RANCANG BANGUN SERVER AAA BERBASIS TACACS+ DAN RADIUS PADA JARINGAN LAN MENGGUNAKAN IPSEC

Ardian Fachreza[1], Rendy Munadi [2], Tody Ariefianto Wibowo[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Sebagai seorang ahli keamanan dalam suatu ISP tentunya memiliki tugas untuk monitoring keamanan jaringan dan perangkat seperti switch dan router yang berjumlah tidak sedikit serta mengamankan trafik informasi yang ada di ISP. Untuk melakukan monitoring keamanan jaringan yang begitu besar tentunya tidak dapat dilakukan oleh seorang administrator saja sehingga diperlukan pengaturan priviliges (hak akses) tertentu kepada co-admin di setiap router dan switch. Pemberian priviliges tersebut kurang efisien apabila di terapkan dalam jaringan yang sangat besar. Sehingga dibutuhkan pengaturan priviliges secara terpusat untuk memudahkan kinerja administrator dalam monitoring kondisi jaringan dan keamanan informasinya. TACACS+ dan RADIUS menjadi solusi untuk manangani masalah akses keamanan jaringan yang sedang terjadi saat ini.Dalam tugas akhir kali ini akan menganalisa kelebihan dan kekurangan kedua protokol tersebut baik dari segi kompatibilitas layanan dan keamanan layanan data yang bersifat penting dengan cara melakukan simulasi di GNS 3 dan menambahakn layanan IPSec pada setiap router untuk melindungi trafik informasi yang ada di setiap router Pada Tugas akhir kali ini dihasilkan bahwa delay yang dibutuhkan untuk melakukan proses otentikasi dengan AAA ± 1 detik lebih lama jika dibandingkan otentikasi tanpa menggunakan AAA dan penambahan IPSec tidak terlalu membebani jaringan karena hanya memerlukan ± 1% dari kapasitas yang disediakan.

Kata Kunci : Teknologi berkembang, kompleksitas layanan, TACACS+, RADIUS, IPSec

Abstract

As a security expert in an ISP must have a task for network security and monitoring devices such as switches and routers are not small amounts of traffic and secure information in the ISP. For monitoring network security is so great of course can not be done by an administrator priviliges just so necessary settings (permissions) specific to the co-admin at every router and switch. Giving priviliges are less efficient when implemented, in very large networks. So it takes a centralized setting priviliges to facilitate the performance of administrators in monitoring the condition of the network and information security. TACACS + and RADIUS manangani be a solution to the problem of network security access is happening at this time ini.Dalam thesis will analyze the advantages and disadvantages of these two protocols in terms of both compatibility and security services data services that are vital to the way of doing simulations on GNS 3 and menambahakn service at each router IPSec to protect traffic information in each router At the end of this time the task is generated that the delay is needed to make the process of authentication with AAA ± 1 second longer than without using AAA authentication and IPSec additions not overload the network because it requires only ± 1% of the capacity provided.

Keywords : Technology evolves, The complexity of the service, TACACS, RADIUS, IPSec

BAB I

PENDAHULUAN

1.1. Latar belakang masalah

Pada saat ini dunia telekomunikasi baik di Indonesia maupun di duniaterus-menerus berevolusi, kebutuhan akan keamanan suatu informasi semakin besar, sebesar perkembangan teknologi pendukung lainnya. AAA merupakan suatu metode yang cocok untuk penerapan sistem kemanan jaringan dalam skala besar. Dengan metode ini memungkinkan pengaturan jaringan pada setiap node/ router dalam skala besar akan lebih aman. Pengaturan ACL (Access List) meruapak kunci dari metode AAA karena di setiap user mempunyai tingkat ACL yang berbeda beda.

