Analisis dan Pengujian Permasalahan Pada Sistem *Remote Access* IPSec

Arini, MT, Giri Patmono
Program Studi Teknik Informatika
Fakultas Sains Dan Teknologi
UIN Syarif Hidayatullah Jakarta
arinizoel@yahoo.com, giripatmono@gmail.com

***Abstract*— VPN (*Virtual Private Networking*) sebagai teknologi *remote access* yang memungkinkan pengguna jarak jauh dapat mengakses sumber daya yang ada di jaringan komputer utama. Untuk mengimplementasikan remote access VPN berbasis protokol IPsec memiliki berbagai masalah dan kebutuhan yang menghambat penerapannya secara luas. Kajian ini akan mencari solusi masalah dan kebutuhan dalam penerapan *remote access* VPN berbasis protokol Ipsec dengan penggunaan perangkat lunak IKEv2 strongSwan. Kesimpulan yang kami dapatkan dari hasil penelitian skripsi ini adalah bahwa sistem *remote access* IPsec berbasis perangkat lunak IKEv2 strongSwan mampu mengatasi semua masalah dan kebutuhan dalam penerapan *remote access* VPN berbasis IPsec. Pengembangan selanjutnya yang dapat dilakukan adalah melakukan simulasi penerapan IPsec *Extensible Authentication Protocol* (EAP) dan simulasi pengujian interoperabilitas antara Linux IKEv2 strongSwan sebagai *server* dan klien berbasis Windows.**

***Index Terms*— *Extensible Authentication Protocol* (EAP), IPSec, *Remote Access*, VPN (*Virtual Private Networking*).**

I. PENGANTAR

VPN (*Virtual Private Networking*) merupakan teknologi untuk membangun jaringan virtual dengan melibatkan teknik tunneling menggunakan dua skenario umum yaitu *Site-to-Site* dan *Remote Access*. *Site-to-Site* menghubungkan antar jaringan komputer LAN sedangkan *Remote Access* digunakan antara pengguna *remote* (jarak jauh) seperti *telecoworker* atau *mobile worker*. VPN mampu menyediakan solusi dengan biaya murah dibandingkan dengan *dedicated line* ataupun *leased-line*. *Internet Protocol Security* (IPsec) yang bekerja pada level lapisan network adalah salah satu standar teknologi yang dapat digunakan untuk membangun VPN. IPsec terdiri dari beberapa protokol diantaranya yaitu *Authentication header* (AH), *Encapsulating Security Payload* (ESP), dan *Internet Key Exchange* (IKE). AH dan ESP berfungsi untuk memberikan layanan kriptografi, sedangkan IKE bertugas menangani manajemen parameter *Security Association* (SA) [6]. Saat ini telah tersedia protokol IKEv2 yang merupakan pengembangan dari protokol IKE (IKEv1). Salah satu teknologi yang mengimplememtasikan IKEv2 adalah StrongSwan dalam lingkungan sistem operasi Linux dengan lisensi GPL (GNU Public License) sehingga ia bersifat *free* dan *open source*.

Penerapan VPN yang berberbasis IPsec dengan skenario *Remote Access* (*Remote Access IPsec*) IKEv2 ternyata masih memiliki beberapa permasalahan disamping itu juga diperlukan adanya spesifikasi kebutuhan tertentu untuk mendukung penerapannya secara luas. Oleh karenya perlu dilakukan kajian untuk menemukan solusi implementasi *Remote Access Ipsec IKEv2* tersebut.

II. TEORI PENUNJANG

A. *Remote Access IPsec*

Remote access IPsec merupakan salah satu tipe *remote access* VPN yang aman menggunakan fungsi-fungsi kriptografi. *Remote access* VPN memiliki karakteristik utama yaitu adanya pengguna *remote* (jarak jauh) yang memiliki alamat IP yang dinamis yang mengakses jaringan target (jaringan LAN utama) melalui jaringan publik *Internet*.

