed by performance analysis at key exchange generation speed, IKE SA time established and network performance. The results obtained from the test show one key exchange algorithm with the best performance that can be implemented on IPSec, it is ecp384.

Keywords: IPSec, IKEv2, cryptography, key exchange algorithm.