TACACS+ & RADIUS didefinisikan sebagai protokol yang mampu dalam menyediakan layanan AAA secara tersentralisasi. Penerapan AAA menggunakan TACACS+ & RADIUS merupakan langkah yang tepat untuk di implementasikan dalam jaringan yang mempunyai lingkup luas misalnya seperti pada jaringan *Metro Ethernet*.

Pengaturan AAA secara tersentralisasi sangat memudahkan *administrator* jaringan dalam membatasi dan memantau akses suatu *client* dalam setiap komunikasi yang di lakukan.Dengan hal ini diharapkan seorang administrator jaringan tidak perlu bersusah payah untuk mengatur AAA secara detail pada setiap router. Namun,cukup mengatur AAA secara global dan mengarahkan ke IP TACACS+ atau RADIUS *server*, dimana di dalam TACACS+ dan RADIUS server terdapat database yang berfungsi untuk mengatur AAA pada setiap *user*/ group yang akan melakukan akses ke suatu router.

Penambahan IPSec sangat memberikan keuntungan tersendiri dalam implementasi RADIUS dan TACACS+ kerena semua data di enkapsulasi menggunakan ESP yang ada pada Ipsec sehingga data akan menjadi lebih aman. Dengan hal ini diharapkan sistem manajemen AAA ini dapat lebih aman dan bermanfaat.

1.2. Perumusan masalah

Permasalahan yang akan dibahas dalam pengerjaan Tugas Akhir ini adalah :

1.2.1. Bagaimana membuat Simulasi TACACS+ & RADIUS dengan GNS 3 ?

1.2.2. Mengapa menggunakan pengamanan TACACS+, RADIUS dan menggunakan keamanan tambahan IPSec ?

1.2.3. Seberapa amankah penggunaan sistem AAA dan tambahan Protokol Security IPSec dalam pertukaran informasi .

1.3. Tujuan

Tujuan dari penyusunan Tugas Akhir ini adalah :

1.3.1. Menganalisa paket overhead dari suatu jaringan ketika menggunakan protokol RADIUS.

1.3.2. Menganalisa paket overhead dari suatu jaringan ketika menggunakan protokol TACACS+

1.3.3. Menganalisa delay otentikasi ketika menggunakan layanan AAA dan tanpa AAA

1.3.4. Menganailsa paket overhead dari suatu jaringan ketika menggunakan protokol keamanan tambahan berupa IPSec.

1.4. Batasan Masalah

Adapun batasan dari sistem antara lain :

1.4.1. Menggunakan server TACACS+, RADIUS dan pembuatan manajemen AAA.

1.4.2. Tentang penggunaan pengamanan TACACS+ , RADIUS dan IPSec pada linux maupun Router serta tidak membahas secara detail tentang metode Enkripsi keamanan.

1.4.3. Hanya Menggunakan aplikasi GNS 3 untuk simulasi AAA TACACS+ & RADIUS.

1.4.4. IPSec hanya diterapkan point-to-point tidak point-to-multipont

1.5. Metodologi penyelesaian masalah

Metodologi penyelesaian masalah antara lain :

1) Studi Lapangan

   Merupakan tahap awal, dimana pada tahap ini akan digali lebih dalam mengenai segala sesuatu yang berkaitan dengan TACACS+, RADIUS dan IPSec. Selain itu akan dicari literatur yang berhubungan dengan Sistem yang akan dibuat. Sumber literatur diperoleh dari buku, paper ilmiah, maupun website. Study lapangan dilakukan saat awal pengerjaan dan memahami kondisi apa saja yang terjadi di lapangan dalam membuat server.

2) Pemodelan Sistem

   Pada tahapan ini akan dirancang pemodelan dari sistem ini. Antara lain objek-objek yang akan diperlukan untuk visualisasi dan fungsionalitas-fungsionalitas dari aplikasi yang akan dibangun.

3) Implementasi Sistem

   Dalam tahap ini sistem akan mulai dibangun dengan mengimplementasikan objek-objek dan fungsionalitasnya, serta penggunaan system untuk beberapa tahun kedepan.