Remote access IPsec menyediakan mekanisme *tunneling* dan fungsi keamanan dengan mengenkapsulasi paket data dari protokol jaringan yang satu ke protokol jaringan lainnya. Dengan *tunneling*, data yang berasal dari jaringan LAN lokal dapat dikirimkan melewati jaringan *Internet* menuju jaringan tujuan. *Tunnel remote access IPsec* diterminasi pada ujung-ujung *tunnel endpoint* yaitu pada *remote access client* itu sendiri dan suatu *gateway* keamanan dalam hal ini adalah *gateway IPsec*.

IPsec dibentuk oleh tiga protokol utama yaitu IKE, AH, dan ESP. Fungsi manajemen kunci kriptografi dan parameter SA disediakan oleh protokol IKE. Protokol AH dan ESP berfungsi sebagai penyedia mekanisme tunneling komunikasi data, layanan *confidentiality*, *data integrity*, dan *data source authentication*.

Remote access IPsec yang dibangun menggunakan media jaringan publik *Internet* memiliki kelebihan finansial dibanding *remote access* menggunakan media *leased line*. Fitur keamanan yang disediakan oleh IPsec

pun menjadi insentif pertumbuhan *remote access* berbasis IPsec.

B. IKEv2

Internet Key Exchange (IKE) adalah protokol yang digunakan untuk melakukan manajemen seperti pembuatan, pembaharuan, dan penghapusan *security association* (SA) dalam suatu *suite* protokol *IPsec*. IKEv2 bertugas untuk melakukan fungsi autentikasi dari masing-masing pihak yang berkomunikasi.

IKE menggunakan mekanisme pertukaran kunci *Diffie-Hellman* untuk membuat kunci *shared session secret*, yang nantinya digunakan dalam proses pembuatan kunci kriptografi lebih lanjut. Autentikasi antara pihak-pihak yang membangun komunikasi dilakukan dengan menggunakan teknik berbasis *public key* atau berbasis *pre-shared key*. IKE yang pertama (IKEv1) didefinisikan pada November 1998 oleh *Internet Engineering Task Force* (IETF) dalam suatu rangkaian publikasi *Request for Comments* (RFC) yaitu RFC 2407, RFC 2408, and RFC 2409.

IKE kemudian diperbaharui menjadi versi dua (IKEv2) pada Desember 2005 dalam RFC 4306. IKEv2 telah diperluas oleh RFC 4301 (*Security Architecture for the Internet Protocol*) sampai RFC 4309 (*Using AES CCM Mode with IPsec ESP*).

Protokol IKEv2 menggunakan paket UDP pada port 500 dan port 4500, dan biasanya membutuhkan 4 paket dalam 2 kali pertukaran pesan (pesan IKE_SA_INIT dan pesan IKE_AUTH) untuk membuat SA IKE dan SA IPsec bagi kedua *peer* yang dikenal dengan *initial exchange*. Material kunci yang dinegosiasikan kemudian diberikan pada *IPsec stack* di *kernel*. Sebagai contoh, material tersebut bisa berupa kunci AES, informasi identifikasi *endpoint IPsec* dan *port* yang mesti dilindungi serta tipe *tunnel IPsec* yang telah dibangun. *IPsec stack*, di lain pihak, melakukan intersepsi terhadap paket IP dimana proses enkripsi/dekripsi yang sesuai akan diterapkan [28], [32].

Semua komunikasi pada IKE selalu terdiri dari sepasang *request-response.* Sepasang pesan pertama (IKE_SA_INIT) menegosiasikan algoritma kriptografi, mempertukarkan *nonce*, dan melakukan pertukaran Diffie-Hellman (DH). Sepasang pesan kedua (IKE_AUTH) melakukan autentikasi terhadap pesan sebelumnya, mempertukarkan identitas dan sertifikat, dan membangun CHILD_SA pertama. Sebagian pesan pada fase ini terenkripsi dan *integrity protected* dengan kunci yang telah dibuat pada proses pertukaran IKE_SA_INIT, sehingga identitasnya terlindungi dan pesannya terautentikasi [30].

