

**IMPLEMENTASI KEAMANAN JARINGAN WIRELESS DENGAN
MENGUNAKAN IPSEC DAN WEP**

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk mendapatkan gelar Ahli Madya
pada Jurusan Teknologi Informasi Program Studi Teknik Komputer

Oleh :

DIAN SUNERTA
05092018



**PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK UNIVERSITAS ANDALAS
PADANG**

2010

ABSTRAKSI

Kemajuan teknologi informasi pada saat ini terus berkembang seiring dengan kebutuhan manusia yang menginginkan keamanan, kemudahan, kecepatan dan keakuratan dalam memperoleh informasi. Salah satunya berdampak pada kemajuan teknologi informasi dibidang transmisi data.

Media Transmisi data yang menggunakan kabel UTP dan konektor RJ-45 atau yang sering disebut dengan wired LAN sudah mulai tergantikan dengan media transmisi berupa udara dengan menggunakan frekuensi radio yakni Wireless.

Pada tugas akhir ini dibahas analisa keamanan wireless yang telah berjalan di labor teknologi informasi dan juga perancangan serta implementasi keamanan wireless. Dan diharapkan dengan adanya keamanan wireless dapat meningkatkan beberapa *performance* jaringan yang ada, antara lain : Access data lebih aman, tidak perlu dirisaukan tentang kehilangan data. Penggunaanya yang sangat fleksibel dalam pembentukan koneksi baru.

Kata Kunci, Acces point, IP Security, WEP.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam dunia jaringan yang sudah berkembang dengan sangat pesat, kecepatan transfer data dan pelayanan aplikasi jaringan yang *bonafit* sangat berpengaruh untuk meningkatkan kualitas jaringan yang akan dibuat. Disamping itu seorang administrator harus mempunyai kehandalan dan kecakapan dalam mengantisipasi hal – hal yang terjadi pada jaringan misalnya ketika seorang *user /client* melakukan browsing data dan menggunakan aplikasi / layanan dalam jaringan. Administrator harus mampu membatasi hak – hak akses *client* dan aplikasi apa saja yang layak dan pantas untuk digunakan oleh seorang *client*.

Dalam hal ini dibutuhkan sebuah aplikasi / *software* yang mampu memberikan keamanan dalam, membatasi dan mengontrol lalu lintas data yang terjadi pada jaringan tersebut, sehingga apabila terjadi hal – hal yang tidak diinginkan misalnya terjadi kehilangan data yang penting atau tujuan yang kurang baik pada jalur komunikasi suatu komputer, maka administrator mampu mengambil tindakan dengan cepat dan mengantisipasi hal tersebut. Salah satu *software* yang mampu melakukan hal tersebut adalah IPsec dan *WEP*. Aplikasi ini memiliki keunggulan yaitu selain mampu memberikan keamanan data juga mengamankan management user. Untuk mendapatkan *software* ini pun cukup mudah karena sebagian besar telah terdapat dalam sistem operasi *Windows server2003*, dengan menggunakan

Aplikasi IPsec dan WEP seorang administrator dapat melayani permintaan client dengan baik dan proses lalu lintas data dalam jaringan dapat teratur dan terarah sesuai dengan keinginan administrator.

1.2 Rumusan Masalah

Supaya pembuatan tugas akhir lebih terarah , maka dalam hal ini penulis membatasi pada pembahasan :

1. Bagaimanan manfaat aplikasi IPsec dan WEP pada jaringan?
2. Bagaimana cara mengamankan jaringan wireless dengan menggunakan aplikasi IPsec dan WEP?

1.3 Tujuan

Adapun tujuan dari penulisan tugas akhir ini adalah :

1. Bagi jaringan wireless keamanan jaringanya dapat digunakan aplikasi IPsec dan WEP ini sangat berguna, karena dengan aplikasi ini memiliki keamanan jaringan yang bagus dan mudah dalam instalasinya.
2. Aplikasi IPsec dan WEP ini di install menggunakan server 2003 dan nanti akan bekerja buat monitoring client yang melakukan browsing.

1.4 Batasan Masalah

Dalam penulisan tugas akhir ini dapat di batasi masalah yakni :

1. Implementasi rancangan IPsec dan WEP.
2. Pada WEP yang dibahas hanya Settingan pada akses point.
3. Pembahasan tentang cara kerja dari IPsec.

BAB V KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Setelah melakukan analisa terhadap keamanan wireless yang berjalan di labor teknologi informasi politeknik padang, dan merancang keamanan wirelessnya, maka dapat diambil kesimpulan sebagai berikut:

1. Keamanan *Wireless* di labor teknologi informasi dapat diamankan dengan mengaplikasikan sitem operasi *windows 2003 server* serta menunjang proses belajar mahasiswa.
2. Dengan adanya keamanan wireless menggunakan IP security di teknologi informasi dapat melihat browser apa yang ingin di lihat oleh mahasiswa.
3. Mempermudah dalam proses *browsing*

5.2 SARAN

Untuk lebih meningkatkan kinerja keamanan wireless yang akan dijalankan, terdapat beberapa saran yang perlu diperhatikan:

1. Untuk memperoleh hasil yang lebih memuaskan diharapkan agar secepatnya pembangunan hardware untuk keamanan jaringan wireless maksudnya seperti yang telah dikatakan oleh teknisi labor teknologi informasi.
2. Sebaiknya keamanan wireless sangat di perhatikan keberadaanya karena wireless dapat digunakan oleh siapapun karena jaringanya tidak menggunakan kabel.

DAFTAR PUSTAKA

- Gunadi. (2006). *Teknologi Wireless dan Aplikasinya*. Alex Media Komputindo, Jakarta.
- Info Komputer. (Januari 2006). *Membangun Jaringan Wi-fi*. Informatika, Bandung.
- Madcoms (2003). *Dasar Teknis Instalasi Jaringan Komputer*. Andi Offset, Yogyakarta.
- Octomo, Budi S. D. (2004) *Konsep dan Perancangan Jaringan Komputer*. Andi Offset, Yogyakarta.
- Sugeng, Winarno. (2005) *Instalasi Wireless*. Informatika, Bandung.
- Tanerboum, Andrew S. (1996) *Jaringan Komputer Jilid 1 : Edisi Bahasa Indonesia*. Prentice-Hall Inc, New Jersey.
- Tutang (2005). *Membangun jaringan LAN berbasis Windows 2000 Server bagi Pemula*. Andi Offset, Yogyakarta.
- Bin Iadjamudin, Al-Bahra. *Metode perancangan program (pemograman terstruktur)*. Tangerang.2004
- <http://seminyak.com/net/modules.php?name=Wifi>, 30 Mei 2008.
- http://www.bl.ac.id/dosen/tri_daryanto/wilan.PDF, 30 Mei 2008.
- http://www.infoteknologi.com/isi_lan.htm, 30 Mei 2008.
- www.bluetooth.com, 30 Mei 2008.
- www.bogor.net/idkf/broadbandwireless/WiLan.ppt, 30 Mei 2008.
- www.ilmukomputer.com, 30 Mei 2008.
- www.infoteknologi.com, 8 Juni 2008.
- www.openbsd.org/faq/faq13.html 2009
- Jones, D., 2003, *Microsoft Windows Server 2003*, QUE, Indianapolis.