4) Dokumentasi Sistem

   Pada tahap yang terakhir ini, segala kegiatan yang berhubungan dengan perancangan aplikasi ini akan dicatat dan disusun ke dalam bentuk sebuah dokumentas

1.6. Sistematika Penulisan

Penulisan Tugas Akhir ini akan dibagi beberapa bagian sebagai berikut:

Bab I Pendahuluan

Berisi latar belakang, perumusan masalah, batasan masalah, tujuan pembahasan, metodologi penyelesaian masalah dan sistematika penulisan.

Bab II Dasar Teori

Berisi tentang dasar-dasar teori yang diperlukan serta literatur-literatur yang mendukung dalam *Rancang Bangun Server AAA berbasis TACACS+ dan RADIUS pada jaringan LAN menggunakan IPSec.*

Bab III Desain dan Konfigurasi Sistem

Berisi tentang pembahasan *Rancang Bangun Server AAA berbasis TACACS+ dan RADIUS pada jaringan LAN menggunakan IPSec* dimana akan diimplementasikan di jaringan privat AccessNet Lab

Bab IV Pengujian dan Analisis Sistem

Menjelaskan tentang tingkat akurasi dan analisa dari beberapa skenario yang dilaksanakan.

Bab V Kesimpulan Dan Saran

Berisi tentang kesimpulan akhir dan saran pengembangan tugas akhir.

BAB V
PENUTUP

5.1. Kesimpulan

Dari hasil implementasi dan perancangan serta pengambilan data dan analisis yang telah dilakukan pada implementasi jaringan *Rancang Bangun Server AAA berbasis TACACS+ dan RADIUS pada jaringan LAN menggunakan IPSec*. dapat diambil kesimpulan sebagai berikut :

1. Paket overhead RADIUS menggunakan TELNET lebih kecil dibanding menggunakan SSH dimana TELNET sebesar 0.016% sedangkan ketika menggunakan SSH sebesar 0.025%.
2. Paket overhead TACACS+ menggunakan TELNET lebih kecil dibanding menggunakan SSH dimana TELNET sebesar 0.017% sedangkan ketika menggunakan SSH sebesar 0.026%.
3. Berdasarkan hasil uji diatas proses otentikasi RADIUS ± 1 detik apabila dibandingkan dengan TACACS+ dikarenakan RADIUS menggunakan protokol transport UDP dimana tidak memerlukan proses pembentukan koneksi.
4. Paket Overhead IPSec ketika menggunakan TELNET sebesar 0.041% sedangkan ketika menggunakan SSH 0.06%.

5.2. Saran

1. Menambahkan perangkat PIX firewall untuk melindungi server dari serangan hacker/cracker yang mengancam avaibility server.
2. Implementasi IPSec dan AAA pada komunikasi nirkabel menggunakan WLAN.

DAFTAR PUSTAKA

1. Andrew S. Tanenbaum, ” Jaringan Komputer ”, Jakarta , 2000.
2. Cisco system,Inc,”Network Security 1”. 2006.
3. Klotz S., Russell R., and Shastry Y., "*Evaluating the effect of iSCSI protocol parameters on performance*, " *In Proceedings of the Parallel and Distributed Computing and Networks*. 2005
4. *Jo S., “Security Engine Management of Router based on Security Policy,” proceedings of world academy of science, engineering and technology, volume 10, ISSN 1307-688, 2005.*
5. *Generic AAA Architecture*.[online]: http://tools.ietf.org/html/rfc2903
6. The TACACS+ Protocol Version 1.78.[online]: *http://tools.ietf.org/html/draft-grant-tacacs-02.*
7. RADIUS.[online]: http://tools.ietf.org/html/rfc2865.
8. *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*.[online]: *https://tools.ietf.org/html/rfc6071.*
9. Gark, Deepak.*Distributed Access Control*.[online]: www.cs.cmu.edu/