C. IKEv2 StrongSwan

Kebanyakan implementasi perangkat lunak IPsec terdiri dari suatu *daemon* service IKE yang berjalan pada level *user space* dan suatu *IPsec stack* pada level kernel yang memproses paket IP. *Daemon* pada *user space* memiliki akses yang mudah terhadap penyimpanan data yang mengandung konfigurasi informasi. Informasi tersebut adalah seperti alamat *endpoint* IPsec, kunci dan sertifikat. Modul IPsec pada kernel di lain pihak, bisa memproses paket secara efisien dan dengan *overhead* minimum yang penting terhadap performa. Terdapat beberapa implementasi IPsec dan layanan *daemon* IKEv2 yang bersifat *open source* pada lingkungan sistem operasi Linux seperti Openswan, strongSwan, OpenIKEv2, dan racoon2.

StrongSwan merupakan suatu perangkat lunak aplikasi yang menerapkan protokol IPsec dan IKEv2 yang bersifat *open source* dan *free* untuk lingkungan sistem operasi Linux berbasis kernel 2.4 dan 2.6. Ia merupakan turunan dari proyek FreeS/WAN. strongSwan menerapkan IPsec melalui *daemon* IKEv2 bernama charon dan layanan *IPsec stack* berbasis kernel linux NETKEY. NETKEY merupakan implementasi IPsec *native* pada kernel Linux 2.6.

Proyek strongSwan memiliki fokus terhadap mekanisme autentikasi yang kuat dengan menggunakan sertifikat kunci publik X.509 dan penyimpanan *private key* dalam suatu *smartcard* melalui antarmuka standar PKCS#11. Salah satu fitur unggulan yang dimiliki strongSwan adalah penggunaan atribut sertifikat X.509 untuk menerapkan skema *advanced access control* berbasis pada keanggotaan grup. Proyek pengembangan strongSwan disponsori oleh *University of Applied Sciences Rapperswil*, Astaro (sebuah perusahaan yang menawarkan solusi keamanan TI), dan *StrongSec* GmbH.

III. PEMBAHASAN

A. Fase Analisis

Pada tahap ini melakukan penentuan masalah dan penentuan kriteria kebutuhan sistem. Berikut adalah hasil identifikasi fase analisis.

Dari hasil studi *literature* yang telah dilakukan, ditemukan masalah-masalah dan kebutuhan yang bersifat mendasar dan opsional untuk penerapan *remote access IPsec* yaitu sebagai berikut:

1. Kebutuhan algoritma kriptografi yang kuat.
2. Kebutuhan pengulangan autentikasi.
3. Masalah ketidakcocokan NAT dan IPsec.
4. Masalah alamat IP klien IPsec yang *overlapping*.
5. Masalah NAT *Traversal mode transport*.
6. Kebutuhan *peer* IPsec yang *mobile* dan *multihoming*.

1) Kebutuhan algoritma kriptografi yang kuat

Kriptografi dalam *remote access* IPsec dapat dibagi menjadi kedalam beberapa bagian yaitu algoritma *endpoint authentication*, algoritma pembuatan kunci *shared secret*, algoritma *message integrity*, algoritma enkripsi. Saat ini berbagai vendor penyedia solusi sistem *remote access* IPsec memiliki suatu *set* algoritma kriptografi atau *algorithm suite* sendiri. Pilihan–pilihan algoritma yang bervariasi tersebut belum tentu

menyediakan tingkat keamanan yang baik. Salah satunya adalah pilihan algoritma *digital signature* RSA sebagai algoritma autentikasi *endpoint*, pilihan grup MODP Diffie-Hellman 768bit dan 1024bit sebagai input dalam algoritma pembuatan *shared secret*, pilihan HMAC-MD5-96 sebagai algoritma *message integrity*, dan pilihan algoritma 3DES atau CAST128 sebagai algoritma enkripsi.

Permasalahnya adalah dengan semakin berkembangnya kekuatan komputasi, mereka membutuhkan ukuran kunci yang besar untuk tetap aman. Peningkatan ukuran kunci akan meningkatkan beban pemrosesan komputer dan juga akan meningkatkan ukuran paket data sehingga menyebabkan lalulintas data tambahan pada jaringan.

2) Kebutuhan pengulangan autentikasi

Dalam skenario *remote access*, terkadang masing-masing *peer* IPsec ingin melakukan autentikasi mutual diulangi secara periodik. Proses ini disebut sebagai pengulangan autentikasi. Tujuan pengulangan autentikasi adalah untuk membatasi waktu bahwa suatu SA dapat digunakan oleh pihak ketiga yang telah mengambil alih kendali *peer* IPsec.

Masalahnya adalah proses pengulangan autentikasi bisa saja dilakukan dengan secara sederhana mengulang proses *initial exchange*, akan tetapi pada skenario remote access IPsec akan menjadi masalah karena dibutuhkan interaksi user pada klien remote access untuk membuat ulang proses *initial exchange*. Oleh karena itu, dibutuhkan suatu prosedur otomatis yang bisa menjalankan skema pengulangan autentikasi secara periodik tanpa interaksi user. Selain itu dibutuhkan suatu standar rentang waktu untuk pengulangan autentikasi.

3) Masalah ketidakcocokan NAT dan Ipsec

Remote Access VPN terutama digunakan untuk menyediakan akses bagi pengguna *remote access* seperti *teleworker* (bekerja dari rumah) atau *mobile user*. Pengguna tersebut umumnya berada dalam suatu lingkungan yang menjalankan fungsi NAT. Berdasarkan RFC3715 (IPsec-NAT *Compatibility Requirements*), diketahui bahwa penerapan IPsec dalam suatu lingkungan NAT tidak dapat berjalan lancar atau dengan kata lain terdapat ketidakcocokan antara IPsec dengan NAT. Luasnya penggunaan NAT membuat penerapan IPsec sebagai solusi standar VPN khususnya *remote access* VPN mengalami hambatan.

Salah satu penyebab masalah ketidakcocokan antara NAT dan IPsec adalah mekanisme kerja kedua teknik tersebut yang saling bertolak belakang. Di satu sisi, NAT memodifikasi data alamat dan nomor port pada header IP. Di sisi lain, IPsec mencoba memberikan suatu tingkat pengamanan komunikasi data dengan mengantisipasi adanya modifikasi itu. Jadi pada dasarnya IPsec berfungsi untuk mencegah apa yang NAT lakukan dan secara *fundamental* saling berlawanan.

4) Masalah alamat IP klien-klien IPsec yang overlapping

Berdasarkan RFC3715 (IPsec-NAT *Compatibility Requirements*) pada bagian 2.1 poin e, terdapat sebuah kemungkinan kasus yang dapat menimbulkan konflik pada penerapan IPsec *mode* operasi *tunnel* dalam situasi NAT *Traversal*. Yaitu ketika terdapat *IPsec Remote Access Client* (IRAC) yang memiliki alamat IP yang saling *overlapping* (tumpang tindih). *IPsec Remote Access Server* (IRAS atau *gateway* IPsec akan melihat klien-klien tersebut sama karena memiliki alamat IP yang sama sehingga akan memiliki SA IPsec yang akan *overlapping*. *Server* bisa saja menggunakan SA yang salah ketika akan mengirimkan paket dari jaringan LAN ke klien IPsec. Masalah ini membutuhkan solusi lain yang tidak dapat diselesaikan hanya dengan menggunakan mekanisme NAT *Traversal* saja.

5) Masalah NAT Traversal mode transport

Berdasarkan RFC3938 (*UDP Encapsulation of IPsec ESP Packets*) pada bagian 5.2, terdapat situasi yang berpotensi menimbulkan masalah IPsec pada *mode* operasi *transport* dalam situasi NAT *Traversal*. Misalnya terdapat beberapa klien dibelakang NAT yang sama membangun suatu VPN IPsec mode *transport*. Bagi *server* IPsec, dalam mode *transport*, klien-klien dibelakang NAT adalah klien yang sama baginya, yaitu alamat IP NAT eksternal. SA yang dibangun antara server IPsec dan NAT memuat *traffic description* yang berisi keterangan protokol dan informasi *port*. Jika *traffic description* tersebut saling *overlapping* (tumpang tindih), maka server bisa mengirimkan paket IPsec ke klien dengan SA yang salah.

6) Kebutuhan peer IPsec yang mobile dan multihoming

IKEv2 digunakan untuk melakukan autentikasi mutual dan juga untuk membangun dan mengelola SA (Security Association). SA IKE dan SA IPsec mode tunnel dibuat secara implisit antara alamat IP yang digunakan ketika SA IKE dibangun. Alamat IP ini kemudian digunakan sebagai *outer IP header* (*header* IP terluar) pada paket IPsec mode *tunnel*. Jika SA IKE telah dibuat, maka menjadi tidak mungkin untuk mengubah alamat IP tersebut. Terdapat skenario dimana alamat IP tersebut bisa berubah. Misalnya terdapat suatu klien IPsec yang *mobile* dan sering berpindah jaringan sehingga memiliki alamat IP yang sering berubah. Selain itu terdapat juga klien yang bersifat *multihoming* yang terhubung ke lebih dari satu jaringan dengan *interface*-nya masing-masing. Jika *interface* yang digunakan untuk membangun *tunnel* IPsec tiba-tiba *down*, maka *peer* IPsec itu harus membangun dari ulang kembali SA IKE dan SA IPsec. Pembangunan ulang *tunnel* bukan merupakan pilihan yang ideal bagi *user remote access* dikarenakan

dibutuhkan adanya interaksi *user*. Untuk alasan tersebut, dibutuhkan suatu mekanisme yang mampu melakukan *update* alamat IP untuk SA IKE dan IPsec tanpa membuat ulang *tunnel* baru.

IV. KESIMPULAN

Kesimpulan yang didapatkan yaitu dari beberapa permasalahan yang ditemukan pada penerapan Remote Access IPSec VPN berbasis IPsec seperti masalah kebutuhan algoritma kriptografi yang kuat, kebutuhan pengulangan autentikasi, masalah ketidakcocokan Network Address Translator (NAT) dan IPsec, masalah konflik alamat klien IPsec yang overlapping, masalah NAT Traversal mode transport, masalah kebutuhan peer IPsec yang mobile dan multihoming berhasil diatasi dengan menggunakan sistem *Remote Access* IPsec berbasis perangkat lunak IKEv2 strongSwan dengan beberapa solusi skenario yang dibangun.

Untuk pengembangan lebih lanjut dapat dikaji penerapan sistem autentikasi IPsec *Extensible Authentication Protocol* (EAP) dalam IKEv2, dan juga dapat dilakukan pengujian interoperabilitas antara Sistem Linux sebagai IPsec *server* dan klien berbasis sistem operasi Windows dalam kerangka protokol IKEv2 serta melakukan implementasik IKEv2 Strongswan dalam suatu lingkungan sistem jaringan yang menawarkan *redundancy* seperti konsep *IPsec failover and redundancy* atau *high cluster IPsec server, dan juga m*elakukan manajemen terhadap *Remote Addres Virtual* IP menggunakan suatu *database* berbasis SQL.

DAFTAR PUSTAKA

[1] A. Huttunen, B. Swander , V. Volpe , L. DiBurro , M. Stenberg , "UDP Encapsulation of IPsec ESP Packets" , RFC 3948, January 2005

[2] B. Aboba, W. Dixon , "IPsec-Network Address Translation (NAT) Compatibility Requirements", RFC 3715, March 2004

[3] Burnett, Steve, Stephen Paine, RSA Security's Official Guide to Cryptography, California: McGraw-Hill/Osborne, 2004

[4] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005

[5] Comparison and Analysis of IP and IKEv2 Mobility Extensions, Chandani Haresh, HelsinkiUniversityof Technology

[6] Forouzan, Behrouz A., Data Communications and Networking Third Edition, NY: McGraw-Hill, 2003

[7] Harrell, Charles, Biman K Ghosh, Royce O. Bowden Jr., Simulation Using Promodel Second Edition, NY:McGraw-Hill, 2004

[8] Internet Key Exchange (IKE) protocol vulnerability risks, Ari Muittari, Master's thesis seminar 18.5.2004, HUT, Networking Laboratory

[9] IPSec/IKE Protocol Hacking ToorCon 2K2 – San Diego CA, Anton Rager Sr. Avaya Security Consulting

[10] "IPSec and NAT-T: Finally in harmony?", Steve Riley, Microsoft Tech Ed. 03 10th anniversary

[11] Joel M Snyder, IPsec and SSL VPNs: Solving remote access problems, http://searchsecurity.techtarget.com/searchSecurity/downloads/Snyder.VPN.ORIGINAL.ppt, diakses 30 Juli 2010 15:24WIB

[12] L. Law and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 4869, May 2007.

[13] Nasuhi, Hamid, Ropi Ismatu, dkk. Pedoman Penulisan Karya Ilmiah Skripsi, Tesis dan Disertasi. Jakarta: CeQDA, 2007.

[14] NAT Traversal for IPsec, Research Seminar on Data communications Software HIIT, 09.11.2005

[15] Pandia, Henry. Teknologi Informasi dan Komunikasi. Jilid I, II dan III. Jakarta: Erlangga, 2007.

[16] P. Erone , "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[17] Rawles, Philip T., James E. Goldman, Applied Data Communications: A Business-Oriented Approach, 2001 ISBN 0-471-37161-0

[18] Scott Kelly, IPsec Remote Access Requirements, IPsec Remote Access Working Group 49th IETF, http://www.vpnc.org/ietf-ipsra/ietf49-requirements.ppt, diakses 30 Juli 2010 15:24WIB

[19] Special Publication 800-57, *Recommendation for Key Management* , National Institute of Standards and Technology, 2007

[20] Sunyoto, Aris Wendy, VPN Sebuah Konsep, Teori dan Implementasi, BukuWeb Networking, 2008

[21] Tanenbaum, Andrew S., Modern Operating Systems Second Edition, NJ: Prentice-Hall, 2001

[22] T. Kivinen , B. Swander , A. Huttunen, V. Volpe , "Negotiation of NAT-Traversal in the IKE" , RFC 3947, January 2005

[23] Tulloch, Mitch, Microsoft Encyclopedia of Networking eBook, Microsoft Press, 2000

[24] White Paper: Remote Access VPN and IPSec , NCP Secure Communication, April 2001, http://www.symtrex.com/pdfdocs/wp_ipsec.pdf, diakses 30 Juli 2010 15:24WIB

[25] White Paper: Virtual Private Networks Solutions for Remote Access, Comparison of IPSEC and SSL, 2004 Schlumberger Information Solutions, Houston, Texas.http://www.slb.com/media/services/consulting/infrastructure/whitepaper_vpnsra.pdf, diakses 30 Juli 2010 15:24WIB

[26] Wijaya, Ir. Hendra, Cisco ADSL Router, PIX Firewall, dan VPN, Jakarta:PT Elex Media Komputindo, 2006

[27] Y. Nir, "Repeated Authentication in Internet Key Exchange (IKEv2) Protocol", RFC 4478, April 2006

[28] http://www3.tools.ietf.org/html/rfc4306, Internet Key Exchange (IKEV2) Protocol, 30 Juli 2010, 15:23 WIB

[29] http://www3.tools.ietf.org/html/rfc4869, Suite B Cryptographic Suites for IPSec, 30 Juli 2010, 15:23 WIB

[30] http://www3.tools.ietf.org/html/rfc4478, Repeated Authentication in Internet Key Exchange (IKEV2) Protocol , 30 Juli 2010, 15:23 WIB

[31] http://www3.tools.ietf.org/html/rfc3947, Negotiation of NAT-Traversal in the IKE, 30 Juli 2010, 15:23 WIB

[32] http://www3.tools.ietf.org/html/rfc3948, UDP Encapsulation of IPSec ESP Packets , 30 Juli 2010, 15:23 WIB

[33] http://www3.tools.ietf.org/html/rfc4555, IKEV2 Mobility and Multihoming Protocol (MOBIKE) , 30 Juli 2010, 15:23 WIB